H4CK3R #13

PARENTAL ADVISORY
EXPLICIT SOFTWARE

Exploits

+de 60 programas para explorar vulnerabilidades em:

- Windows Server 2003
- Windows 98
- Windows Media Player
- Microsoft Word
- Word Perfect
- mIRC
- MySQL
- DCP Portal
- HPUX
- Easy File Sharing
- PHP
- Red Hat
- IBM DB2
- roteadores Cisco
- MyPHPNuke
- Solaris
- RealOne Player

Trainers

Seja um fera nos games, destruindo seus inimigos sem fazer força. Programas para os jogos:

- Mace Griffin: Bounty Hunter
- Western Outlaw: Wanted Dead or Alive
- Warlords 4
- Commandos 3: Destination Berlin
- Max Payne 2: The Fall of Max Payn
- Command & Conquer: Generals - Zero Hour
- WarCraft 3 (Mission Unlocker
- Test Drive 6
- Alone in the Dark 4
- Championship Manager 4
- Hitman 2: Silent Assassin
- Silent Hill 2: Director's Cut
- Halo: Combat Evolved
- Freedom Fighters
- Tony Hawk's Pro Skater 4

Patches

Atualize seu sistema. Pacotes de correções para os SOs:

- Debian
- SuSE
- Red Hat
- Windows

E ainda:

Discador Digerati: a primeira Internet grátis para Linux do Brasil! (também com versão para Windows)

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

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

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

Redes Alternativas

Cansado do KaZaA? Então teste estas alternativas perfeitas para hackers

- Apollon 0.8 (Linux)
- BitSpirit 1.0.7 Beta
- BitTorrent ++ (Linux)
- BitTorrent 3.3
- Effusion 0.3
- eMule 0.30b LSD
- eMule 0.30c Sivka v10
- giFT (Linux)
- giFTcurs (Linux)
- giFToxic (Linux)
- Matrix Public Net 0.3-2 (Linux)
- MLDonkey (Linux)
- MLDonkey Server Spy 1.2 (Linux)
- NovaP2P 1.8
- PySoulSeek (Linux)
- Tesla 3.04t2
- The Hunting of the Snark (Linux)
- TorrentSniff 0.30 (Linux)
- Waste (Linux)
- Web giFT (Linux)
- xMule 1.6.1 (Linux)
- Xnap 3.0
- Xnap 3.0 (Linux)

Registro

Tutorial completo e ferramentas para você dominar de verdade o seu Windows. Inclui aplicativos de edição, backup e monitoração de ações suspeitas no registro (como vírus, trojans, etc.):

- Advanced Registry Optimizer 1.3.2
- Regmon 6.06 (NT/2000/XP)
- RegKey Backup 1.0
- MV RegClean 3.1
- DiamondCS Registry Prot 2.0
- Reg Cool 2.408
- Registrar Lite 2.00
- Registry Mechanic 2.01
- Registry Medic 2.9
- Registry TuneUp 1.0
- Win/Crypto
- NT REG
- Ms Decripter
- Rm Toolkit
- NT Reg Pack
- Cain
- Chron
- Anna Klean

Segurança

Pacote especial com as 30 melhores ferramentas para transformar o seu computador em uma superfortaleza. Destaques:

- Nmap v3.48
- IPTables v1.2.8
- Nessus v2.0.8a
- Big Brother v1.9b
- BlackHole Spam/Virus Filter v1.0.9
- SSH v3.0.0
- IPChains v1.3.10
- SAINT v5.0.6
- TCPDump v3.7.2
- Tripwire v2.3.1-2
- Firestorm NIDS v0.5.4
- Socks via HTTP v1.0.1
- VisualRoute v7.0
- SMTP HoneyPot
- Snort v2.02
- AirSnort v0.2.2a
- Anti-Spam SMTP Proxy Server v1.0.6
- Tight VNC v1.2.9

SlackPKG: Mantenha seu Slackware atualizado e seguro para não ter de esquentar a cabeça

H4CK3R

grep -i root

A intimidade do Windows

HACKING DE REGISTRO

Quem domina o registro é o senhor do SO

No CD:

Mais de 15 programas para recuperar senhas, otimizar seu sistema e limpar evidências presentes no registro do Windows

Sentry Firewall Linux

Firewall Completo

Sem Instalar

Proteja seu PC e sua rede com um sistema de defesa completo que não precisa ser instalado e já vem com as melhores ferramentas, incluindo: Nmap, Snort, Apache, Samba e muito mais

Linux Essential Security Kit

Linux Box Indestrutível

No CD: Seleção com os melhores softwares de segurança para Linux. Confira no verso!

Programação segura e eficiente

Profiling

Aprenda a programar com performance e segurança redobradas

Consultas DNS

Os segredos do footprint, BIND e consultas reversas

Veja mais destaques do CD no verso da revista

R$ 11,90 Ano III # 13
www.digerati.com.br
ISSN 1676-3068

EDITORIAL

Será que o Brasil está virando realmente um laboratório do cybercrime? Esse é o título da matéria que saiu no jornal New York Times, citando inclusive a nossa revista. É realmente difícil acreditar na imprensa não-especializada (na especializada também) quando a discussão é hackerismo e conhecimento avançado em computação. Como as pessoas não conseguem entender a cultura digital, partem para os estereótipos fáceis. Para o NYT, o Brasil é um grande celeiro de criminosos digitais. Por outro lado, para a revista de uma emissora "jovem" de São Paulo, geeks são os tarados pela Rede. São mais estereótipos para um geek: moleque com problemas de relacionamentos pessoais, cheio de espinhas e meio doido. Nada mais longe da realidade.

A diferença está na relação com o conhecimento. A revista H4ck3r não se preocupa em ensinar coisas ilegais, mas também não evita assuntos porque alguém pode usar o conhecimento para coisas ilegais. Então, o negócio é evitar os estereótipos e partir para o estudo sistemático. E nada de se dedicar somente à computação. Há diversos outros assuntos desafiadores, esperando respostas.

O Editor

TOW

Falha no DB2 cede controle do sistema

IBM já tem patch

Esta notícia é problema para usuários de grandes sistemas corporativos de bancos de dados. Um dos mais usados e confiáveis deles, o DB2, da IBM, possui duas sérias falhas de segurança que permitem que um intruso assuma o controle completo do servidor. As versões são a 7.2 para Linux em plataforma Intel, e a 7.2 para Linux em máquinas s390.

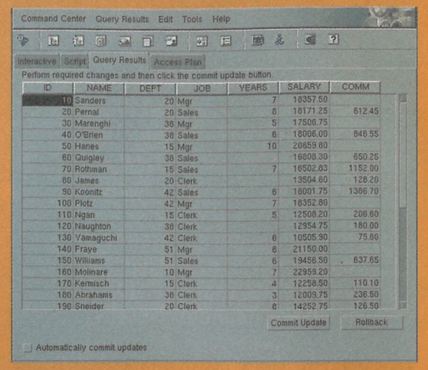
As falhas permitem que um atacante provoque um estouro de memória e ganhe o direito de executar programas no sistema com nível de superusuário.

Para saber mais sobre essa falha, acesse o site do Core Security Technologies, na URL abaixo:

www.coresecurity.com/common/showdoc.php?idx=366&idxseccion=10

A correção oferecida pela IBM para eliminar a brecha está disponível em:

www-3.ibm.com/cgi-bin/db2www/data/db2/udb/winos2unix/support/download.d2w/report



Microsoft IIS é o software mais vulnerável

Lista foi elaborada pela SANS

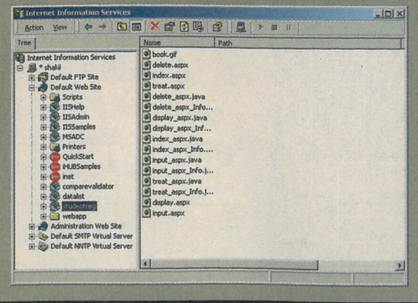
Só para não dizerem que é má vontade nossa, quem está dizendo isso é a SANS (SysAdmin Audit Network Security). A empresa de segurança chegou à conclusão que todos, empiricamente, já haviam observado. O IIS, servidor Web da Microsoft, é o programa com maior número de vulnerabilidades no último ano. Só não dá pra entender por que ainda tem gente preferindo usar esse software em vez do Apache...

Na lista feita pelo site com o top 20 de vulnerabilidades, o IIS ganhou disparado. Só no último ano, a Microsoft deu alarme de mais de meia dúzia de vulnerabilidades. Fora isso, houve também o vírus CodeRed, que se aproveitava de uma falha nesse servidor para se disseminar na Rede.

Logo depois, aparecem na lista para plataforma Windows o MSSQL Server, Windows Authentication e Internet Explorer.

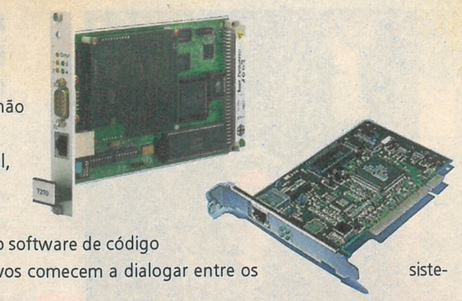
Para Unix, os programas com mais falhas são o BIN Domain Name Services, os serviços de RPC e, só em terceiro (numa lista com programas bem mais seguros que os de plataforma Windows), o servidor Web Apache.

A lista com o top 20 de vulnerabilidades da SANS pode ser vista em *http://isc.sans.org/top20.html*.



Troca-troca digital

Projeto faz Linux rodar drivers de Windows



Atualmente, em termos de aplicações comuns, como os softwares de escritório, não há motivos para evitar a migração do Windows para o Linux. Com efeito, são inúmeros os softwares como os do pacote OpenOffice, além de clientes de e-mail, browsers, etc. que não fazem feio frente às suas versões proprietárias. E mais: normalmente, esses softwares também têm suas versões para Win.

Bom, disso você sabe. E qual a novidade desta nota? É que o desenvolvimento do software de código aberto está tão avançado que agora o pessoal quer que os drivers de dispositivos comecem a dialogar entre os sistemas operacionais.

Subvertendo a tradição de que um driver só pode ser escrito exclusivamente para a plataforma a que se destina, a empresa canadense Linuxant acaba de criar o DriverLoader, que, grosso modo, nada mais é do que um tipo de emulador que possibilita ao Linux carregar e reconhecer drivers escritos para Windows.

Até o fechamento desta edição, os pacotes do DriverLoader estavam disponíveis para download gratuito por meio de uma licença trial. Trial? Sim, ainda não há certeza de que o DriverLoader permanecerá sempre livre para os usuários finais.

De qualquer forma, vale a pena conferir, ao menos enquanto não há confirmação disso. O DriveLoader é compatível com os kernels 2.4 e 2.6, tem enfoque em drivers para LANs e, no momento, oferece um "demo" que permite usar, no Linux, dispositivos wireless 802.11g (CardBus e PCI) baseados em chipsets Broadcom, cujos drivers são escritos para Win32.

Site: *www.linuxant.com/store*

Antivírus para proteção de celular

Especialistas afirmam que código malicioso está próximo

Em 2004, os celulares terão antivírus. Esse é o projeto que está sendo desenvolvido por duas grandes empresas do ramo, a NTT DoCoMo e a McAfee. A japonesa NTT é uma das maiores empresas de telecomunicações do mundo, pioneira na inserção de conteúdo multimídia em celulares.

O objetivo é se antecipar à distribuição de códigos maliciosos que deverão começar a surgir por causa dos novos celulares que aceitam inclusive a instalação de softwares. Até o momento, felizmente, só um worm que ataca telefones móveis foi descoberto, o Timofonica.

Apesar de preocupante, o worm não era muito perigoso, já que ele só reenviava mensagens SMS a números telefônicos gerados aleatoriamente. As pesquisas estão sendo aceleradas pelas proporções de um vírus que poderia se propagar de forma muito rápida.

Emprego zero

Lista reúne profissionais e empresas especializados em segurança

Você sabe tudo sobre segurança digital, tem um monte de cursos no currículo, experiência a dar com pau e, no entanto, não consegue de jeito nenhum arrumar um trabalho digno? A solução pode estar em uma lista de discussão.

Não. Não se trata de mandar currículo para os amigos, mas de uma lista hospedada no Yahoo! Groups especialmente criada para esse fim: a SecurityGuys, que pretende agregar empresas e profissionais de segurança.

A lista imita a SecurityJobs, que pertence ao SecurityFocus.com. Não são permitidas discussões entre os membros, apenas o envio de informativos de interesse profissional e, claro, anuncios de empregos. Além disso, há moderação, para evitar mensagens fora do tema. A iniciativa é do especialista Ronaldo Vasconcellos.

Site: *groups.yahoo.com/group/SecurityGuys*

Pior que o sonso

Tinha que ser o patch do Windows

Tem acontecido sempre com os Service Pack da Microsoft: você faz o download pensando em tornar o seu Windows mais seguro, e milhões de problemas acabam aparecendo, especialmente em performance. Parece que as equipes de programadores da Microsft andam meio estafadas.

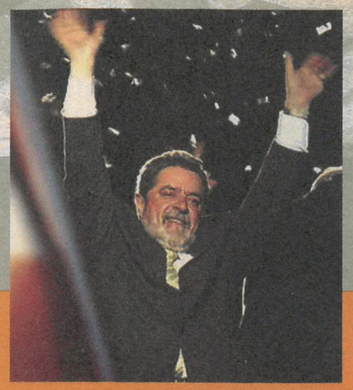
Agora foi a vez do Windows 2000 SP4 na versão para alguns idiomas, entre eles o português de Brasil e Portugal. O pacote causa erros de execução de alguns programas e instabilidade no sistema operacional.

Uma das correções de segurança do SP4 é uma vulnerabilidade que permite a execução de código explorando uma falha de buffer overflow nos controles ListBox e ComboBox do Windows.

Os usuários experimentaram, depois de instalar o pack, um problema com o antivírus e muitas telas azuis da morte (como se já não aparecessem em número suficiente).

Até o fechamento desta edição, não havia ainda uma solução para os imeasses do patch. A única saída é desinstalá-lo e manter o sistema aberto a hackers.

Ele e Aos usuários, só resta chorar



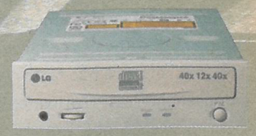
Lula Livre!

Linux vira pré-requisito para utilização de serviço governamental

Por essa as desenvolvedoras de softwares proprietários não esperavam. O software livre deverá tornar-se obrigatório para a instalação de banda larga no novo serviço público que será criado para possibilitar o uso de recursos do FUST (Fundo de Universalização dos Serviços de Telecomunicações).
A informação foi dada pelo ministro das Comunicações, Miro Teixeira, que, no entanto, também disse que haverá um período de transição, no qual será permitida a convivência entre softwares livres e proprietários, como Linux e Windows. O novo serviço de telecomunicações para acesso à Web em banda larga deve entrar em consulta pública em novembro de 2003 (após a data de fechamento desta edição).
Ele foi a solução encontrada pelo governo Lula, Anatel e Tribunal de Contas da União para estimular a concorrência nas licitações que poderão usar o FUST, cujo saldo já ultrapassa R$ 2 bilhões. Isso porque a lei exige que o dinheiro do fundo só possa ser gasto com a contratação de uma concessionária de serviço público.
Desenvolvendo a nova ferramenta, empresas de telefonia, operadoras de TV a cabo e outras companhias poderão participar das licitações do FUST. E o governo Lula dá mais um incentivo ao Linux. Yeah!

Novo Mandrake 9.2 destrói drives LG

Cuidado com o pingüim



Os novatos que se cuidem. Distribuições populares andam chegando com bugs para assustar de vez qualquer newbie. A versão 9.2 do Mandrake, por exemplo, se revelou uma bomba para diversos modelos de drives LG.
O problema estaria no firmware do drive, que se deixa sobrescrever por um arquivo de sistema do Mandrake. Mas, obviamente, como o SO foi desenvolvido posteriormente, é a sua programação que contém a falha, por não prever esse comportamento por parte do firmware.
O problema ocorre durante a instalação, seja via CD-ROM ou por uma rede. A mensagem "unable to install the base system" surge na tela e, após o computador ser reinicializado, o drive de CD simplesmente deixa de funcionar.
Para saber mais detalhes e consertar a falha, vá ao site www.mandrakelinux.com/en/lgerrata.php3

Drives afetados:

- COMPAQ CRD-8322B(CP1, também usado no IBM Aptiva 2158-125)
- CRD-8400B (usado no Dell Optiplex GX1 e IBM PC 300PL)
- CRD-8400C (Compaq)
- COMPAQ CRD-8402B
- LG CRD-8480C (usado no Dell XPS T650r)
- GCR-8481B (usado no Dell Optiplex gx270; ROM versão 1.06, junho de 2003)
- CRD-8482B (usado no Dell Optiplex GX1 e Dell Precision 220)
- GOLDSTAR CDR-8482B (usado no HP Vectra VL400; versão do firmware: 1.01)
- Computadores HP Vectras série VL4xx
- GCC-4480B DVD/CD-R/RW/CDROM (Firmware 1.00 - atualizar o firmware para a versão 1.01 evita o problema)

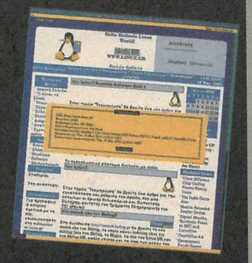
Free software never dies!

Projeto GNU completa 20 anos de vida

Muito se fala e se estuda sobre o sistema operacinal open source "Linux", independente de sua superioridade e qualidade o sistema tornou-se conhecido em todo mundo simplesmente por ter profissionais totalmente capacitados por trás levando o projeto a serio. Com toda clareza, podemos dizer que hoje em dia o Linux é uma ameça ao reinado da Microsoft, principalmente em PCS home users. O fato que poucos sabem é que o Linux não é somente um sistema operacional criado por Linus Torvalds, ou por uma empresa sem fins lucrativos, por trás de Torvalds e do Linux existe o projeto "GNU" ou "GNU/Linux", como queiram denominar.
Em 27 de setembro de 1983, Richard Stallman, então pesquisador do laboratório de inteligência artificial do MIT, enviou uma mensagem para a rede UseNet com a frase "Libertem o Unix!". Com isso, ele deu o pontapé inicial do projeto GNU, com o propósito de criar um sistema operacional similar ao Unix, mas com

Links com suporte gráfico

Navegador em modo texto agora mais prático



O pequeno browser em modo texto que sempre foi sinônimo de praticidade e velocidade agora ganhou suporte GUI. Assim, a mesma funcionabilidade e agilidade já oferecidas em modo texto podem ser aproveitadas em modo gráfico - ter a possibilidade de visualizar imagens nos mais variados formatos no terminal é um fato que, na opinião de muitos usuários, torna o browser praticamente perfeito! Para quem utiliza um sistema operacional como o Linux, por exemplo, e quer navegar na Web sem muitas frescuras, o Links é a melhor opção. E isso vale sobretudo para quem não possui um PC extremamente rápido e tem muita dor de cabeça quando tenta visualizar uma página utilizando o Mozilla ou outro navegador do gênero, que são extremamente pesados.
O funcionamento do Links é simples: basta executá-lo em um terminal, de preferência, sendo que ele fica ainda mais prático ao ser executado em uma outra seção no Linux.
Para mais informações, consulte o site:

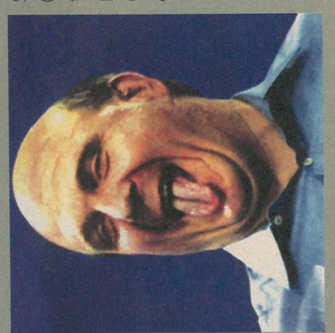
http://atrey.karlin.mff.cuni.cz/~clock/twibright/links/features.html

uma diferença primordial: possível de ser copiado, distribuído e alterado por qualquer pessoa.
Hoje o projeto é apoiado por diversos usuários e tem milhares de colaboradores em todo o mundo, graças a esse projeto, o Linux é um dos sistema operacionais mais utilizados no mundo, só perdendo para o sistema da Microsoft, o Windows.

Microsoft IIS é o software mais vulnerável

Lista foi elaborada pela SANS

Só para não dizerem que é má vontade nossa, quem está dizendo isso é a SANS (SysAdmin Audit Network Security). A empresa de segurança chegou à conclusão que todos, empiricamente, já haviam observado. O IIS, servidor Web da Microsoft, é o programa com maior número de vulnerabilidades no último ano. Só não dá pra entender por que ainda tem gente preferindo usar esse software em vez do Apache...
Na lista feita pelo site com o top 20 de vulnerabilidades, o IIS ganhou disparado. Só no último ano, a Microsoft deu alarme de meia dúzia de vulnerabilidades. Fora isso, houve também o vírus CodeRed, que se aproveitava de uma falha nesse servidor para se disseminar na Rede.
Logo depois, aparecem na lista para plataforma Windows o MSSQL Server, Windows Authentication e Internet Explorer.



Para Unix, os programas com mais falhas são o BIN Domain Name Services, os serviços de RPC e, só em terceiro (numa lista com programas bem mais seguros que os de plataforma Windows), o servidor Web Apache.
A lista com o top 20 de vulnerabilidades da SANS pode ser vista em *http://isc.sans.org/top20.html*.

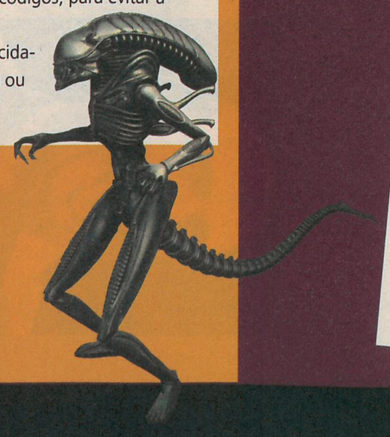
Eles estão chegando

Cuidado com os vírus do futuro

Se você já morre de medo das pragas virtuais de atualmente, espere só pra ver a nova geração desses vermes que povoam as nossas caixas de e-mail. Os novos tipos de spam e malware de hoje em dia já dão dicas sobre esse futuro.
Segundo a empresa de consultoria britânica de segurança mi2g, surgirá uma nova ameaça: os "agentes malware inteligentes distribuídos", ou DIMA.
Eles terão, misturados em um só código, recursos de worms, trojans e vírus, constituindo-se numa só ameaça. A empresa chegou a citar as principais características que os DIMA podem ter, e todas elas provam que teremos que enfrentar criaturas cada vez mais inteligentes.

A ameaça dos DIMA

O que poderão fazer os vírus do futuro
- Ocultar-se até que muitas máquinas já estejam infectadas
- Apagar seus rastros com eficiência
- Infectar plataformas múltiplas
- Fazer o download de cavalos de Tróia, spyware e outros códigos maliciosos de locais remotos, até mesmo via wireless
- Mapear a topologia de sistemas
- Fragmentar códigos, para evitar a detecção
- Possuir capacidade de latência ou incubação



Rootcheck v0.3

Nova versão do programa que detecta rootkits

Rootcheck é um programa que tem a função de detectar rootkits em sistemas. A partir do momento em que uma máquina está conectada à rede, a primeira está exposta a ataques dos mais variados tipos nos mais diversos serviços "daemons", sendo que, na maioria das vezes, o ataque é efetuado com sucesso. E por mais que o sistema atacado seja seguro, a cada dia surgem novos bugs que podem colocar todo um trabalho e reputação a perder.
Por esse motivo, a utilização de um IDS, ou, no caso mais específico, de um Rootkit, é essencial, pois quando o ataque do HACKER é executado sucesso, ele vai querer ter acesso novamente à máquina, instalando um conjunto de ferramentas que garanta seu acesso "invisível" no futuro, no caso um rootkit.
O Rootcheck detecta os principais rootkits, como o suckit, adore, etc. Para mais informações, consulte o site:

http://www.honeypot.com.br/tools.htm

MS patrocina software livre

Se não pode vencê-los, junte-se a eles

Será essa a idéia da Microsoft ao patrocinar um evento internacional de software livre que acontece na cidade de Curitiba, em novembro. Afinal, depois de tantos ataques contra o software livre e contra a GPL, será que a empresa de Bill Gates agora resolveu mudar de estratégia?
Para qualquer conhecedor das artimanhas da Microsoft, é preciso tomar muito cuidado, uma vez que a empresa é versada em acabar com a concorrência, incorporando empresas. Ou seja, compra a concorrente.
O patrocínio foi mal recebido na comunidade Linux, gerando até protestos na Internet.

Java virtual machine não é segura

Estudante quebra proteção com lâmpada comum

O estudante indiano Sudhakar Govindavajhala anunciou recentemente que havia conseguido quebrar a proteção de segurança das máquinas virtuais Java em diversos devices, desde PCs até Smart Cards. O anúncio causou um grande alvoroço na comunidade de informática do mundo. O estudante, atualmente cursando a Universidade de Princeton, nos EUA, afirma que conseguiu a proeza usando uma lâmpada comum e um pequeno programa escrito em Java.
Depois da primeira demonstração no Institute of Electrical and Electronic Engineers (IEEE), a agenda de Govindavajhala ficou lotada. Foram palestras na NASA, Intel e IBM entre outras empresas voltadas para segurança e desenvolvimento de hardware.
A descoberta da falha de segurança é uma das mais importantes dos últimos tempos e será o principal desafio dos próximos anos, principalmente para as empresas de equipamentos portáteis.

Falsa identidade

Novo worm age passando-se por antivírus

Falar de worms em uma revista como a Hacker parece até brincadeira. Afinal, qualquer pessoa mais ligada em segurança sabe que a Web está abarrotada de códigos desse tipo - e, normalmente, também sabe como se proteger.
Entretanto, quando um worm consegue enganar os usuários afirmando ser um antivírus, a estratégia é digna de nota.
Descoberto recentemente, o Sober.A usa o nome de vacinas famosas para se propagar. Ele chega por e-mail trazendo arquivos anexos que copiam nomes de antivírus conhecidos.
As mensagens de texto que apareceram até o momento estão em inglês ou alemão, e o worm tem a peculiaridade de gerar duas cópias de si no computador, de modo que, mesmo se uma for removida, a outra continuará a gerar estragos.
Estragos que, na verdade, não parecem muito grandes, ao menos segundo apuramos até o fechamento desta edição.
Quando muito, o Sober consome memória, no qual se instala - além, é claro, de se propagar pela lista de endereços por meio de um sistema SMTP particular.
Quando o arquivo anexo é carregado, o worm também exibe uma mensagem de erro, como esta que ilustra a nota.
O estratagema de usar nomes de antivírus, porém, merece atenção. Vai que surge um worm menos inocente que compre a idéia?

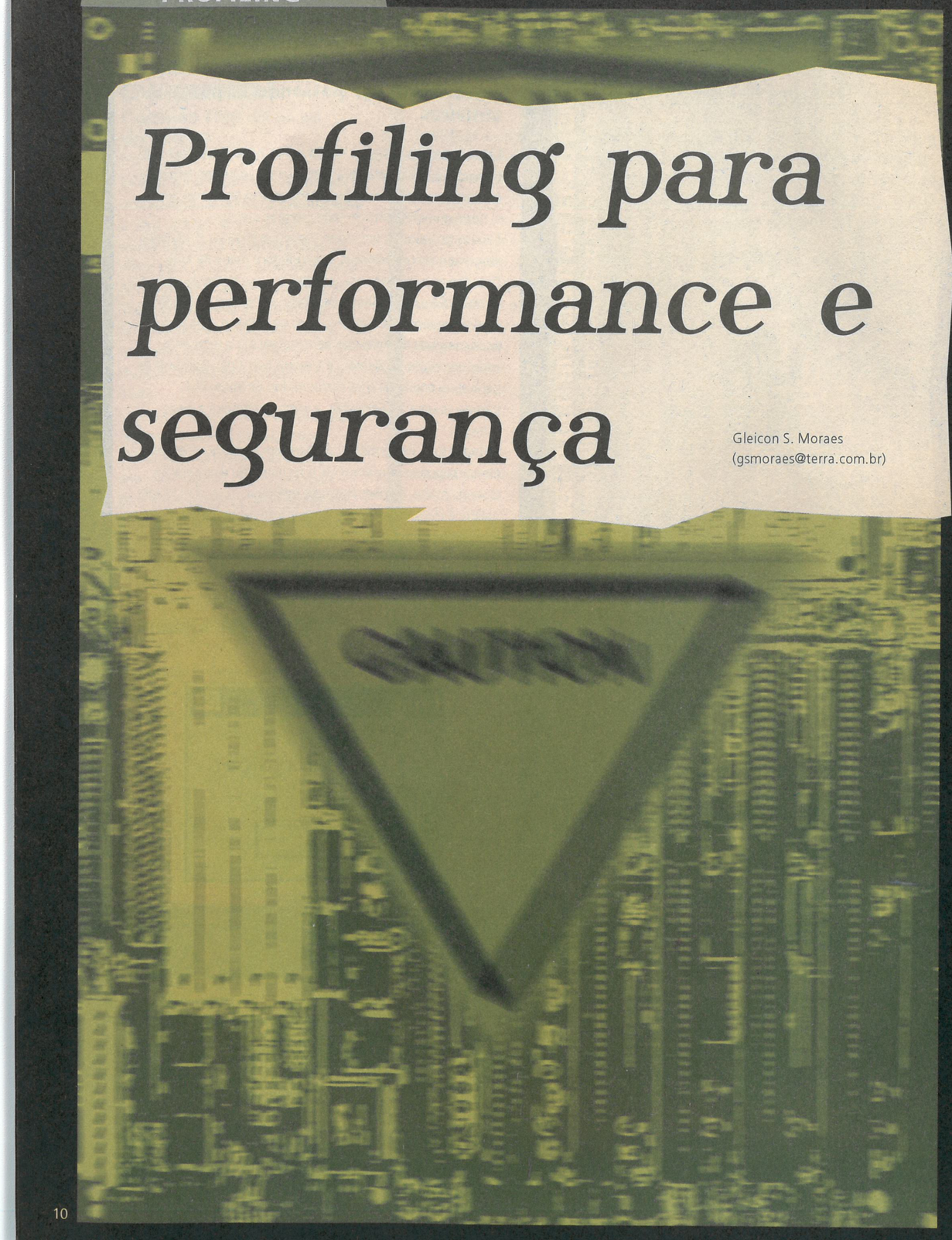
Spam é crime

Não use seu e-mail como uma arma: a vítima pode ser você

O Senado dos Estados Unidos aprovou uma lei que torna o spam ilegal. Os spammers, responsáveis por bilhões de mensagens comerciais, pornográficas e hoaxes, podem pegar até prisão e pagar multas milionárias.
Os senadores norte-americanos só agora entenderam algo que os usuários já perceberam há tempos: o spam atrapalha a vida de todos e desgasta a credibilidade da comunicação em rede.
Segundo pesquisa feita pelo instituto Pew Internet, um entre quatro entrevistados afirmou usar menos o e-mail por causa da quantidade de spams que recebe.

Profiling para performance e segurança

Gleicon S. Moraes
(gsmoraes@terra.com.br)



Mesmo com o poder de processamento de um simples PC, hoje em dia várias vezes superior às máquinas de 10 anos atrás, um desenvolvedor experiente se preocupa com a performance de seus produtos.

Esta preocupação é justificada, visto que, em um nível mais baixo, muito tempo pode ser perdido em rotinas montadas de forma errônea. Ou mesmo com alguns ajustes e modificações, uma boa velocidade pode ser alcançada.

O assunto é muito extenso e tema para livros dedicados a aspectos tão distintos quanto banco de dados, programação distribuída e outros tantos, mas é possível começar a conhecer este campo que, com a estabilização e a definição da área de informática, vai começar a ser cada vez mais exigido e necessário.

No começo, eram os programas simples criados para resolver um pequeno problema. E pelo menos quando falamos em ambientes Unix, muitos programas "duram" anos e anos, rodando sem problemas por um bom tempo.

Esse foi o tempo da criação e experimentação, em que muitos programas eram criados por pessoas sem experiência na área, que era relativamente nova. Com o tempo, essas pessoas adquiriram habilidades e mudaram seus estilos de resolver problemas (ou seja, programar). Alguns se direcionaram para outras áreas (portanto seus programas simples que estavam rodando por aí ficaram sem pai), e outros se dedicaram ao desenvolvimento.

Alguns desses profissionais se atreveram a mexer no que já funcionava para tentar melhorar, ou seja, economizar recursos de memória, velocidade, máquina, ou para implementar outro modo de resolver o mesmo problema.

Já as grandes corporações, têm seus produtos sendo utilizados por um enorme número de pessoas leigas (clientes que pagam pelos programas e exigem performance, qualidade e suporte). Mas após um certo ponto, quando uma aplicação está pronta, não sobra muito para o desenvolvedor criar para mudar o quadro existente.

Nas duas situações citadas, o caminho natural foi partir para uma área chamada, em inglês, de "profiling", ou seja, a medição de pontos da aplicação (partes, procedimentos, atividades), e para a análise dessas medições com a finalidade de determinar o que poderia ser mudado, reescrito ou retirado para o objetivo desejado, ou seja, a melhora da performance.

Claro que muito de profiling é feito em alto nível, ou na área de projetos, mas é uma prática interessante para aprender a identificar esses pontos e ter alguma experiência real com essas técnicas. Pode ser até com algum código que nós mesmos desenvolvemos.

Além do código, a análise pode ser feita diretamente na fonte por pessoas que já têm essa experiência, ou utilizando-se de algum pacote de profiling (programas que auxiliam nesta tarefa).

Antes de analisar programas mais complexos, vamos testar uma ferramenta bem simples de *profiling* presente na maioria das instalações: o comando **time**:

```
$ time /bin/ls

(...)
real    0m0.005s
user    0m0.000s
sys     0m0.000s
```

O comando time fornece o tempo de execução de um binário em três medidas de tempo: **real**, ou seja, o tempo total utilizado pela aplicação, desde a sua execução até o retorno ao shell; **user**, que é o tempo de CPU gasto pelo processo; e **sys**, o tempo gasto pelo sistema para ajeitar tudo em kernel mode, ou seja, carregar, mover o código e iniciar a execução. Como o programa que testei é bem simples (ls), os números são bem baixos.

Um programa simples para fazer testes e comparar alguns métodos de profiling e otimização é o que se segue:

programa 1 - matrizes.c

```
#include <stdio.h>
/* tamanho das matrizes */
#define SIZE    500

/* C = AB */

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

        double a[SIZE][SIZE], b[SIZE][SIZE],
c[SIZE][SIZE];
        double temp;
        int x, y, z;

        for (x = 0; x < SIZE; x++)
                for (y = 0; y < SIZE; y++) {
                        temp = 0.0;
                        for (z = 0; z < SIZE;
z++)       temp += a[x][z]*b[z][y];
                        c[x][y] = temp;
                }
}
```

Este programa implementa a multiplicação de duas matrizes em uma terceira e utiliza bastante memória e CPU. Digite e compile com:

```
cc matrizes.c -o matrizes1
cc matrizes.c -o matrizes2 -O3
```

Os dois binários resultantes vão representar uma situação utilizando o compilador sem nenhuma otimização e com otimização média.

O algoritmo utilizado é bem básico, sem otimizações em assembly, como em bibliotecas dedicadas a processamento 3D, em que essas funções encontram a necessidade de maior velocidade. Ao testarmos os dois binários digitando *time matrizes1* e *time matrizes2*, podemos ter uma boa idéia da diferença do emprego de otimizações e do uso do comando time para medir os tempos de execução, uma das funções mais rudimentares em profiling.

Um outro aplicativo geralmente presente nas instalações de Linux com ambiente de desenvolvimento é o gprof. O gprof fornece um relatório detalhado de chamadas para funções, tempos de execução e dados.

Para utilizá-lo, deve-se compilar o programa com a chave -pg, executar o binário e, em seguida, o gprof com a sintaxe: gprof *<binario>*. O relatório fornecido dá uma boa idéia dos trechos e chamadas que estão consumindo mais tempo no fluxo do programa.

Outra forma interessante é o código-fonte implementar timers, até mesmo utilizando a função *gettimeofday* e construindo seu próprio framework de profiling para cada chamada de função. Geralmente a função é chamada antes e depois de um ponto a ser analisado, e o tempo gasto é em microssegundos.

```
programa 2 - gettimeofday.c

#include <stdio.h>
#include <sys/time.h>

/* multiplica matrizes marcando o tempo que cada
elemento da matriz final consumiu */

/* tamanho das matrizes */

#define SIZE    10

/* C = AB */

double mygettime(void) {
        double temp;
        struct timeval tp;
        int rtn;
        rtn=gettimeofday(&tp, NULL);
        temp=(double)tp.tv_sec+(1.e-
6)*tp.tv_usec;
        return temp;
}

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

        double a[SIZE][SIZE], b[SIZE][SIZE],
c[SIZE][SIZE];
        double temp;
        int x, y, z;

        double t1,t2,elapsed;

        for (x = 0; x < SIZE; x++)
                for (y = 0; y < SIZE; y++) {
                        temp = 0.0;
                        t1=mygettime();
                        for (z = 0; z < SIZE; z++)
temp += a[x][z]*b[z][y];
                        c[x][y] = temp;

                        t2=mygettime();
                        elapsed=t2-t1;
                        fprintf(stderr,"c[%d][%d]
- tempo: %f segundos\n", x,y,elapsed);
                }
}
```

Compilando com *cc gettimeofday.c, -o gettimeofday* produz um binário sem otimização. Adicione a chave -O3 e, para cada uma, use o comando time para testar a performance e os números exibidos.

Para ter um exemplo do relatório fornecido pelo gprof, recompile o programa com *cc gettimeofday.c -o gettimeofday -pg,* execute o binário *gettimeofday* e, em seguida, execute o comando *gprof gettimeofday | less.* Acompanhe as informações fornecidas, inclusive o número de chamadas para a função *mygettime().*

Existem outros pacotes, como o cprof (*http://www.cprof.sf.net*) e alguns mais caros.

Muitas vezes, alguns loops estão mal projetados, contendo cálculos repetitivos ou chamadas a funções pesadas, tais como consultas a SQL ou alocação de memória, tornando-se pontos para o aparecimento dos chamados gargalos. Isso é muito comum em aplicações web, em que um loop desses pode resultar em um timeout, ou aquelas páginas que demoram um século para aparecer.

Para este tipo de problema, os testes de estresse de aplicação são indispensáveis. Desde programas de benchmark, como no caso citado, específico para webservers e cgi/scripts, até pequenos scripts feitos com finalidades específicas. A linguagem PERL é excelente para este tipo de construção, pois possibilita a criação de ferramentas de forma rápida e simples.

Geralmente um desenvolvedor cria um script em ASP ou PHP para a Web, e testa em rede local (no máximo pede para um amigo testar), e quando colocado em ambiente de produção, falha miseravelmente, sobrecarrega a máquina e acaba com os recursos reservados para os outros processos que estavam funcionando.

Nesses casos, não somente o profiling da aplicação é interessante, mas de todo o ambiente. Um erro muito comum, além das queries de SQL dentro de loops enormes, são tabelas mal projetadas, sem índices ou com índices incorretos. Nem sempre dá para seguir os livros de banco de dados, ainda mais em setups mais simples, portanto cabe ao desenvolvedor modelar seu banco de acordo com o que tem à mão.

Falando em SQL, as queries e stored procedures devem ser examinadas também para analisar outras formas de realizar a mesma tarefa e evitar aqueles bugs relacionados com caracteres especiais, do tipo aspas, apóstrofres e caracteres que representam comentários dentro da query. Esses bugs são os responsáveis pela maioria das "invasões" a servidores, pois abrem uma porta direta ao coração do sistema.

Claro que a filtragem de caracteres especiais deve vir do programa, e geralmente não é isso o que acontece, pois a checagem dos parâmetros não é realizada.

Portanto, o profiling de uma aplicação é importante também sob o ponto de vista de segurança. Muitos bugs de programação, que no resultado final se apresentam como grandes falhas de segurança, têm seu início em códigos mal pensados ou avaliados.

Um exemplo clássico são os bugs relacionados a *format strings*, que assolaram e ainda acontecem em muitos programas. Como no caso do desenvolvedor que resolveu um problema com um código, mas não voltou mais a trabalhar com ele para evoluir.

Esta classe de bugs é relativamente nova, não que a existência seja recente, mas há relativamente pouco tempo que começaram a ser explorados. Justamente naqueles softwares mais antigos, que estão rodando há muito tempo, sem a preocupação com técnicas de programação que levam em conta práticas de construção de código seguro. Em comparação com os overflows existentes, que já são conhecidos e explorados há muito tempo, esta classe de bugs aparece em locais diversos.

Um dos softwares que mais sofreu com isso foi o wu-ftpd, até então vítima de alguns overflows, mas que foi muito desacreditado pela quantidade de bugs existentes relacionados a format strings.

Apenas para relembrar, um *overflow*, seja de buffer, ou heap, stack, tem como princípio um código que foi criado e não checa os limites de suas variáveis, permitindo assim que seja injetado um código malicioso no seu espaço na memória, e executado com a permissão do programa rodando. Muitos deles são locais ou remotos, ou seja, podem ser efetivos via Internet/Rede local.

Uma forma de bug desses é o uso de funções sem a checagem do tamanho do buffer de destino, tais como *strcat, strcpy, sprintf*. Para cada buffer do programa, é necessário levar em conta seu tamanho, mesmo que em todas as situações normais este valor nunca seja superado. São nas situações não pensadas que os exploits atuam.

Um bug de *format string* aparece em um caso como o descrito abaixo, por exemplo:

```
printf(mystring);
```

Quando o correto seria:

```
printf("%s", mystring");
```

Este é apenas um pequeno exemplo, mas que demonstra a falta de cuidado na criação do código. Com isso, pode-se derrubar o processo ou até utilizar esta janela para inserir um código a ser executado, usado como um buffer overflow.

As boas práticas de programação são adquiridas conforme a experiência, mas utilizar, ou mesmo desenvolver seus métodos de profiling, é um dos meios mais rápidos de ter resultados positivos neste campo.

Para um software livre, esses conceitos são mais importantes, pois não trabalham com segurança baseada em segredos. Seu código-fonte está na Internet, sendo testado, abusado e utilizado por muitas pessoas e organizações. Por isso temos mais agilidade neste campo do que em produtores de software fechado. Com o desenvolvimento distribuído e tantos interesses, geralmente leva uma questão de horas para que uma correção seja postada na Internet.

Com software fechado, temos situações como a da Microsoft e os bugs recentes de RPC/DCOM, em que mesmo com os patches fornecidos, a vulnerabilidade persiste ou é localizada em outro local.

O quadro parece simplista, mas não é uma defesa de um sistema ou de outro, mas apenas uma demonstração de como o profiling feito de maneira correta e por indivíduos ou grupos interessados surte efeitos às vezes surpreendentes.

Negação de Serviço: Implementação, Defesas e Repercussões

Toniclay Andrade Nogueira
toniclay@globo.com
Othon Marcelo Nunes Batista
othonb@yahoo.com

Abstract: this paper describes a study about denial of service and distributed denial of service, in which are presented aspects related to the atacks themselves and their concepts, defenses, implementations, their types, functioning and their repercurssions. Beyond that, it was done a study about the tools TFN and TRIN00, ones of the most utilized in this area. By this way, it'll be shown the importance of prevention of these atacks.
Keywords: denial of service, distributed denial of service, security, computer networks.

Resumo: este artigo descreve um estudo sobre negação de serviço e negação de serviço distribuída, no qual são apresentados os aspectos relacionados ao ataque de negação de serviço e seus conceitos, defesas, implementação, seus tipos, funcionamento e suas repercussões. Além disso, é feito um estudo sobre as ferramentas TFN e TRI00, duas das mais utilizadas em ataque nessa área. Dessa forma, será mostrada a importância da prevenção desses ataques.
Palavras-Chave: negação de serviço, negação de serviço distribuída, segurança, redes de computadores.

1. Introdução

Desde o surgimento da Internet, a segurança da informação tem sido um assunto constante. A partir do momento em que cada empresa se conecta à rede mundial, seus dados ficam expostos. Esse crescimento da quantidade de informações disponíveis, naturalmente aumentou o interesse das pessoas com relação à segurança de redes. Muitas formas de invasão surgiram e muitas maneiras de defesa também foram elaboradas, com a finalidade de garantir que os dados da empresa permanecessem em segurança. Esse estudo mostrará como surgiu a negação de serviço, asim com sua definição , seus tipos de ataque, como funciona , além de exibir suas implementações (TRI00 e TFN). Também veremos técnicas de defesa e explicaremos as repercussões causadas por um ataque de negação de serviço em uma empresa.

2. Negação de Serviço

2.1 Como Surgiu a Negação de Serviço

Em 1988, houve a primeira detecção de ataque DoS. Em setembro de 1996, o Provedor *Public Access Network Corporation* (PANIX) ficou cerca de uma semana sob o efeito do ataque. Em maio de 1999, uma série de ataques DoS atingiu as redes do *Federal Bearout of Investigation* (FBI) e de vários outros órgãos governamentais norte-americanos.
Segundo [1], no Brasil nenhum site assumiu publicamente ter sofrido um ataque DoS, mas existem sinais de que alguns grandes portais tenham sido atingidos.

3. Definição de Negação de Serviço

Segundo a definição de [2], Negação de Serviço (DoS) é um ataque que permite que uma pessoa deixe um sistema inutilizável ou consideravelmente lento para os usuários legítimos por meio do consumo de seus recursos, de maneira que ninguém consegue utilizá-los.

4. Definição de Negação de Serviço Distribuída

A Negação de serviço distribuída (DDoS) utiliza-se do conceito de computação distribuída para efetuar os ataques. O atacante invade e se apropria de diversos computadores para executar o ataque a partir de diferentes origens simultaneamente.

5. Ataques Locais

O DoS Local é um ataque de negação de serviço que, para poder ser executado, é necessário estar logado ao sistema. Outro método antigo é o ataque a disco, que simplesmente lota o HD do sistema com dados espúrios.

6. Ataques Remotos

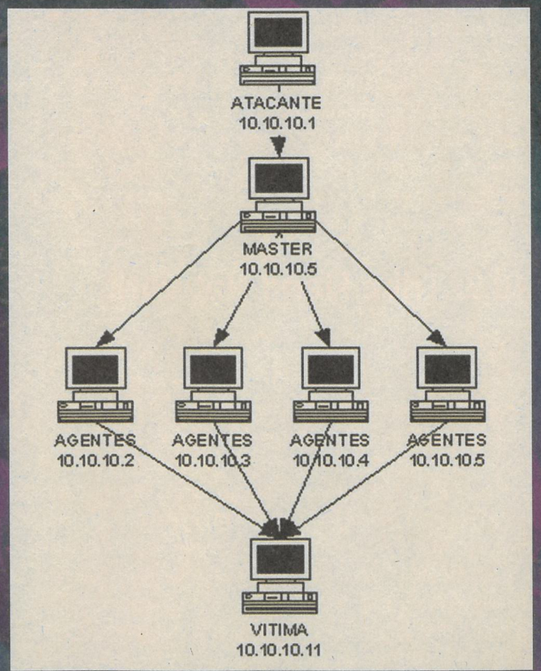
Os ataque DoS remoto pode ser executado sem estar logado ao sistema DoS Remoto Multiprotocolar, que consiste em ataques que funcionam independente do sistema operacional, por causa de falhas em diversos protocolos ou de força-bruta. Neste caso, o atacante envia para a rede um número de pacotes superior ao limite que o destino é capaz de absorver.

7. Funcionamento de um Ataque DDoS

Os ataques de Negação de Serviço Distribuído (DDoS) podem ser classificados pelo nível de automação, pela vulnerabilidade explorada, pela dinâmica e pelo impacto causado. Segundo a vulnerabilidade explorada, existem dois tipos de ataques DDoS: os ataques aos protocolos e os ataques de força-bruta.

8. Topologia

A topologia de uma rede DDoS é dividida em quatro partes. Os sistemas comprometidos são divididos em mestres e agentes. Os agentes geram o tráfego que irá resultar na negação de serviço e são controlados por um ou mais mestres. A utilização de duas camadas (mestres e agentes) entre o atacante e a vítima dificulta o rastreamento.



Topologia de uma rede DDoS.

9. A Criação de uma Rede DDoS

Antes de efetuar um ataque DDoS, uma rede deve ser montada. Computadores devem ser identificados como possíveis vítimas a fim de ganhar acesso administrativo ao maior número de sistemas possíveis. Esses computadores devem pertencer a diversas redes ou endereços IP. A utilização de uma grande quantidade de endereços IP dificulta a identificação e o bloqueio do ataque.

10. Implementações de Negação de Serviço

10.1. Trin00

O Trin00 utiliza os protocolos TCP e UDP para se comunicar com o servidor, o que torna necessária a utilização de portas e faz com que a troca de mensagens seja mais facilmente percebida. Os agentes Trin00 podem ser instalados em sistemas Linux e Solaris.
A utilização do Trin00 pode ser detectada pela observação de tráfego UDP tipo 17, que é utilizado para a comunicação entre os mestres e os agentes. Os mestres mantêm uma lista dos agentes que poderão ser contatados.
As portas utilizadas pelo Trin00 podem ser usadas para a detecção e mesmo para o bloqueio, impedindo que os computadores da rede sejam utilizados para os ataques.
Uma vez executado o agente Trin00, ele anuncia a sua disponibilidade pelo envio de um pacote UDP contendo a *string* "*HELLO*" para o endereço IP de seu respectivo mestre. O mestre responde com outro pacote UDP, desta vez com a *string* "PONG".

10.2. Tribe Flood Network

Esta foi a primeira ferramenta de ataque DDoS disponível publicamente. O TFN foi escrito por Mixter. Os ataques efetuados pelo TFN são: UDP *Flooding*, TCP SYN *Flooding*, ICMP *Flooding* e Smurf. O controle dos mestres é feito por linha de comando, e a execução do programa deve ser acompanhada dos parâmetros desejados com a sintaxe: *tfn <iplist> <type> [ip] [port]*, onde *<iplist>* é a lista dos agentes que podem ser utilizados, *<type>* é o tipo de ataque desejado, *[ip]* é o endereço da vítima e *[port]* é a porta desejada para ataques TCP SYN *flooding*, que pode ser definida como um número aleatório (parâmetro 0).
O TFN é bastante "discreto". A comunicação entre os mestres e os agentes é feita por mensagens ICMP tipo 0, o que torna difícil o monitoramento dessas comunicações, pois muitas ferramentas de monitoramento não analisam o campo de dados de mensagens ICMP.

11. Como Se Defender da Negação de Serviço

Em razão da arquitetura e força do DoS/DDoS, não existe uma maneira totalmente eficaz de evitar o ataque. Uma solução ideal seria que todos os computadores fossem configurados e protegidos de maneira a não serem utilizados para a formação da rede DDoS. Apesar de não haver uma solução definitiva contra ataques DDoS, existem várias maneiras de minimizá-los, como um plano de contingência que é a melhor solução contra ataques do tipo força-bruta, que consomem todos os recursos da rede por terem origem em redes mais numerosas ou com mais recursos. Trata-se de uma política de segurança para garantir que todos seus usuários legítimos não sejam eventuais colaboradores de possíveis ataques. Para evitar que senhas possam ser facilmente descobertas, é fundamental que elas tenham um tamanho mínimo adequado, e sejam trocadas com freqüência. O acesso físico deve garantir que o sistema apenas seja alcançado pelos seus administradores autorizados. Além disso, as atualizações dos sistemas devem ser constantes. Quanto à detecção e prevenção de vírus, é necessário possuir programas antivírus instalados e atualizados e as portas de comunicação devem ser só aquelas que realmente precisar. Em relação à largura de banda, deve ser estipulado um limite por serviço. Deve haver a desativação da difusão para poder impedir que a rede seja usada como amplificadora para ataques e o tráfego deve ser analisado com cuidado. A real necessidade da utilização de Ping em endereços de *broadcast*, o bloqueio de endereços da Internet, caso aconteça um ataque e possuir um sistema de detecção de intrusos antes de implantar a segurança da rede. [3]Deve-se verificar se a rede não está comprometida e, por fim, possuir um plano de reação.

12. Ferramentas de Detecção de Negação de Serviço

O Zombie Zapper serve para bloquear um ataque em andamento. Caso o IDS indique que a rede está sendo utilizada como plataforma de ataque, o Zombie Zapper funciona enviando comandos para os agentes interromperem o ataque.
Find_ddos é a ferramenta que foi desenvolvida por um órgão do FBI em função da grande quantidade de ataques DDoS ocorridos. O find_ddos localiza no sistema os Masters e Agentes das ferramentas Trin00, Tribe Flood Network, TFN2k e Stacheldraht.
O DDoS Ping é um programa desenvolvido por Robin Keir. Ele possui interface gráfica, tornando mais acessível e fácil a sua utilização edetecta Agentes Trin00, Tribe Flood Network e Stacheldraht. O rastreamento é feito pelo envio de datagramas e mensagens UDP e ICMP para uma relação de endereços IP definidos pelo usuário.

13. Repercussões

Algumas repercussões causadas por ataques DoS/Ddos foram relatadas na imprensa em modo geral, como foi o caso do site da Alldas[5], o da RIAA[6], o da SCO e o da Al Jazira[7]. Isso mostra que os ataque DoS e DDoS geram prejuízos de formas incalculáveis, tanto na parte financeira como na parte das informações.

14. Conclusão

O DoS e DDoS tornaram-se uma grande ameaça a partir do momento em que as ferramentas para sua execução fica ram disponíveis na grande Rede de computadores. Hoje, devido ao grande número de ferramentas disponíveis, um ataque DoS/DDoS de grandes proporções pode ser realizado sem muitas dificuldades, mesmo por pessoas que não tenham conhecimento técnico de como estas ferramentas funcionam num ataque.
Os ataques aos protocolos podem ser evitados pelo conserto das vulnerabilidades depois de sua descoberta. Por outro lado, os ataques do tipo força-bruta não podem ser evitados facilmente, principalmente por precisarem ser impedidos na sua origem. A ameaça de um ataque DDoS é impossível de ser eliminada, pois se um equipamento estiver conectado,sempre há a possibilidade de receber dados em quantidade acima do limite suportado.
Atualmente, por causa Internet, não existe a possibilidade de garantir a segurança total de qualquer dispositivo conectado à Rede. Existem várias formas de minimizar a possibilidade de um DDoS, mas nenhuma é infalível. Se o atacante possuir tempo e recursos disponíveis, o ataque inevitavelmente será bem-sucedido.
Uma solução alternativa seria um desenvolvimento de sistemas de segurança a serem implementados em pontos-chave da grande Rede de computadores com a finalidade de interromper os ataques em suas origens [4]. A partir do monitoramento dos principais roteadores da Internet, qualquer ameaça DDoS teria imediatamente o seu tráfego reduzido ou mesmo bloqueado. Após o ataque, o tráfego voltaria a ser liberado aos poucos, de maneira a não causar inundação em seus destinos.
Os recentes ataques mostram que não apenas as empresas, mas toda a infra-estrutura da Internet está vulnerável. Por isso é fundamental que o DDoS continue a ser estudado a fim de garantir a segurança da Internet.

Referências

[1] MAIA, Luiz Paulo. Analisando Ataques do Tipo Distributed Denial of Service — DDoS. Developers Magazine. Rio de Janeiro, n. 54, p. 26–27, Mar. 2003.
[2] STEIN, L. & STEWART, J. Securing Against Denial of Service Attacks. Disponível em: <http://www.w3.org/Security/Faq/wwwsf6.html>. Acesso em 16 de Abril de 2003.
[3] MIRKOVIC, J. D-WARD: DDoS Network Attack Recognition and Defense. PhD Dissertation Prospectus. Los Angeles: University of California, 2002.
[4] TORRES, G. *Redes de Computadores*. Rio de Janeiro: Axcel Books, 2001.
[5] ALLDAS. Ataques DDoS. Disponível em: <http://www.terra.com.br/informatica/2001/07/16/003.htm>. Acesso em 10 de maio de 2003.
[6] RIA. Ria Recebe Ataque de Negação de Serviço. Disponível em: <http://www.terra.com.br/cgi-bin/AT-Informaticasearch.egi>. Acesso em 10 de maio de 2003.
[7] Terra. Site da Al-Jazira em Inglês é Atacado e Sai do Ar. Disponível em: <http://www.terra.com.br/informatica/2003/03/25/012.htm>. Acesso em 11 de maio de 2003.

Por Antônio Marcelo
amarcelo@plebe.com.br

NTOP 2

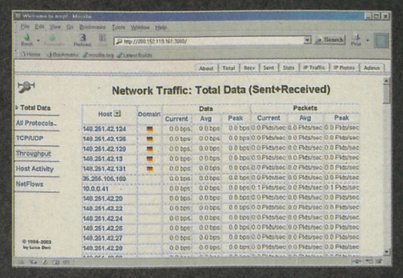
Uma Ferramenta de Gerência de Tráfego de Redes

Introdução:

Recentemente, tive uma experiência nada agradável com usuários de um grande cliente meu. A empresa tinha feito uma recente mudança de seu CPD e aguardava um upgrade de link. A rede suportava uma VPN interligando a sede no Rio com filiais em São Paulo, Minas Gerais e no estado do Rio de Janeiro, além da Internet e um serviço de mensagens baseado em Jabber.

Era de se esperar que a performance não fosse lá grandes coisas, já que o link era apenas de 256 Kb. Contudo, três semanas após as mudanças, verificou-se uma perda de performance assustadora, que em alguns momentos causava paralisia de diversos serviços on-line. Estudos feitos com o tradicional Iptraf, do Linux apontaram diversos usuários utilizando serviços de P2P, chat e ICQ. Logo, foi adotada uma política de bloqueio, que ajudou em muito o link, mas os problemas ainda continuavam e era necessária uma ferramenta que fosse mais informativa e que pudesse ser consultada a qualquer momento via Web.

A solução foi o NTOP (Network Traffic Probe), um programa que pode ser utilizado em plataformas livres, como o Linux e o BSD, e proprietárias, como o Windows. Trata-se de uma excelente ferramenta, capaz de obter diversas informações interessantes sobre uma rede. O software é tão bom que a própria Cyclades já está querendo colocá-lo em seus roteadores.



Um exemplo de leitura do NTOP

Obtendo e Configurando o NTOP:

Inicialmente, a plataforma que escolhemos foi um firewall montado em Linux com duas placas de rede, conforme o esquema ao lado:

O objetivo era estudar o tráfego da rede e, assim, detectar pontos importantes e gargalos proporcionados por usuários que utilizavam a rede de maneira não autorizada. Em seguida, o NTOP foi baixado do site http://www.ntop.org, e o arquivo foi descompactado em um diretório conforme o seguinte comando:

```
tar-xzvf  ntop-2.2.tar.gz
```

Em seguida acesse o diretório descompactado

```
cd /ntop-2.2
```

Temos agora um ponto importante aqui, não abordado no site da NTOP: as bibliotecas de função. São criados dois diretórios:

a) gdchart0.94c – diretório que contém a biblioteca gdchart para a criação dos gráficos no NTOP. Esse diretório é composto pela seguinte árvore:

zlib-1.1.4 – Biblioteca zlib. Você precisa instalá-la antes. Para isso, entre no diretório e digite:

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

gd-1.8.3 – Bibliotca gd. Esta é que dá mais trabalho na instalação. Dentro de seu diretório, você encontrará os seguintes subdiretórios:

libpng-1.2.4 – Este diretório é da libpng, responsável pela criação de figuras. Dentro dele, existe um subdiretório chamado scripts para o makefile de instalação de cada sistema operacional. Um deles é para o Linux. Digite o comando abaixo:

```
cp scripts/makefile.linux makefile
```

e depois :

```
make
make install
```

Depois da libpng instalada, volte ao diretório do gd-1.8.3 e digite:

```
make
make install
```

Voltando ao diretório do gdchart, depois da zlib e da gd-1.8 instaladas, finalmente digite:

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

Vamos agora instalar o NTOP. Volte para o diretório ntop e, dentro dele, digite:

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

Pronto. A instalação está finalizada

Rodando o NTOP pela primeira vez:

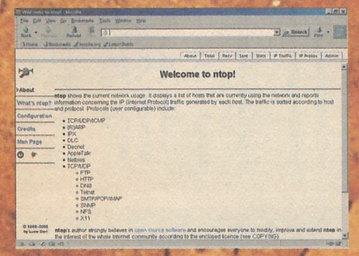
Execute o NTOP com o seguinte comando:

```
/usr/bin/ntop -P /tmp -u nobody -A
```

A opção -P indica onde iremos guardar o banco de dados das informações temporárias daquela seção. A -u indica o usuário que irá executar o ntop; o -A pede uma senha para o administrador, a qual você deverá digitar quando for pedida. Se tudo correu de acordo, vá para seu navegador e digite:

```
http://localhost:3000
```

Surgirá a seguinte tela:



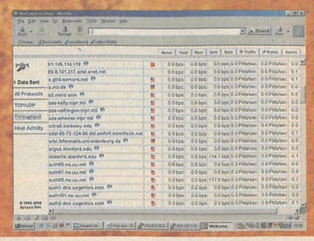
O NTOP roda normalmente na porta 3000, e esta é a sua tela de entrada quando ele está em operação. Podemos ver acima opções importantes como: Total, Recv, Sent, Stats, IP Traffic, IP Protos, Admin. Vamos ver um exemplo na prática de sua utilização.

Alguns Pontos Práticos:

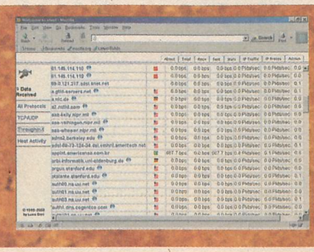
O NTOP tem quatro menus importantes:

Recv – Indica os pacotes recebidos pelo host (Data Received)
Sent – Indica os pacotes enviados (Data Sent)
Statistics – Mostra as estatísticas da utlização da rede
IPTraffic – Mostra o tráfego de entrada e saída da rede

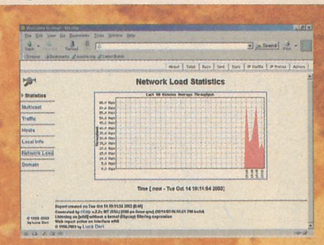
Vamos observar o seguinte: o troughput de dados enviados para for, aparentemente está com atividade baixa.



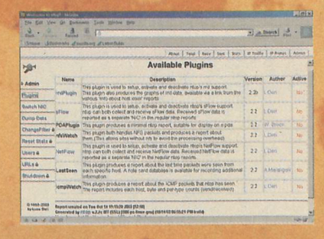
Outro ponto que podemos analisar são os pacotes recebidos:



Agora o mais interessante é visualizarmos a carga de rede nas estatísticas:



O NTOP possui ainda muito mais características interessantes. Explore-o e você descobrirá muitas informações úteis. O software conta ainda com um módulo de administração e de gerenciamento de plug-ins, que vale a pena você dar uma olhada.



Colocando o NTOP em produção:

Para finalizar o nosso artigo, queremos exemplificar uma instalação que hoje está em produção para que nossos leitores possam repetir em seus ambientes de teste. Inicialmente foi instalado o NTOP no firewall Linux e foram alterados os seguintes arquivos:

```
/etc/rc.d/rc.local - Foi acrescentada a seguinte linha de comando:

/usr/bin/ntop -P /tmp -i eth0 &
```

No caso, a interface que queríamos escutar somente era a eth0.

No script de firewall, foram acrescentadas as seguintes linhas:

```
#NTOP - Só acessa as máquinas escolhidas pelo admin de rede.
iptables -A INPUT -p tcp -s 0.0.0.0/0 –dport 3000 -j DROP
iptables -A INPUT -p tcp -s IPMAQUINA1 –dport 3000 -j ACCEPT
iptables -A INPUT -p tcp -s IPMAQUINA2 –dport 3000 -j ACCEPT
iptables -A INPUT -p tcp -s 127.0.0.1 –dport 3000 -j ACCEPT
iptables -A INPUT -p tcp -s IPDAMAQUINADONTOP –dport 3000 -j ACCEPT
```

O parâmetro IPMAQUINAX é o endereço IP das máquinas internas do administrador. Liberamos também o loopback e o próprio endereço IP da interface eth0 (IPDAMAQUINADONTOP). Lembrando que a porta 3000 é bloqueada por padrão.

Finalizando :

O NTOP é uma resposta do software livre às ferramentas de gerenciamento de rede. Além de ser poderosa, é excelente para as atividades do dia-a-dia, principalmente em máquinas que agem como firewalls ou bridges de redes. A versão Linux é muito poderosa e está em regime GPL, podendo ser baixada e instalada à vontade. A Windows é paga. Lembramos que, para os administradores de rede, é fundamental ter uma ferramenta dessas em seu cotidiano.

Tutorial de Linux - Lição 4 - Arrays

Introdução :

Olá, pessoal! Cá estamos nós com nossa lição 4 de nosso tutorial. No último artigo, vimos um tópico essencial a respeito de funções. Vimos que elas são importantes e que podem ser utilizadas em diversos exemplos e programas. Agora vamos começar a explorar uma área do C, que é o início da exploração das rotinas que trabalham com a memória: os arrays.
Os arrays são posições locais da memória agrupadas, pois possuem o mesmo nome e o mesmo tipo. São entidades estáticas, já que suas características (como tamanho, por exemplo) não são alteradas durante a execução de um programa.

Os arrays ocupam espaços na memória, ou seja, o programador irá reservar quantas posições forem necessárias. Por exemplo, se quiséssemos reservar 10 posições para um array, declararíamos o seguinte :

```
int valores[10];
```

Ou seja, reservamos dez posições para a variável "valores". O mesmo pode ser feito para variáveis do tipo "char". Veja o exemplo abaixo:

```
char dias[] = 'segunda', 'terça',
'quarta', 'quinta', 'sexta',
'sábado', 'domingo';
```

Logo, o valor dias[2] será igual à terça. Um outro ponto importante é que podemos limitar a entrada de caracteres de um array do tipo char. Se quiséssemos colocar no máximo 30 caracteres numa variável chamada "nome, faríamos da seguinte forma:

```
char nome[30];
```

No máximo poderíamos digitar 30 caracteres. Veja nosso primeiro exemplo simples:

```
#include <stdio.h>

main()
  char nome[30];
  printf("Entre com seu nome :
");
  scanf("%s", nome);
  printf("nome e %s: ",nome);
  return 0;
```

Eis um programa que lê uma variável de teclado e joga em um array. Manipulando os arrays:
Vamos ver outro exemplo interessante com arrays de caracteres:

```
#include <stdio.h>

main()
char vogal[] = 'a', 'e', 'i',
'o', 'u';
int i;
printf("Entre com numero da
vogal : ");
scanf("%d",&i);
printf("A vogal e
%c",vogal[i]);
return 0;
```

Rode o programa e digite um número. Algo estranho aconteceu, não? Quando você digitou 1, apareceu a letra e, e não a letra a, por que será? Para um array, o primeiro elemento é sempre o 0, logo o valor de da letra a é o vogal[0] ! o vogal[1] seria a letra e. Vamos agora brincar um pouco mais com um programa que recebe a nota de quatro alunos e calcula a média da turma:

```
#include <stdio.h>

float notas[4];
float total;
float media;

main()

    notas[0] = 3.4;
    notas[1] = 7.5;
    notas[2] = 8.2;
    notas[3] = 7.6;

    total = notas[0] + notas[1] +
notas[2] + notas[3];
    media =  total / 5.0;
    printf("Total %f Media %f",
total, media);
    return (0);
```

No caso, utilizamos a variável do tipo float para os números decimais. O programa abaixo é um dos típicos programas que fazemos na faculdade. Ele lê uma cadeia de trinta caracteres (texto[30]) e os inverte.

```
#include <stdio.h>

char capturado;
char texto[30];
int i = 0;

main()

      printf("Digite a linha do
texto:  ");

       while(capturado != '')

         scanf("%c",&capturado);
         texto[i++] = capturado;

       for (i=i-1; i >= 0; i--)
       printf("%c", texto[i]);

       printf("");
       return(0);
```

Arrays Bidimensionais/ Multidimensionais

Temos em C a possibilidade de declarar arrays de mais de uma dimensão, ou seja, um array pode ser escrito da seguinte maneira:

```
Array bidimensional - int matriz
[3] [3]
Array Multidimensional - int
matriz [3] [5]
```

E assim sucessivamente. Você já deve ter reparado que propositalmente colocamos uma variável com o nome de matriz, já que esta é uma das várias aplicações de arrays. Vamos mostrar um simples programa que recebe dados e os transforma em uma matriz:

```
#include<stdio.h>

#define LINHAS 2
#define COLUNAS 3

main()
     int i, j;
     int matriz[LINHAS][COLUNAS];
     printf("Entre com os elemen-
tos da Matriz : ");
     for (i=0; i<LINHAS; i++)
          for (j=0; j<COLUNAS;
j++)
               scanf("%d",
&matriz[i][j]);

     for (i=0; i<LINHAS; i++)
          for (j=0; j<COLUNAS;
j++)
               printf("%4d",
matriz[i][j]);
               printf("");

     return 0;
```

Este programa mostra como podemos montar um array multidimensional e, assim, termos matrizes e diversos elementos interessantes. Vejamos um outro exemplo muito bom, agora com um array bidimensional de caracteres:
Este exemplo retorna o dia da semana, lembarndo que o primeiro elemento do array sempre é o zero. logo, segunda-feira é o dia[0].

```
#include <stdio.h>

main()

    char dia[][20] =
"segunda","terça","quarta",
"quinta","sexta","sábado","domingo";
    int i;

    printf("Qual o dia ? ");
scanf("%d", &i);
    printf("%s",dia[i]);
```

Cuidados com os Arrays

Finalizando a nossa aula, queríamos falar de um problema em que os programadores nunca prestam atenção, ou seja, o maldimensionamento de arrays. Quando declaramos um array, reservamos espaços na memória. veja o seguinte esquema:

```
char nome [5] = "Vania" ;
```

Endereço Memória	*Valor do Array*	*Caracter*
00001h	*nome[0]*	*V*
00002	*nome[1]*	*a*
00003h	*nome[2]*	*n*
00004h	*nome[3]*	*i*
00005h	*Nome[4]*	*a*

Com este esquema, dizemos que a variável "nome" pode ter no máximo cinco caracteres. Mas o que aconteceria se de repente colocássemos sete caracteres ?
Acontece o chamado Segmentation Fault, que é definido como uma falha de segmentação que pode ocorrer em qualquer programa. Isso acontece se o programa tem um bug e/ou foi mal programado. Em nosso caso, o programa precisava ler parte da memória que não foi devidamente inicializada, ou que não pertencia a ele. Normalmente, o sinal SISEGV, pára a execução do programa. Veja como ficaria com seis caracteres:

```
char nome [5] = "Pliscka ;
```

Endereço Memória	*Valor do Array*	*Caracter*
00001h	nome[0]	P
00002h	nome[1]	l
00003h	nome[2]	i
00004h	nome[3]	s
00005h	Nome[4]	c
00006h	Não	k
00007h	Reservado	a

Aí teríamos um SEGFAULT, ou seja, nosso programador dimensionou mal a sua área de memória para a variável e assim teríamos um erro. O mais perigoso problema advindo de falhas como esta é o temido Buffer Overflows. Todos os programas que manipulam variáveis necessitam de buffers, que são áreas da memória onde são armazenados dados que estas mesmas variáveis recebem. Esta área normalmente é limitada e, quando em um determinado momento há um estouro por um excesso de informações, ocorre o Buffer Overflow, ou estouro do buffer. Este problema é responsável pelos principais exploits, programas que exploram vulnerabilidades, podendo causar assim a invasão de sistemas. Mas isso, pessoal, é papo para um curso de segurança. Vamos ensinar mais à frente como fazer um código tolerante a falhas.

Desafios:

No final de toda lição, eu proponho um desafio. Nesta vamos pedir o seguinte:

a) Faça um programa em C que retorne o mês do ano
b) Faça um programa em C que some duas matrizes 2 x 2
c) Faça um programa em C que multiplique duas matrizes 2 x 2

Bom Divertimento!

Conclusões:

Bem, esta lição é preparatória para um dos tópicos mais polêmicos e complexos do C: os ponteiros. Na nossa próxima lição, começaremos a manipular ponteiros com todo a sua potencialidade. Até lá! programem!

Antonio Marcelo é especialista de segurança e autor de diversos livros no Brasil de 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 orgãos governamentais do Brasil. Além de ser um pesquisador independente, é também CEO da Gurgel e Fonseca Consultores Associados, empresa brasileira de conectividade e segurança. Atualmente também é idealizador e mantenedor do projeto Honeypot-BR (http://www.honeypot.com.br). Pode ser encontrado no endereço: http://www.plebe.com.br. Para Dúvidas e críticas sobre este artigo, escrevam para amarcelo@plebe.com.br.

Por Piter PUNK

Slackpkg: histórico e funcionamento

1. História

Pessoa: – O ruim do Slackware é que tem que recompilar um monte de coisa quando sai um exploit em algum programa.
Eu: – Hein? É só baixar o patch no /patches, não tem segredo.
Pessoa: – Mas é muito complicado!
Eu: – Como complicado? Envolve três passos: 1) olhar o ChangeLog, 2) baixar o pacote e 3) instalar o pacote! Não tem segredo nenhum!
Pessoa: – Ah, mas com a ferramenta xyz da distro abcd dá para fazer automático...
Eu: – Bah! Fazer algo para baixar pacotes e instalar é coisa para um script de 15 minutos!
Pessoa: – Sei...

Para adquirir o SlackPKG acesse: http://slackpkg.sourceforge.net/

E foi assim que começou o slackpkg. Para falar a verdade, demorou mais de 15 minutos, mas no fim da tarde já estava mostrando a ferramenta para alguns amigos (e para a Pessoa). No dia seguinte, lancei a primeira versão no SourceForge.

O slackpkg foi criado com uma finalidade bem específica: baixar os patches de segurança do Slackware e facilitar a vida dos preguiçosos. Mas enquanto estava programando, foram surgindo novas idéias, como possibilitar a instalação de pacotes novos e remover os já instalados. Foi lançado, assim, o primeiro release com essas funções (que na minha opinião deveria se chamar 1.0, já que fazia tudo que eu queria).

Depois do pacote pronto e lançado, começaram a vir as sugestões dos usuários e, além das sugestões, os patches e bug reports. Isso mostra algo bem interessante: da mesma maneira que vários outros projetos, o slackpkg começou de um esforço individual, e, depois que já havia um release utilizável, a comunidade começou a contribuir. Normalmente essa é uma fórmula vitoriosa, enquanto que os projetos que começam pela página/lista de discussão/fórum e só depois são concretizados normalmente caem no limbo.

Ainda hoje, 90% do código é escrito e mantido pelo main developer, ou seja, eu. Poucas pessoas que utilizam o slackpkg fazem alguma alteração no código dele, e menos ainda enviam o código alterado para mim.

Isso tem um lado bom, pois ler o código que enviam, verificar o que é útil e qual a melhor maneira de incluí-lo dentro do slackpkg é extremamente trabalhoso. Algumas vezes as idéias são boas e o código não, por isso eu acabo tendo que reescrever o código para inserir no slackpkg. Outras vezes, o código é ótimo e a idéia é não é tão boa, e por aí vai... Muitas idéias e códigos bons ficam de fora pela própria filosofia do slackpkg, que é se manter simples. Algumas estruturas de programação são extremamente criptográficas e tentamos manter o código do slackpkg inteligível.

Se você pretende iniciar um projeto de software livre, lembre que ele vai ser "seu" filho e provavelmente você será o principal desenvolvedor por um bom tempo. Se é isso que você gosta – programar, pensar em features, corrigir, melhorar, etc. –, então estará no céu.

Atualmente, o slackpkg está incluso no Slackware 9.1 (diretório /extra), e tenho recebido mais contribuições e idéias que antes. É bem gratificante receber esses e-mails e até mesmo aqueles com dúvidas ou bug-reports – isso mostra que tem gente que usa e se importa com o slackpkg. Como ele já tem todas as funções que acho interessantes, estou na fase de torná-lo mais rápido para (em breve) lançar a versão 1.0 -:))

2. O que é?

O slackpkg é uma ferramenta para auxiliar o pkgtool no gerenciamento de pacotes do Slackware. Embora tenha sido inicialmente projetado para atualizar os patches de segurança, agora é possível fazer várias outras coisas, como instalar pacotes novos via rede, descobrir em qual pacote está um determinado arquivo e até mesmo realizar o upgrade da distribuição inteira via rede. Uma diferença dele para outras ferramentas semelhantes é que o primeiro segue a política KISS (Keep It Simple, Stupid), ou seja, tenta se manter o mais simples possível, apenas com os recursos necessários para uma ferramenta de download/upgrade de pacotes. Até mesmo na escolha da linguagem para programar o slackpkg resolvemos mantê-lo simples: ele é todo escrito em shell, uma linguagem conhecida de 11 entre 10 administradores de sistemas, e, portanto, pode ser facilmente adaptável para suas necessidades.

Ele depende exclusivamente de arquivos encontrados nos mirrors do Slackware (ou no CD-ROM), não dependendo de nenhum arquivo externo à distribuição. Não é realizada nenhuma resolução de dependências, e muito menos são executadas configurações automáticas. Sinceramente, esse tipo de coisa é tarefa do administrador do sistema. Uma coisa é automatizar o download/upgrade, que é uma tarefa mecânica; saber se deve fazer ou não uma determinada configuração não é tarefa da ferramenta de download/upgrade, e sim de quem a executa.

3. Como funciona?

```
# slackpkg update
```

A partir de agora, você tem acesso a todas as outras funções do slackpkg: upgrade, install, reinstall, blacklist, search e remove. Com exceção do search, todas essas funções seguem o padrão:

```
# slackpkg função <padrão>
```

No qual o padrão pode ser o nome de um pacote (ou parte dele) ou de um diretório do CD do Slackware. Por exemplo:

```
# slackpkg install kde/
```

irá instalar todos os pacotes da série KDE. Enquanto:

```
# slackpkg upgrade patches
```

irá realizar o upgrade de todos os patches de segurança. Só com isso que mostramos já cumprimos as principais funções de uma ferramenta de manipulação de pacotes via rede: instalar e atualizar os pacotes. Esses e os outros comandos são melhor explicados na próxima seção.

4. Comandos

Os comandos são descritos na manpage (contribuição de um usuário, agora faltam as manpages dos arquivos de configuração), mas vamos vê-los um pouco melhor:

install|reinstall

Os dois fazem basicamente a mesma coisa: baixam e instalam um pacote. A diferença de um para o outro é que o reinstall instala apenas pacotes já instalados, enquanto o install instala apenas pacotes novos.
Como explicado anteriormente, você pode utilizar o nome de um pacote, parte do nome ou uma série inteira. Depois do slackpkg detectar quais pacotes casam com o padrão, ele irá lhe mostrar uma lista com todos os pacotes que serão instalados/reinstalados. Basta responder sim (Y) ou não (N), e, no caso da resposta afirmativa, irá começar o download e a instalação dos pacotes.

upgrade

Segue o mesmo padrão do install|reinstall e serve apenas para atualizar pacotes já instalados. O padrão mais comum a ser utilizado com ele é:

```
# slackpkg upgrade patches
```

Embora possa ser utilizado para efetuar o upgrade da distribuição inteira:

```
# slackpkg upgrade slackware
```

Apenas tome cuidado com isso, pois um upgrade completo requer alguns pequenos cuidados (como executar o lilo depois de fazer upgrade do pacote do kernel).

blacklist

Este é um comando novo e serve para colocar um pacote (ou um conjunto deles) na blacklist do slackpkg. Os pacotes listados em /etc/slackpkg/blacklist não são mais instalados/upgradeados/reinstalados pelo slackpkg.
Este comando é ideal para colocar vários pacotes ao mesmo tempo na blacklist. Eu acho particularmente útil colocar todos os kdei lá dentro...

```
# slackpkg blacklist kde-i18n
```

... e nunca mais ver pacotes com traduções do KDE em aramaico, sânscrito, tuaregue e outras línguas estranhas.

remove

Sem nenhum segredo. Irá remover os pacotes instalados que casarem com o padrão dado.

search

Procura um determinado arquivo e/ou diretório. Com este comando é possível saber em que pacote está cada arquivo. Útil para detectar em qual pacote está uma biblioteca misteriosa qualquer.

5. Fazendo o upgrade completo

Para passar o Slackware do 9 para o 9.1 utilizando o slackpkg, são necessários alguns comandos:

```
# slackpkg update          [ realiza o update das
listas de pacotes ]
# slackpkg install coreutils    [ pacote novo, mas
necessário para o 9.1 ]
# slackpkg install utempter     [ mesmo caso do
coreutils           ]
# slackpkg upgrade slackware    [ realiza o upgrade
de todos os pacotes
                                instalados. Se não fossem
adicionados
                                pacotes novos na distri-
buição, este
                                seria o único comando
necessário além
                                do "update"
                              ]
```

Se não fossem alterados os nomes de alguns pacotes, o upgrade poderia ser feito apenas com os dois comandos abaixo:

```
# slackpkg update
# slackpkg upgrade slackware
```

Se você não quiser fazer apenas o upgrade dos pacotes existentes, mas também deseja instalar os pacotes novos, incluídos no 9.1, o comando a ser utilizado é:

```
# slackpkg install slackware
```

Recomendo que sejam instalados alguns dos pacotes novos para deixar a sua vida mais agradável e já compatível com o kernel 2.6: instale todos os que fazem parte do ALSA (slackpkg install alsa) e o module-init-tools.

Arquivos de configuração

Todas as configurações do slackpkg ficam dentro do /etc/slackpkg. Elas estão distribuídas em três arquivos:

mirrors

O mirrors tem a lista de mirrors do Slackware. Você pode incluir lá qualquer mirror que goste, precisando apenas seguir a regra:

```
http://lal.../lal...lala/ -> para mirrors via web
ftp://lala.../lala...ala/ -> para mirrors via ftp
file://la...l/lalal...la/ -> para mirrors locais
```

Um sinônimo para file:// é cdrom://. Os dois são tratados como sendo mirrors locais, podendo ser um CD-ROM, um HD ou mesmo um diretório montado via NFS ou SAMBA.

blacklist

Neste arquivo ficam listados os pacotes que NÃO deverão ser instalados ou atualizados. É muito importante colocar apenas o nome de UM pacote por linha e que não haja nada depois do nome do pacote. Sim, é um arquivo bem "fresco" para ser editado, mas os pacotes podem ser inclusos nele por meio do comando "blacklist".

slackpkg.conf

Aqui ficam as verdadeiras configurações do slackpkg. São uma série de variáveis de ambiente, com fartos comentários de como utilizar cada uma, mas nunca é demais esclarecer:

TEMP - Os pacotes, quando forem baixados da Internet, irão todos para este diretório, e é interessante que este tenha espaço para pacotes grandes, como os do TEX ou o kernel-source

DELALL - Se for 0, os pacotes que estão no TEMP serão mantidos (até você apagá-los manualmente); se for 1, eles serão todos apagados após o download (o que é uma boa idéia para você não acabar com o espaço no seu HD com zilhões de pacotes)

CHECKPKG - Esta variável indica se o pacote que você baixou será verificado ou não antes de ser instalado. Dica de amigo: faça a verificação.

WGETFLAGS - Parâmetros para passar ao wget. Você pode querer colocar aqui as configurações do seu proxy, por exemplo.

FIRST, SECOND, THIRD e FOURTH - Estabelecem a prioridade de busca dos pacotes. Por default, primeiro eles são procurados no patches, depois no slackware, no extra e, por fim, no pasture. Com isso, se você mandar fazer um "upgrade slackware" e um pacote do patches for mais novo, ele irá baixar o pacote do patches.

São poucas variáveis, e a configuração padrão costuma ser suficiente para todos os casos. Um cuidado especial para a definição do diretório temporário: coisas estranhas acontecem se acabar o espaço nele.

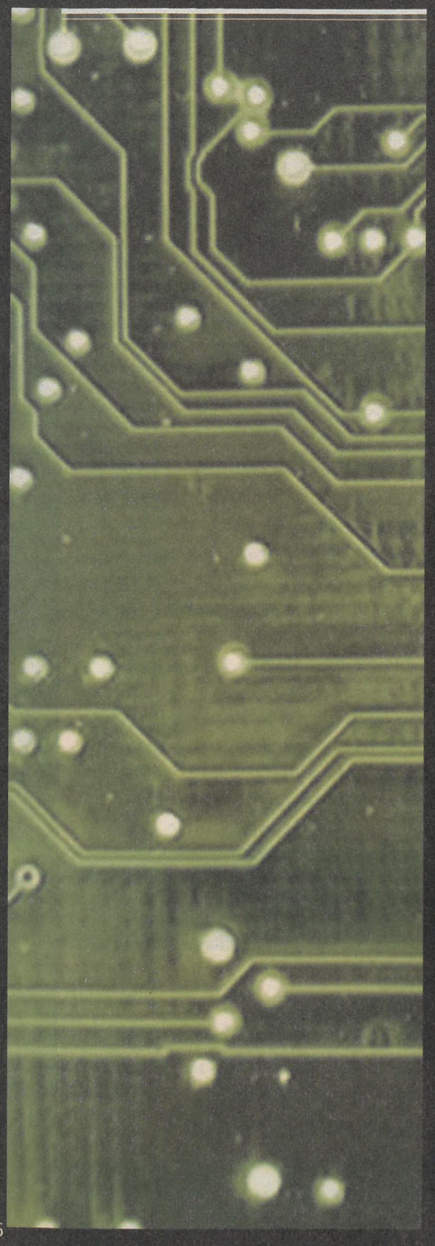
Finalizando

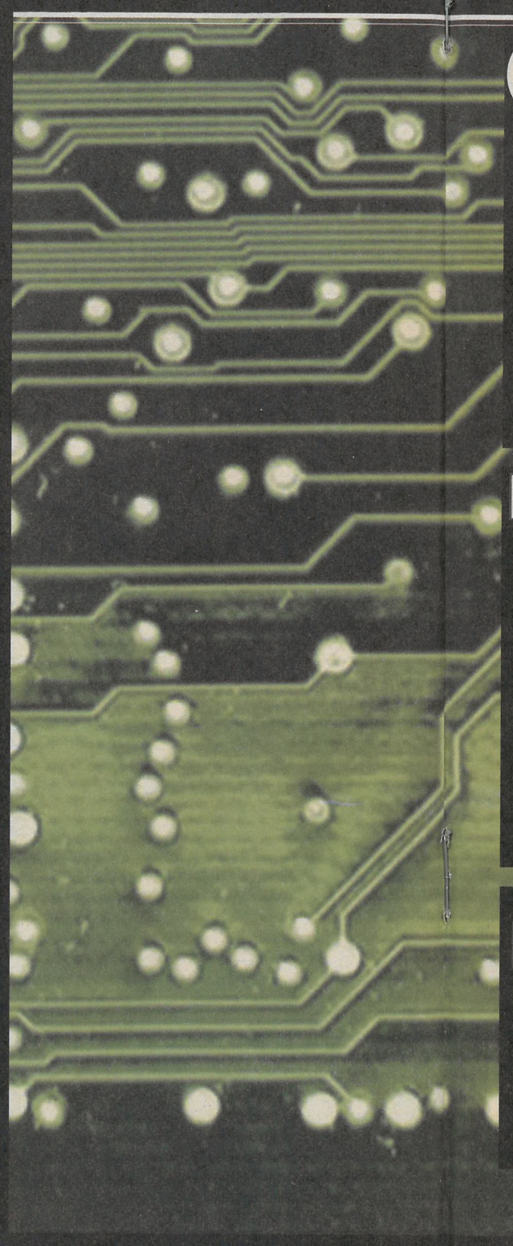
Neste artigo vimos como foi criado o slackpkg, como ele funciona e para que serve. Se você tem alguma dúvida, sugestão, patch, bug report para o slackpkg ou para este artigo, entre em contato: piterpk@terra.com.br.

IDS

Terminologia

Parte I





Os IDSs (Intrusion Detection Systems, ou Sistemas de Detecção de Intrusão) estão ainda em sua infância, mas, em termos de desenvolvimento, estão evoluindo a uma velocidade extraordinária, juntamente com toda sua terminologia. Como resultado de seu rápido crescimento em termos de marketing por parte de seus desenvolvedores, algumas confusões vêm surgindo acerca do significado correto dos termos-chave. Em alguns casos, o mesmo termo pode ser usado por diferentes desenvolvedores para dizer coisas diferentes. Este artigo divide-se em partes que pouco a pouco irão ensinar-lhe os IDSs, e vamos discutir, ao longo delas, o uso destes, como o Snort. Mas, primeiramente, vamos entender sua terminologia. A primeira parte aqui presente discute a terminologia do IDS, incluindo termos que podem causar certa divergência na comunidade.

> Alerts ou Events (Alertas ou Eventos)

Um alerta IDS é um aviso emitido pelo IDS ao operador de sistema quando ele detecta atividade suspeita. O IDS manda o alerta tanto local quanto remotamente de várias formas. O bespoke GUI é considerado a forma mais comum para os analistas que recebem essa informação, diretamente ou via database.
Tenho visto syslogs, event logs, arquivos flat, e-mail, pop-ups e até mensagens de celular sendo usados. O uso mais impressionante que eu vi de um telefone foi o de um rapaz que configurou o seu honeypot para que este mandasse, para o seu celular, os logs de cada passo do hacker que estava dentro de seu sistema, e isso lhe permitia cortar a conexão quando surgia algum risco.

> ArchNIDS (Advanced Reference Archive of Current Heuristics for Network Intrusion Detection Systems)

Desenvolvido por Max Vision's White Hats, ArachNIDS é um banco de dados que registra os perfis de ataques usados dinamicamente para criar assinaturas compatíveis com vários NIDS (Network IDS).

> Automated/Active Response (Resposta Automática)

Assim como alertam um ataque, alguns IDSs podem automaticamente defender-se deles. Isso é ativado por uma série de formas: primeiro, reconfigurando roteadores e firewalls para rejeitar tráfego pesado do mesmo destinatário, ou, segundo, criando pacotes na rede pra resetar a conexão.
Entretanto, existem problemas nos dois métodos. Um atacante pode, por exemplo, utilizar-se de um endereço spoofado para convencer o firewall, router ou o que seja a bloquear um endereço amigo, já os resets podem causar um falso positivo, causando interrupção no tráfego normal.
Os atacantes usam os resets por meio de seu ataque para descobrir, por entre os pacotes TTL, onde o IDS da rede está, uma vez que alguns distribuidores marcam seus resets com variáveis TTL.
Outras considerações são: os resultados vão para ambos, origem e destino? Onde o pacote é injetado na rede? Finalmente, e os pacotes UDP?
Sinceramente, acho que o Automated Response só deve ser usado em ambientes nos quais as chances de um falso positivo são mínimas, e mesmo assim o administrador deve correr o risco.

> Bandwidth (Largura de banda)

Bandwidth é a maior quantia de dados que pode atravessar um segmento de rede. O uso da largura de banda é uma grande ferramenta para os analistas de IDS, uma vez que o aumento inesperado pode ser um alerta de DDOS ou algum ataque co-relativo.

> Blacklist (Lista Negra)

Milhares de organizações mantêm atualizada uma lista de endereços já identificados por elas como ameaças, que irão ou vão ser bloqueados ou monitorados de perto. Alguns sites na Internet mantêm essas listas para download, como o http://www.kgb.to/.

CIDF - Common Intrusion Detection Framework (Sistema Público de Detecção de Intrusão)

O CIDF consiste num esforço para padronizar a detecção de intrusão, desenvolvendo protocolos e aplicações e programando interfaces, nas quais os programas de detecção possam trocar informações e recursos para que registros anteriores possam ser reutilizados no sistema.

CISL - Common Intrusion Specification Language (Sistema Público de Especificação de Linguagem de Intrusão)

CISL é a linguagem usada pelo CIDF para comunicar-se entre si.

Content Monitoring (Monitoramento de Conteúdo)

Esta consiste na habilidade de aplicar regras de segurança ao corpo das comunicações em transmissões de rede. Em conjunto, refere-se à filtragem de URL e e-mail.
De maneira diferente dos elementos de infra-estrutura, como roteadores, firewalls e alguns IDS, que vasculham o conteúdo independentemente do contexto, o sistema de monitoramento de conteúdo deve reunir as transmissões de rede para análise do contexto, para depois analisar o conteúdo.

Consoles

Para fazer o IDS se adequar à aplicação corporativa, os sensores do IDS dispersados precisam se reportar a um console principal. Agora, muitos desses consoles aceitam dados de outras fontes, como IDSs de outros fabricantes, firewalls, roteadores, etc. Essas informações podem ser relacionadas para apresentar uma imagem mais bem formada do ataque. Onde o console aceita múltiplas fontes, cada produto irá reportar o mesmo evento de formas diferentes. O console principal de segurança terá sua própria taxonomia, permitindo que os eventos sejam analisados, enquanto que o evento a ser entendido será somente o transmitido pelo console.

Correlation (Correlação)

Correlação é a interação de múltiplas fontes de dados para explorar um entendimento maior de um incidente.

CVE – Common Vulnerabilities and Exposures (Vulnerabilidades Públicas)

Um problema antigo quando se trata de vulnerabilidades é que os fabricantes de diferentes scanners chamarão a mesma vulnerabilidade por um nome diferente. Mais ainda: alguns fabricantes têm assinaturas múltiplas da mesma vulnerabilidade, aumentando o banco de dados de seu produto e tornando-o, ilusoriamente, mais efetivo. A MITRE foi a fundo e, com o CVE, padronizou nomes de vulnerabilidades – por favor, visitem www.cve.mitre.org.

DeepSight Analyzer e DeepSight Threat Management System

Os DeepSight Analyzer e TMS são um serviço gratuito oferecido pela SecurityFocus e Symantec (SecurityFocus pertence à Symantec), no qual redes conectadas à Internet devem passar seus eventos de segurança de rede anonimamente. Os eventos são, então, correlacionados por diferentes IDS e firewalls, permitindo ao usuário monitorar com muito mais confiança o seu sistema.

Desynchronization (Veja Evasão)

Originalmente, o termo foi usado como método de evasão utilizando seqüência de números. Essa técnica foi vista em 1998 e está obsoleta.

Enumeration (Enumeração)

É quando o atacante procura descobrir em uma rede quais serviços e hosts estão presentes. Essa ação não é mais passiva, portanto pode ser detectada.

Evasion (Evasão)

Evasão é o processo de mandar um ataque sem que o IDS detecte-o com sucesso. O truque é fazer o IDS ver uma coisa e o alvo, outra. Uma forma de evasão é setar diferentes tempos de vida (TTL) para diferentes pacotes. Dessa forma, a informação passa pelo IDS como inofensiva – mas o TTL considerado inofensivo não seria o suficiente para alcançar o alvo. Uma vez, além do IDS e perto do alvo, o pacote inofensivo é abandonado, deixando o pacote nocivo ativo.
Esse exemplo está extremamente resumido. Para se aprofundar mais no assunto, acesse a URL abaixo para ver alguns dos princípios de evasão, inserção e DoS (em inglês): http://www.securityfocus.com/library/745.

False Negatives/Miss (Falso Negativo/Perda)

Um falso negativo acontece quando um ataque ou evento ou não é detectado pelo IDS, ou é considerado benigno pelo analista. Geralmente, o termo falso negativo se aplica ao IDS, não reportando um evento.
Quanto ao analista, ocorre o seguinte: ele vê certa assinatura dia apos dia e sabe que ela é benigna, ignorando-a, mas um dia o IDS reporta um ataque genuíno com a mesma assinatura. O analista, então, ignora-o, acreditando ser benigno, assim gerando um Falso Negativo.

False Positives/False Alarm

É um evento que é pego como ataque pelo IDS, mas que na verdade é benigno.

Fragmentation (Fragmentação)

Se um pacote é grande demais para passar em um segmento de rede, ele terá que quebrá-lo em pedaços menores (fragmentos). Geralmente, a fragmentação é vista em redes que têm diferentes MTU (Maximum Transmission Units, ou Número Máximo de Unidades de Transmissão). Por exemplo, para redes em anel, o MTU é 4464, e para Ethernet é 1500. Então, se um pacote se move da rede em anel à Ethernet, ele terá de ser fragmentado em pedaços menores, e estes, reagrupados no alvo depois.
Hackers vêem a fragmentação como um método de evasão aos IDS, e há também alguns ataques de DoS que usam essa técnica.

Heuristics (Heurística)

O termo deve ser usado com inteligência artificial (AI), usada por IDSs na detecção de intrusões. É do conhecimento geral que eles ainda não são "espertos" o suficiente e que podem ser treinados por hackers a ignorar o tráfego malicioso.

Honeynet Project (Projeto Honeynet)

De acordo com a desenvolvedora, uma honeynet "é uma ferramenta de aprendizado". Trata-se de uma rede de sistemas de produção que foi desenhada para ser atacada. Uma vez comprometida, a informação é capturada e analisada, para aprender sobre a comunidade black hat. A Honeynet é uma fonte de recursos de extremo valor, provendo uma visão interna de um ataque.

Honeypot

Honeypots são ferramentas de segurança que apresentam grande flexibilidade. Elas não solucionam um problema específico, mas têm múltiplos usos, como prevenção de intrusão, detecção ou reunião de informações. Todos os honeypots partilham o mesmo conceito: um recurso de segurança que não deve ter produção ou atividade autorizada - e isso o torna de fácil uso.
Existem, no geral, dois tipos: produção e pesquisa. O honeypot de produção é conhecido como honeypot de baixa interação, de fácil uso, de captura de informação limitada apenas e é usado primariamente por companhias ou corporações para monitorar assuntos internos. Os honeypots de pesquisa são complexos de desdobrar e manter, capturam grande quantidade de informação e são usados primariamente para pesquisa por organizações militares ou governamentais. Outro propósito é atrasar atacantes em sua busca de alvos legítimos, causando uma perda de tempo razoável no honeypot, em que o alvo original está seguro, deixando os dados de real valor protegidos. Em alguns países, os órgãos da lei não podem ser acionados tendo o honeypot como prova de invasão.

Bibliografia:

Artigo de Andy Cuff sobre IDS para a SecurityFocus

Fernando Giannaccari
fernando@delta5.com.br
www.Delta5.com.br

Consultas DNS

por Frederico Argolo
fredargolo@ufrj.br

Uma das fases mais importantes da invasão é o *footprint*, método em que o atacante busca o máximo de informações sobre o *host* alvo para, a partir delas, tentar a invasão efetivamente. Um meio de se obter tais informações que merece destaque é por meio de consultas à base de DNS.

O foco deste artigo é mostrar, na prática, a importância da configuração doDNS, pois uma vez que este é mal configurado, informações valiosas podem ficar disponíveis na Internet, em que qualquer um pode obtê-las.

1 - O que é e como funciona o DNS ?

DNS é a sigla para *Domain Name System* ou Sistema de Nomes de Domínios.

É uma base de dados hierárquica, distribuída para a resolução de nomes de domínios em endereços IP e vice-versa.

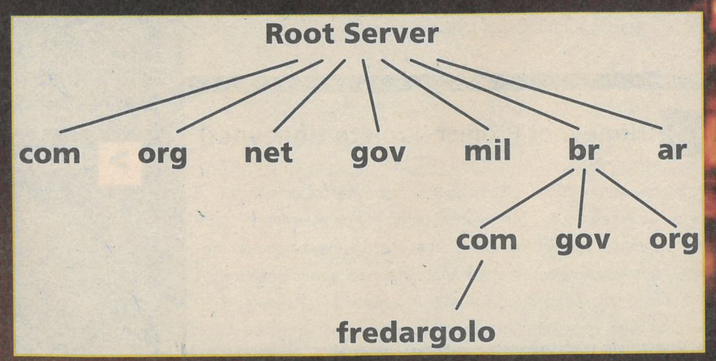
A estrutura de nomes na Internet tem o formato de uma árvore invertida na qual a raiz é conhecida como *root server* (servidor raiz).

Os ramos imediatamente inferiores ao servidor raiz são os *Top-Level Domain Names* (TLDs), divididos em dois tipos: os de três e de duas letras.

TLDs de três letras foram os primeiros a serem criados, sendo originalmente domínios estadounidenses. Mais tarde, três deles foram reclassificados como TLDs genéricos, chamados de GTLDs, que são os .COM, .NET e .ORG. Os demais (.EDU, .MIL, etc.) continuam sendo exclusivos dos EUA.

Já os TLDs de duas letras surgiram com a internacionalização da Internet, e suas letras correspondem a um código para cada país. São os ccTLDS (Country Codes TLDs), como, por exemplo, .br para o Brasil e .ar para Argentina.

Então, ao fazermos uma consulta por fredargolo.com.br, a árvore ficaria assim:



2 – Primeiras consultas

Entendido o funcionamento do DNS, podemos ir adiante. Existem diversos tipos diferentes de registro disponíveis na especificação DNS, mas a maioria deles não está relacionada às pesquisas do *host* para a obtenção do IP e vice-versa.

Esses outros registros, porém, têm uma tendência a vazar informações para o atacante quando utilizados.

Os mais utilizados são:

A	**Host Adress**	**define o endereço IP relacionado ao nome de máquina**
CNAME	**Canonical Name**	**cria um alias para um domínio**
HINFO	**Host Information**	**cpu e sistema operacional do HOST**
NS	**Name Server**	**indica quem é servidor DNS do domínio**
MX	**Mail Exchanger**	**host que atua como mail exchanger do domínio**
PTR	**Pointer Register**	**nome do host para um dado endereço IP**
SOA	**Start of Authority**	**define o servidor DNS**
TXT	**Arbitrary text**	**texto sobre a máquina**

Vamos fazer uma consulta a todos os registros do domínio fredargolo.com.br, usando as ferramentas nslookup, host e dig. Esse é um domínio fictício que será usado nos exemplos e que possui o BIND como servidor DNS.

```
nslookup with
  the '-sil[ent]' option to
prevent this message from
appearing.
  > set type=any
  > fredargolo.com.br
  Server: 127.0.0.1
  Address: 127.0.0.1#53
  fredargolo.com.br
  origin = ns.fredargolo.com.br
  mail addr =
root.fredargolo.com.br
  serial = 2003082500
  refresh = 28800
  retry = 14400
  expire = 3600000
  minimum = 86400
  fredargolo.com.br nameserver =
ns.fredargolo.com.br.
  Name: fredargolo.com.br
  Address: 192.168.0.1
  fredargolo.com.br text = "Labo-
ratório do 1o. andar"
  fredargolo.com.br hinfo = "i686"
"Slackware"
```

```
——— Usando host ———

$ host -a fredargolo.com.br
Trying "fredargolo.com.br"
;; ->>HEADER<<- opcode: QUERY,
status: NOERROR, id: 1690
;; flags: qr aa rd ra; QUERY: 1,
ANSWER: 5, AUTHORITY: 0,
ADDITIONAL: 1
;; QUESTION SECTION:
;fredargolo.com.br. IN ANY
;; ANSWER SECTION:
fredargolo.com.br. 86400 IN SOA
ns.fredargolo.com.br.
root.fredargolo.com.br.
2003082500 28800 14400 3600000
86400
fredargolo.com.br. 86400 IN NS
ns.fredargolo.com.br.
fredargolo.com.br. 86400 IN A
192.168.0.1
fredargolo.com.br. 86400 IN TXT
"Laboratório do 1o. andar"
fredargolo.com.br. 86400 IN
HINFO "i686" "Slackware"
;; ADDITIONAL SECTION:
ns.fredargolo.com.br. 86400 IN A
192.168.0.1
Received 193 bytes from
127.0.0.1#53 in 1 ms

——— Usando nslookup ———

$ nslookup
Note: nslookup is deprecated and
may be removed from future releases.
Consider using the 'dig' or
'host' programs instead. Run
```

```
——— Usando dig ———

$ dig -t any fredargolo.com.br
; <<>> DiG 9.2.2 <<>> -t any
fredargolo.com.br
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY,
status: NOERROR, id: 64765
;; flags: qr aa rd ra; QUERY: 1,
ANSWER: 5, AUTHORITY: 0,
ADDITIONAL: 1
;; QUESTION SECTION:
;fredargolo.com.br. IN ANY
;; ANSWER SECTION:
fredargolo.com.br. 86400 IN SOA
ns.fredargolo.com.br.
root.fredargolo.com.br.
2003082500 28800 14400 3600000 86400
fredargolo.com.br. 86400 IN NS
ns.fredargolo.com.br.
fredargolo.com.br. 86400 IN A
192.168.0.1
fredargolo.com.br. 86400 IN TXT
"Laboratório do 1o. andar"
fredargolo.com.br. 86400 IN
HINFO "i686" "Slackware"
;; ADDITIONAL SECTION:
ns.fredargolo.com.br. 86400 IN A
192.168.0.1
;; Query time: 4 msec
;; SERVER:
127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Aug 10 23:57:13 2003
;; MSG SIZE rcvd: 193
```

As informações do tipo TXT e HINFO não são necessárias para o funcionamento do DNS. Note que, partindo-se delas, descobrimos a localização da máquina (*Laboratório do 1o. Andar*), sua arquitetura (*i686*) e sistema operacional (*Slackware*).

Muitos administradores acham que esses dados são irrelevantes. No entanto, não percebem o quanto isso facilita ao atacante aplicar uma engenharia social contra a sua empresa.

Para evitar que essas informações fiquem expostas, bastar ir ao arquivo de configuração do domínio – que no meu caso é *named.fredargolo* – e apagar as linhas que contiverem os registros HINFO e TXT.

3 – Obtendo a versão do BIND

Outra informação que também não deve ficar exposta é a versão do BIND.

Isso porque os *scripts kiddies* vão procurar, nos diversos repositórios de exploits espalhados pela rede, um que explore alguma vulnerabilidade da versão do seu BIND.

```
——— Usando host ———

$ host -t txt -c CHAOS
version.bind. fredargolo.com.br
Using domain server:
Name: 192.168.0.1
Address: 192.168.0.1#53
Aliases:
version.bind text "9.2.2"

——— Usando nslookup ———

$ nslookup -q=txt -class=CHAOS
version.bind. fredargolo.com.br
Note: nslookup is deprecated and
may be removed from future
releases.
Consider using the 'dig' or
'host' programs instead. Run
nslookup with
the '-sil[ent]' option to
prevent this message from
appearing.
Server: 192.168.0.1
Address: 192.168.0.1#53
version.bind text = "9.2.2"

——— Usando dig ———

$ dig @fredargolo.com.br
version.bind chaos txt
; <<>> DiG 9.2.2 <<>>
@fredargolo.com.br version.bind
chaos txt
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY,
status: NOERROR, id: 27685
```

```
  ;; flags: qr aa rd; QUERY: 1,
ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0
  ;; QUESTION SECTION:
  ;version.bind. CH TXT
  ;; ANSWER SECTION:
  version.bind. 0 CH TXT "9.2.2"
  ;; Query time: 3 msec
  ;; SERVER:
192.168.0.1#53(fredargolo.com.br)
  ;; WHEN: Sun Aug 10 23:54:17
2003
  ;; MSG SIZE rcvd: 48
```

Para esconder a versão do BIND, adicione a linha *version "Not Available"* no trecho *options* do arquivo de configuração */etc/named.conf*, ficando assim:

```
options {
directory "/var/named";
version "Not Available";
};
```

Vamos verificar se funcionou:

```
$ host -t txt -c CHAOS
version.bind. fredargolo.com.br
Using domain server:
Name: 192.168.0.1
Address: 192.168.0.1#53
Aliases:
version.bind text "Not Available"
```

Opa! Agora os *scripts kiddies* vão ter que achar outro servidor que tenha a versão que eles precisam para usar o *exploit*.

4 - Transferência de zona

Transferência de zona é o processo de replicar um arquivo de zona para outro servidor DNS. Assim, o servidor DNS secundário (*slave*) possuirá uma réplica do banco de dados do servidor primário (*master*).

Sempre que há alguma alteração no banco de dados do primário, a transferência de zona do servidor primário para o secundário é realizada. Essa redundância de dados evita que tenhamos somente um ponto de falha, ou seja: se o servidor primário ficar indisponível, o servidor secundário assume.

O problema é que, a princípio, o atacante também pode executar uma transferência de zona e capturar todo o arquivo de zona de DNS. Primeiro, ele precisa conhecer quem são os *Name Server* do domínio.

```
$ host -t ns fredargolo.com.br
fredargolo.com.br name server
ns.fredargolo.com.br.
fredargolo.com.br name server
ns.algumacoisa.com.br.
```

Agora pegamos uma transferência da zona fredargolo.com.br de um servidor ns.algumacoisa.com.br.

```
————Usando host ————

$ host -l fredargolo.com.br
ns.algumacoisa.com.br
Using domain server:
Name: ns.fredargolo.com.br
Address: 192.168.0.1#53
Aliases:
fredargolo.com.br SOA
ns.fredargolo.com.br.
root.fredargolo.com.br.
2003082500 28800 14400 3600000
86400
ns.fredargolo.com.br has address
192.168.0.1
ftp.fredargolo.com.br has
address 192.168.0.2
gw.fredargolo.com.br has address
200.200.200.200
cisco-net32.fredargolo.com.br
has adress 192.168.0.3
intranet.fredargolo.com.br has
address 192.168.0.4
fredargolo.com.br SOA
ns.fredargolo.com.br.
root.fredargolo.com.br.
2003082500 28800 14400 3600000
86400

——— Usando nslookup ———

$ nslookup -q=axfr
fredargolo.com.br
ns.algumacoisa.com.br
Note: nslookup is deprecated and
may be removed from future
releases.
Consider using the 'dig' or
'host' programs instead. Run
nslookup with
the '-sil[ent]' option to
prevent this message from
appearing.
Server: ns.fredargolo.com.br
Address: 192.168.0.1#53
fredargolo.com.br
origin = ns.fredargolo.com.br
mail addr =
root.fredargolo.com.br
serial = 2003082500
refresh = 28800
retry = 14400
expire = 3600000
minimum = 86400
fredargolo.com.br nameserver =
ns.fredargolo.com.br.
Name: fredargolo.com.br
Address: 192.168.0.1
Name: ftp.fredargolo.com.br
Address: 192.168.0.2
Name: gw.fredargolo.com.br
Address: 200.200.200.200
Name: cisco-
net32.fredargolo.com.br
Address: 192.168.0.3
Name: intranet.fredargolo.com.br
Address: 192.168.0.4
fredargolo.com.br
origin = ns.fredargolo.com.br
mail addr =
root.fredargolo.com.br
serial = 2003082500
refresh = 28800
retry = 14400
expire = 3600000
minimum = 86400

——— Usando dig ———

$ dig @ns.algumacoisa.com.br
axfr fredargolo.com.br
; <<>> DiG 9.2.2 <<>>
@ns.fredargolo.com.br axfr
fredargolo.com.br
;; global options: printcmd
fredargolo.com.br. 86400 IN SOA
ns.fredargolo.com.br.
root.fredargolo.com.br.
2003082500 28800 14400 3600000
86400
ns.fredargolo.com.br. 86400 IN A
192.168.0.1
ftp.fredargolo.com.br. 86400 IN
A 192.168.0.2
gw.fredargolo.com.br. 86400 IN A
200.200.200.200
cisco-net32.fredargolo.com.br.
86400 IN A 192.168.0.3
intranet.fredargolo.com.br.
86400 IN A 192.168.0.4
ns.fredargolo.com.br.
root.fredargolo.com.br. 2003082500
28800 14400 3600000
86400
;; Query time: 17 msec
;; SERVER:
192.168.0.1#53(ns.algumacoisa.com.br)
;; WHEN: Mon Aug 25 18:01:30
2003
;; XFR size: 8 records
```

O retorno que esse comando pode oferecer é realmente impressionante. No exemplo, vimos a riqueza das informações que conseguimos obter mapeando o domínio fredargolo.com.br.

Para evitar que o atacante realize uma transferência de zona, você deve definir quais máquinas podem executar as transferências adicionando a linha *allow-transfer* no trecho *options* do arquivo */etc/named.conf*:

```
acl rede {
10.0.1/24;
10.10.0.10/32;
}
options {
.... allow-transfer { rede; };
....
}
```

A acl rede definiu que o IP 10.10.0.10 e a rede 10.0.1 podem realizar transferência de zona. Então, agora, se algum IP além desses tentar executar uma transferência, será recusado. Observe:

```
$ host -l fredargolo.com.br
ns.fredargolo.com.br
Using domain server:
Name: ns.fredargolo.com.br
Address: 192.168.0.1#53
Aliases:
Host fredargolo.com.br not
found: 5(REFUSED)
; Transfer failed.
```

Caso cada zona tenha uma rede ou IPs específicos, coloque a cláusula *allowtranfer* dentro do bloco que define a zona do arquivo */etc/named.conf*.

5 - Consultas reversas

É a forma pela qual você obtém o host a partir do IP (de maneira diferente do que normalmente é feito).

```
——— Usando host ———

$ host 192.168.0.2
2.0.168.192.in-addr.arpa domain
name pointer ftp.fredargolo.com.br

——— Usando nslookup ———

$ nslooup 192.168.0.2
Note: nslookup is deprecated and
may be removed from future
releases.
Consider using the 'dig' or
'host' programs instead. Run
nslookup with
the '-sil[ent]' option to
prevent this message from
appearing.
Server: 127.0.0.1
Address: 127.0.0.1#53
2.0.168.192.in-addr.arpa name =
ftp.fredargolo.com.br.

——— Usando dig ———

$ dig -x 192.168.0.2
; <<>> DiG 9.2.2 <<>> -x
192.168.0.2
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY,
status: NXDOMAIN, id: 42304
;; flags: qr aa rd ra; QUERY: 1,
ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 0
;; QUESTION SECTION:
;2.0.168.192.in-addr.arpa. IN
PTR ftp.fredargolo.com.br
;; AUTHORITY SECTION:
0.168.192.in-addr.arpa. 86400 IN
SOA ns.fredargolo.com.br.
;; Query time: 6 msec
;; SERVER:
127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Aug 31 16:05:51
2003
;; MSG SIZE rcvd: 103
```

Agora, vamos para um exemplo um pouco mais perigoso:

```
$ for i in 'seq 1 5'; do host
192.168.0.$i ; done
1.0.168.192.in-addr.arpa. domain
name pointer ns.fredargolo.com.br.
2.0.168.192.in-addr.arpa. domain
name pointer
ftp.fredargolo.com.br.
3.0.168.192.in-addr.arpa. domain
name pointer cisconet32.
fredargolo.com.br.
4.0.168.192.in-addr.arpa. domain
name pointer
intranet.fredargolo.com.br.
Host 5.0.168.192.in-addr.arpa.
not found: 3(NXDOMAIN)
```

Com uma simples linha de comando como a acima, um atacante poderia executar consultas reversas nos endereços IP da rede para obter os nomes dos *hosts*.

Repare que na consulta reversa mapeamos a rede 192.168.0, enquanto no exemplo da transferência de zona, mapeamos o domínio fredargolo.com.br, que é diferente.

A recomendação, então, é alterar o registro PTR do arquivo de configuração do domínio reverso para algo do tipo

```
1 IN PTR 192-168-0-1.fredargolo.com.br.
```

Fazendo novamente uma consulta reversa, notamos que o atacante não tem como obter nenhuma informação comprometedora.

```
$ host 192.168.0.1
1.0.168.192.in-addr.arpa domain
name pointer 192-168-0-
1.fredargolo.com.br.
```

6 – Conclusão

Espero que este artigo tenha conseguido mostrar a quantidade de informações que podem ser obtidas graças a uma má configuração do servidor DNS, como obtê-las e como evitá-las.

Dúvidas e sugestões podem ser encaminhadas para fredargolo@ufrj.br.

Por Piter PUNK

Configurando um 386SX como roteador

Como utilizar o Linux para transformar um 386 em um roteador

Neste artigo, iremos ensinar como transformar um 386SX com apenas 4 MB de RAM em um roteador útil e funcional. É o Linux (mais uma vez) salvando a pátria e dando uso a um computador considerado, por alguns, como inútil.

1. A máquina

386SX
4 MB de RAM
110 MB de HD
Placa de rede NE2000 ISA
Modem US-Robotics 33600 ISA

2. Instalação

O Linux utilizado foi o Slackware 7.1, mas poderia ser o 7.0 também. Em geral, é melhor utilizar o kernel 2.0.x; no entanto, o objetivo deste artigo é escrever um firewall, e existe muito mais documentação sobre o ipchains (da série 2.2.x) do que sobre o ipfwadm (da série 2.0.x). Se você souber usar o ipfwadm, instale o Slackware 3.3 ou 96, e você terá um desempenho melhor.

O primeiro passo da instalação é retirar o HD do 386 e colocá-lo em outro computador mais possante. Coloque-o como master da primária. Insira o CD do Slackware e dê o boot pelo CD-ROM.

Não existe segredo aqui, eu particionei o meu HD assim:

```
/     /dev/hda1    102MB
swap  /dev/hda2      8MB
```

E sobrou espaço no /. Como sobrou espaço, é mais inteligente fazer desta forma:

```
/     /dev/hda1     90MB
/tmp  /dev/hda2     12MB
swap  /dev/hda3      8MB
```

Assim, você pode montar a partição / como read-only e desligar e ligar o computador direto, sem a necessidade de um shutdown. Tenha em mente que os logs do sistema terão que ser desligados ou enviados para outra máquina, já que nesta tudo opera em read-only. Se você prefere manter seus logs no próprio roteador, utilize a partição / como rw (ou faça uma /var separada).

Depois do reparticionamento, inicie o programa de instalação e siga as instruções normalmente. Quando for formatar a partição, lembre-se de escolher 1024 bytes por inode.

Instale as séries A e N no modo menu para que você possa retirar tudo aquilo que não for utilizar. Instale apenas o necessário para as funções de router e firewall. A minha instalação deu 67 MB, mas nada impede que a sua seja menor. Atenção! Não tente detectar a sua placa de rede: lembre-se que no 386 será outra placa! Depois do Linux instalado, reboote a máquina, mas não devolva o HD para o 386, pelo menos não ainda.

3. Configuração

Agora, vamos configurar a máquina. Se você seguiu a minha dica de particionamento, seu /etc/fstab deverá ficar deste modo:

```
      /dev/hda1  /         ext2
ro              1 1
      /dev/hda2  /tmp      ext2
defaults        1 1
      /dev/hda3  swap      swap
defaults        0 0
      none       /dev/pts  devpts
gid=5,mode=620 0 0
      none       /proc     proc
defaults        0 0
```

Se você não tem partições separadas para o /tmp e para o /, não coloque o / como read-only, caso contrário você terá problemas com isso.

Depois de editar o /etc/fstab, é importante editar o /etc/lilo.conf. Comente as linhas que dizem prompt e timeout e rode o lilo. Com essas alterações, você garante que o computador irá iniciar automaticamente.

Também deve ser editado / etc/rc.d/rc.S, em uma linha na qual está escrito:

```
      /sbin/mount -w -v -n -o
remount /
```

Deve ficar:

```
      /sbin/mount -r -v -n -o
remount /
```

Isso é feito para que o sistema de arquivos / não seja remontado como para escrita-leitura (assim a gente o obriga a ficar apenas como leitura).

Como a máquina em que vamos rodar possui pouquíssima memória, é necessário diminuir ao máximo a quantidade gasta. Para isso, um dos métodos é deixá-la com apenas um console virtual. Para tanto, edite o /etc/inittab, no qual você irá achar:

```
      c1:12345:respawn:/sbin/
agetty 38400 tty1 linux
      c2:12345:respawn:/sbin/
agetty 38400 tty2 linux
      cn:12345:respawn:/sbin/
agetty 38400 ttyn linux
```

Apague todas as linhas, deixando apenas a primeira (c1). O próximo passo é retirar os servidores desnecessários editando o /etc/rc.d/rc.inet2; infelizmente, só você pode saber o que é e o que não é necessário no seu computador.

Por último, edite o /etc/rc.d/ rc.modules e comente as seguintes linhas:

```
      if cat /proc/ksyms | grep
"\[parport_pc\]" 1> /dev/null 2> /
dev/null; then
        echo "parport0 is built-
in, not loading module" > /dev/
null
      else
      if [ -r /lib/modules/`uname
-r`/misc/parport_pc.o ]; then
          # Generic setup example:
          /sbin/modprobe
parport_pc
          # Hardware specific
setup example (required for PLIP
and better
          # performance in gene-
ral):
          #/sbin/modprobe
parport_pc io=0x378 irq=7
        fi
      fi
```

Comente ou apague todas elas (elas são responsáveis pelo carregamento do módulo da porta paralela, é só perda de memória). Também remova as seguintes linhas:

```
      if cat /proc/ksyms | grep
"\[lp\]" 1> /dev/null 2> /dev/null
; then
        echo "lp support built-in,
not loading module" > /dev/null
      else
        if [ -r /lib/modules/
`uname -r`/misc/lp.o ]; then
          /sbin/modprobe lp
        fi
      fi
```

Ainda no rc.modules, você deve habilitar o suporte para a sua placa de rede. Eu descomentei a linha:

```
/sbin/modprobe ne io=0x300 irq=7
```

Certifique-se de que o ppp também está sendo carregado, e descomente as linhas apropriadas sobre os módulos do ip masquerading:

```
      /sbin/modprobe ip_masq_irc
      /sbin/modprobe ip_masq_ftp
      /sbin/modprobe ip_masq_user
```

Esses são os que eu uso, e, dependendo do que você utiliza na Internet, deve descomentar alguns dos outros módulos. Agora é só rodar o pppsetup e configurar o seu modem.

Por último, edite o /etc/rc.d/rc.local e insira as seguintes linhas:

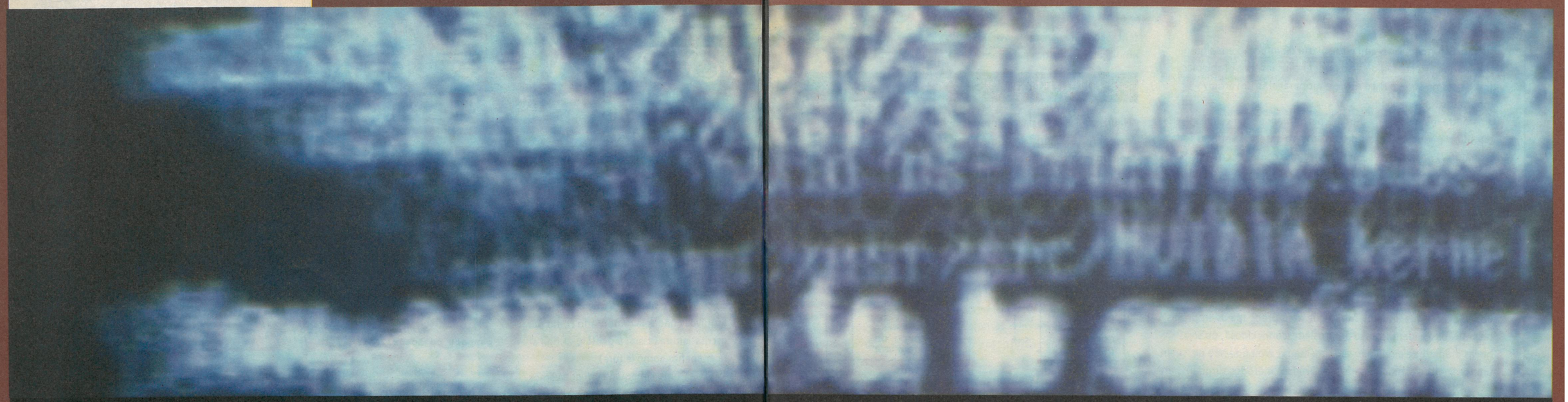
```
      /sbin/ipchains -A forward -j
MASQ
      ifconfig eth0 down
      ppp-on
      ifconfig eth0 up
```

Atenção! Isso apenas habilita o roteamento e o masquerading! Se você quiser um firewall decente, leia os vários HOWTOs escritos sobre esse assunto!

Devolva o HD para o 386 e ligue-o. Automaticamente, ele vai entrar no Linux e conectar na Internet -:) Se você instalou o root como read-only, pode desligar normalmente no power. Caso contrário, aperte CTRL+ALT+DEL para desligar.

4. Conclusão

Agora você possui um roteador – e arranjou um (bom) uso para o seu velho 386. Com o Linux é assim: sempre existe algum uso para o seu computador. Esta é apenas a primeira parte de uma série de artigos sobre como ressuscitar micros antigos. Mande sugestões ou críticaspara piterpk@terra.com.br.



Técnicas para detecção de vírus

Por Marcos Velasco
www.velasco.com.br

Nos últimos anos, as empresas de antivírus precisaram se esforçar ao máximo para criar novas tecnologias de detecção de pragas virtuais. Os antivírus dos anos 80/90 utilizavam técnicas muito diferentes dos atuais. Um exemplo é o modo de pesquisa dos arquivos. Antes, o espaço em disco era limitado a 32 MB, e isso forçava o usuário a possuir poucos dados. Com isso, os antivírus não tinham tanta preocupação em otimizar suas pesquisas, pois rapidamente faziam uma busca completa no HD. Outra peculiaridade era que a contaminação de arquivos estava limitada a poucos tipos de extensão, tais como .com e .exe, e outros poucos métodos de infecção, como o boot e o MBR.

A evolução foi inevitável. Os discos passaram a suportar dezenas de gigabytes e diversos outros formatos de arquivos puderam ser vítimas de infecções, como, por exemplo, .doc, .xls, .vbs, etc. Isso fez com que os antivírus mudassem radicalmente os métodos de pesquisa, já que precisariam melhorar a performance e dar suporte à identificação e remoção de vírus em diversos formatos. Um exemplo simples de otimização foi a necessidade de separar os tipos de vírus e os tipos de infecções, pois não existe necessidade, por exemplo, de um vírus que infecta arquivos .exe ser procurado em arquivos do Word ou Excel, e vice-versa.

Atualmente, a maioria dos vírus ainda é detectada por assinaturas binárias (pequenos blocos de dados utilizados para identificar um determinado vírus). Com a maior abrangência dos vírus, entretanto, foi necessário o desenvolvimento de novas técnicas para identificação, nos casos em que uma pesquisa por assinaturas não era possível. A pesquisa por assinatura é variável conforme o antivírus, mas, em geral, são usados de 2 a 255 bytes para identificar um determinado vírus. Como exemplo de detecção de vírus por assinatura, vamos usar um arquivo de teste chamado EICAR, que é um arquivo padrão da indústria para a verificação do funcionamento das pesquisas de um antivírus, e seu conteúdo não possui nada que possa danificar dados. O EICAR possui apenas 68 bytes e seu conteúdo total é:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
TEST-FILE!$H+H*
```


E o mesmo conteúdo em formato hexadecimal:

```
58 35 4F 21 50 25 40 41 50 5B 34 5C 50 5A 58 35 34
28 50 5E 29 37 43 43 29 37 7D 24 45 49 43 41 52 2D
53 54 41 4E 44 41 52 44 2D 41 4E 54 59 56 49 52 55
53 2D 54 45 53 54 2D 46 49 4C 45 21 24 48 2B 48 2A
```

Existem antivírus que pesquisam por todos os 68 bytes para identificar corretamente o EICAR. Isso significa que se algum caracter for modificado, o EICAR não será identificado. Esta situação ocorre também com o vírus, de modo que muitas variantes são criadas, modificando-se apenas alguns bytes. Para saber se seu antivírus usa a assinatura completa ou não, altere o conteúdo do EICAR e faça uma pesquisa com o antivírus. Um exemplo de EICAR modificado:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
ALTERADO !$H+H*
```

Alguns antivírus usam métodos de pesquisa que podem evitar este tipo de problema e conseguem identificar um arquivo usando caracteres curingas (? e *) em suas assinaturas:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$ [*] !$H+H*
```

Isso significa poder modificar um bloco por qualquer conjunto de caracteres. Com uma assinatura assim, diversos tipos de identificação seriam possíveis:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
TEST-FILE!$H+H*

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-
ALTERADO !$H+H*

X5O!P%@AP[4\PZX54(P^)7CC)7}$ALTERADO!$H+H*

X5O!P%@AP[4\PZX54(P^)7CC)7}$QUALQUER QUANTIDADE DE
BYTES!$H+H*
```

Uma assinatura deve ser bem escolhida para que sejam evitados falsos-positivos. Os falsos-positivos nada mais são que arquivos "sadios", mas que são erroneamente identificados como vírus por um programa antivírus. Usuários comuns não possuem conhecimento necessário para verificar se um arquivo realmente contém vírus

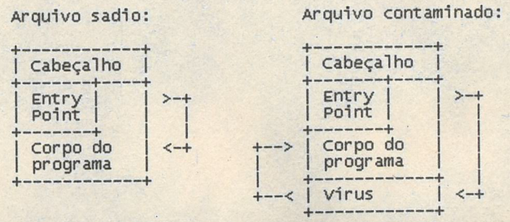
ou não. Se um antivírus emite um alerta de infecção em algum arquivo que esteja "sadio", isso poderá causar sérios problemas, pois o sistema corre o risco de ficar inoperável se um arquivo importante for removido.
Uma outra maneira de melhorar a performance em pesquisas seria identificar pequenas partes de um arquivo antes de verificar toda a assinatura. Por exemplo, se um arquivo não começa com "X5O!", significa que não é um EICAR e portanto não existe a necessidade de verificar o seu restante por esta assinatura. Deve-se lembrar que, para gerar uma assinatura, é necessário possuir um exemplar do vírus, de modo que ele possa ter seu comportamento estudado através de experimentos de infecção controlada.

>>> Detecção de vírus desconhecidos

Pode-se dizer que, atualmente, o que mais preocupa as empresas de antivírus é a identificação de vírus "desconhecidos", ou seja, novas pragas que ainda não são detectadas e/ou que não possuem uma assinatura estudada para isso. Diversos métodos surgiram para tentar conter a constante evolução dos vírus, e conceitos como emulação e heurística passaram a ser obrigatórios nos antivírus.

>>> Heurística

"Heurística" vem da palavra grega "heuriskein", e significa "descobrir". A heurística é uma técnica utilizada para estudar o comportamento, a estrutura e as características de um arquivo para defini-lo como suspeito ou não. Ela pode fazer com que o antivírus emita muitos falsos-positivos, mas é uma técnica que se mostrou bastante útil para evitar vírus desconhecidos. Em geral, um vírus que infecta arquivos .exe age da seguinte forma:



Um arquivo .exe possui um pequeno cabeçalho, um Entry Point – o ponto onde começa a execução de um programa e o programa propriamente dito. Após uma infecção, o Entry Point é alterado, de forma que passe a apontar para o código do vírus. Após a execução do vírus, este pula para o Entry Point original do programa, fazendo-o funcionar normalmente. Como a maioria dos vírus que infectam .exe trabalha desta forma, a pesquisa heurística poderia ajudar. Bastaria verificar se o Entry Point está fora da seção do código do programa ou se o Entry Point é um JMP. Mas, em alguns casos, falsos-positivos são emitidos, pois existem programas comerciais, protetores e compactadores de executáveis que trabalham da mesma forma. Então, a heurística pode ser definida como um complemento da pesquisa, que ajuda na detecção de vírus desconhecidos, mas que não tem certeza se um arquivo está contaminado ou não. Ou seja, heurística não é uma ciência exata.

A heurística consegue identificar de 70% a 90% dos vírus conhecidos e desconhecidos. Podemos dizer que é uma técnica excelente, considerando a complexidade do problema.

>>> Emulação

A emulação foi desenvolvida para tentar identificar os complicados vírus polimórficos, conhecidos como vírus mutantes, pois conseguem modificar a si próprios a cada infecção, dificultando sua identificação. Pesquisas por assinaturas em vírus polimórficos são praticamente inviáveis.

Basicamente, um emulador tenta identificar a rotina de decriptografia do vírus. Quando um vírus polimórfico é executado, primeiramente ele decriptografa seu próprio código executável, usando uma rotina anexada ao próprio vírus. Em alguns casos, uma pesquisa por assinatura poderá ser válida no código da rotina de decriptografia, mas isso não é uma regra. Em muitos casos, os vírus polimórficos ofuscam seu código, usando diversos artifícios para conseguir funcionar, mesmo com um conteúdo diferente em suas novas cópias.

Um exemplo simples: zerar um registrador de diferentes formas, com resultados idênticos.


```
Instrução
Hexadecimal
XOR AX, AX 31 C0
SUB AX, AX 29 C0
MOV AX, 0 B8 00 00
```

Se o código não for muito modificado, poderemos utilizar a heurística para identificar o vírus. Um bom exemplo do uso de emuladores serve para o vírus chamado "Simili", que foi descrito na revista "Virus Bulletin", em maio de 2002. Este vírus contém um decriptografador polimórfico que modifica o tamanho e a localização das infecções. Ele "disassembla" seu próprio código para uma forma intermediária, injeta novas instruções e sujeira ao código e "re-assembla", gerando uma nova cópia polimórfica. As novas cópias podem variar de 30 a 120 Kbytes.
Esse tipo de vírus é localizado apenas com emuladores, e muitas técnicas são exigidas para identificá-lo. O emulador permite analisar o código
disassemblado, adicionar código, criptografar/decriptografar e analisar a probabilidade de uma infecção. Outra maneira de fazer a emulação é interceptar funções da API do sistema operacional ou capturar interrupções do DOS que estejam ligadas diretamente à gravação, leitura ou execução. Se um determinado programa executar uma série de ações suspeitas, o antivírus emitirá aviso de um arquivo suspeito.

>>> Conclusão

Como se pode notar, não existe um método único de detecção para todos os casos. Os antivírus necessitam estar sempre atualizando seus métodos de pesquisa, de modo que possam identificar os novos vírus. Atualmente, por causa da Internet, as pragas se alastram rapidamente. Muitos aproveitam falhas de softwares e vulnerabilidades do sistema para conseguir se alastrar. Esse tipo de ação forçará as empresas de antivírus a criar novos mecanismos para barrar esta forma de ataque. A escolha de um bom antivírus é essencial. Entretanto, não devemos confiar plenamente em um produto antivírus, pois novos vírus são lançados diariamente, muito mais complexos e usando novas técnicas antidetecção. A melhor maneira de evitar vírus é usar o computador com bom senso:

> Evitar abrir e-mails com attachments;

> Não deixar que o boot seja feito por disquetes;

> Evitar softwares piratas;

> Desconfiar de arquivos com duplas extensões, como: .txt, .exe ou .jpg. e .vbs;

> Manter atualizações de softwares e segurança em dia;

> Quanto mais pessoas tiverem acesso a um mesmo computador, mais chance de ser infectado. Evite troca de dados com computadores "públicos".

Tech Bugs

Últimas vulnerabilidades e falhas de segurança

por Bruno Cesar
bruno@digerati.com.br

Nesta edição, o Tech Bugs apresenta somente duas vulnerabilidades, mas são duas ocorrências de segurança muito importantes e que ainda vão dar muita dor de cabeça. Apesar de a Microsoft já ter liberado um patch de segurança para o bug do serviço mensageiro do Windows, sabemos que muitos administradores de sistemas não procuram se informar sobre o que está ocorrendo em seu servidor nem em consultar novas falhas. Estar sempre informado sobre essas ocorrências de segurança significa 50% de chance a menos de o seu servidor não ser invadido. A porcentagem restante é anulada se você patchear o sistema corretamente.
As duas falhas apresentam dois exploits que estão disponíveis para estudo. A revista H4CK3R não se responsabiliza pela má utilização dessas ferramentas.

>>> mIRC USERHOST Buffer Overflow

O mIRC é um dos clientes IRC mais utilizados em sistemas rodando Windows. Também é muito conhecido pela sua facilidade e diversos usuários o utilizam para se comunicar nos mais variados servidores IRC.
O bug no software consiste em um buffer overflow remoto em que o cliente tenta uma conexão com o servidor. Durante o processo de conexão, o cliente é relatado a uma emissão ou a um pedido de USERHOST do qual se espera ter menos de 110 bytes. Assim, qualquer outro pedido de emissão maior que este valor causará o buffer.
A exploração bem-sucedida desta bug pode permitir que o usuário mal-intencionado tenha total disponibilidade de inserir um código arbitrário no contexto do cliente a fim de ganhar acesso desautorizado a um sistema vulnerável.
As versões descritas abaixo estão vulneráveis, porém nada indica que outras não estejam.

>>> Versões Afetadas:

Khaled Mardam-Bey mIRC 6.0 3
Khaled Mardam-Bey mIRC 6.0 2
Khaled Mardam-Bey mIRC 6.0 1
Khaled Mardam-Bey mIRC 6.1

>>> Exploit:

O código-fonte do exploit para estudo pode ser visto e adquirido nos seguintes endereços:

http://whiteroof.netfirms.com/userhost.zip
http://www.securitylab.ru/_exploits/userhost.zip

>>> *Solução:*

Até o momento, seu desenvolvedor não disponibilizou um patch ou correção para a vulnerabilidade. O que basta é aguardar uma nova versão do software com o bug corrigido, ou até esperar por um patch de segurança.

>>> Microsoft Messenger Service Buffer Overrun Vulnerability

O serviço mensageiro do Windows está exposto a uma vulnerabilidade causada por um buffer overrun. Isso ocorre por causa da verificação insuficiente dos limites de mensagens antes que sejam passadas a um buffer interno. A exploração bem-sucedida pode resultar em uma negação de serviço ou na execução de um código malicioso no contexto local do sistema, permitindo um acesso total e sem restrições ao sistema atacado.
A eEye Digital Security disponibilizou um scanner totalmente grátis para verificar se a máquina está vulnerável. Para adquiri-lo, acesse o seguinte endereço:
http://www.eeye.com/html/Research/Tools/MSGSVC.html

>>> Versões Afetadas:

Microsoft Windows 2000 Advanced Server SP4
Microsoft Windows 2000 Advanced Server SP3
Microsoft Windows 2000 Advanced Server SP2
Microsoft Windows 2000 Advanced Server SP1
Microsoft Windows 2000 Advanced Server
Microsoft Windows 2000 Datacenter Server SP4
Microsoft Windows 2000 Datacenter Server SP3
Microsoft Windows 2000 Datacenter Server SP2
Microsoft Windows 2000 Datacenter Server SP1
Microsoft Windows 2000 Datacenter Server
Microsoft Windows 2000 Professional SP4
Microsoft Windows 2000 Professional SP3
Microsoft Windows 2000 Professional SP2
Microsoft Windows 2000 Professional SP1
Microsoft Windows 2000 Professional
Microsoft Windows 2000 Server SP4
Microsoft Windows 2000 Server SP3
Microsoft Windows 2000 Server SP2
Microsoft Windows 2000 Server SP1
Microsoft Windows 2000 Server
Microsoft Windows NT Enterprise Server 4.0 SP6a
Microsoft Windows NT Enterprise Server 4.0 SP6
Microsoft Windows NT Enterprise Server 4.0 SP5
Microsoft Windows NT Enterprise Server 4.0 SP4
Microsoft Windows NT Enterprise Server 4.0 SP3
Microsoft Windows NT Enterprise Server 4.0 SP2
Microsoft Windows NT Enterprise Server 4.0 SP1
Microsoft Windows NT Enterprise Server 4.0
Microsoft Windows NT Server 4.0 SP6a
Microsoft Windows NT Server 4.0 SP6
Microsoft Windows NT Server 4.0 SP5
Microsoft Windows NT Server 4.0 SP4
Microsoft Windows NT Server 4.0 SP3
Microsoft Windows NT Server 4.0 SP2
Microsoft Windows NT Server 4.0 SP1
Microsoft Windows NT Server 4.0
Microsoft Windows NT Terminal Server 4.0 SP6
Microsoft Windows NT Terminal Server 4.0 SP5
Microsoft Windows NT Terminal Server 4.0 SP4
Microsoft Windows NT Terminal Server 4.0 SP3
Microsoft Windows NT Terminal Server 4.0 SP2
Microsoft Windows NT Terminal Server 4.0 SP1
Microsoft Windows NT Terminal Server 4.0
Microsoft Windows NT Workstation 4.0 SP6a
Microsoft Windows NT Workstation 4.0 SP6
Microsoft Windows NT Workstation 4.0 SP5
Microsoft Windows NT Workstation 4.0 SP4
Microsoft Windows NT Workstation 4.0 SP3
Microsoft Windows NT Workstation 4.0 SP2
Microsoft Windows NT Workstation 4.0 SP1
Microsoft Windows NT Workstation 4.0
Microsoft Windows Server 2003 Datacenter Edition
Microsoft Windows Server 2003 Datacenter Edition 64-bit
Microsoft Windows Server 2003 Enterprise Edition
Microsoft Windows Server 2003 Enterprise Edition 64-bit
Microsoft Windows Server 2003 Standard Edition
Microsoft Windows Server 2003 Web Edition
Microsoft Windows XP 64-bit Edition SP1
Microsoft Windows XP 64-bit Edition
Microsoft Windows XP 64-bit Edition Version 2003
Microsoft Windows XP Home SP1
Microsoft Windows XP Home
Microsoft Windows XP Professional SP1
Microsoft Windows XP Professional

>>> Exploit:

Um exploit disponível para estudo, com um exemplo de negação de serviço, pode ser adquirido nos seguintes endereços:

http://www.securityfocus.com/data/vulnerabilities/exploits/MS03-043_poc.c
http://downloads.securityfocus.com/vulnerabilities/exploits/ms03-043.c

>>> *Solução:*

Para alguns, a melhor solução seria desativar o serviço de mensagens, mas isso teria seus contras, pois ele ficaria indisponível para utilização.
Outra opção é bloquear a porta 135 no Windows XP e no Windows 2003 server, utilizando o Internet Connection Firewall (ICF).
A melhor solução é utilizar os patches de segurança que já foram liberados pela Microsoft. Veja as versões para seus respectivos sistemas:

Microsoft Windows 2000 Advanced Server SP4:

Microsoft Patch Security Update for Microsoft Windows 2000: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=99F1B40D-906A-4945-A021-4B494CCCBDE0&displaylang=en

Microsoft Windows 2000, Service Pack 3, Service Pack 4

Microsoft Windows 2000 Professional SP4:

Microsoft Patch Security Update for Microsoft Windows 2000: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=99F1B40D-906A-4945-A021-4B494CCCBDE0&displaylang=en

Microsoft Windows 2000, Service Pack 3, Service Pack 4

Microsoft Windows 2000 Server SP4:

Microsoft Patch Security Update for Microsoft Windows 2000: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=99F1B40D-906A-4945-A021-4B494CCCBDE0&displaylang=en

Microsoft Windows 2000, Service Pack 3, Service Pack 4

Microsoft Windows 2000 Professional SP3:

Microsoft Patch Security Update for Microsoft Windows 2000: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=99F1B40D-906A-4945-A021-4B494CCCBDE0&displaylang=en

Microsoft Windows 2000, Service Pack 3, Service Pack 4

Microsoft Windows 2000 Server SP3:

Microsoft Patch Security Update for Microsoft Windows 2000: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=99F1B40D-906A-4945-A021-4B494CCCBDE0&displaylang=en

Microsoft Windows 2000, Service Pack 3, Service Pack 4

Microsoft Windows 2000 Advanced Server SP3:

Microsoft Patch Security Update for Microsoft Windows 2000: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=99F1B40D-906A-4945-A021-4B494CCCBDE0&displaylang=en

Microsoft Windows 2000, Service Pack 3, Service Pack 4

Microsoft Windows 2000 Advanced Server SP2:

Microsoft Patch Security Update for Microsoft Windows 2000 Service Pack 2: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=A0061377-1683-4C13-9527-5534F6C7CF85&displaylang=en

Microsoft Windows 2000, Service Pack 2

Microsoft Windows 2000 Professional SP2:

Microsoft Patch Security Update for Microsoft Windows 2000 Service Pack 2: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=A0061377-1683-4C13-9527-5534F6C7CF85&displaylang=en

Microsoft Windows 2000, Service Pack 2

Microsoft Windows 2000 Server SP2:

Microsoft Patch Security Update for Microsoft Windows 2000 Service Pack 2: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=A0061377-1683-4C13-9527-5534F6C7CF85&displaylang=en

Microsoft Windows 2000, Service Pack 2

Microsoft Windows XP Home SP1:

Microsoft Patch Security Update for Microsoft Windows XP: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=F02DA309-4B0A-4438-A0B9-5B67414C3833&displaylang=en

Microsoft Windows XP Gold, Service Pack 1

Microsoft Windows XP Professional SP1:

Microsoft Patch Security Update for Microsoft Windows XP: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=F02DA309-4B0A-4438-A0B9-5B67414C3833&displaylang=en

Microsoft Windows XP Gold, Service Pack 1

Microsoft Windows Server 2003 Standard Edition :

Microsoft Patch Security Update for Microsoft Windows Server 2003: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=1DF106F3-7EC4-4EB0-9143-C1E3C9E2F5F8&displaylang=en

Microsoft Windows Server 2003

Microsoft Windows Server 2003 Enterprise Edition :

Microsoft Patch Security Update for Microsoft Windows Server 2003: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=1DF106F3-7EC4-4EB0-9143-C1E3C9E2F5F8&displaylang=en

Microsoft Windows Server 2003

Microsoft Windows Server 2003 Web Edition :

Microsoft Patch Security Update for Microsoft Windows Server 2003: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=1DF106F3-7EC4-4EB0-9143-C1E3C9E2F5F8&displaylang=en

Microsoft Windows Server 2003

Microsoft Windows Server 2003 Enterprise Edition 64-bit :

Microsoft Patch Security Update for Microsoft Windows Server 2003 64-bit Edition: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=8B990946-84C8-4C91-899C-5A44EC13174E&displaylang=en

Microsoft Windows Server 2003 64-bit Edition

Microsoft Windows XP 64-bit Edition Version 2003 :

Microsoft Patch Security Update for Microsoft Windows Server 2003 64-bit Edition: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=8B990946-84C8-4C91-899C-5A44EC13174E&displaylang=en

Microsoft Windows XP 64-bit Edition Version 2003

Microsoft Windows XP 64-bit Edition :

Microsoft Patch Security Update for Microsoft Windows XP 64-bit Edition: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=2BE95254-4C65-4CA5-80A5-55FDF5AA2296&displaylang=en

Microsoft Windows XP 64-bit Edition

Microsoft Windows NT Server 4.0 SP6a:

Microsoft Patch Security Update for Microsoft Windows NT Server 4.0: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=B1949456-996A-485A-9A28-79FD79F26A1B&displaylang=en

Microsoft Windows NT Server 4.0, Service Pack 6a

Microsoft Windows NT Workstation 4.0 SP6a:

Microsoft Patch Security Update for Microsoft Windows NT Workstation 4.0: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=7597FCF4-6615-4074-9E46-A17D808ED38D&displaylang=en

Microsoft Windows NT Workstation 4.0, Service Pack 6a

Microsoft Windows NT Terminal Server 4.0 SP6:

Microsoft Patch Security Update for Microsoft Windows NT Server Terminal Server Edition: KB828035
http://www.microsoft.com/downloads/details.aspx?FamilyId=64AB4B66-1A6E-4264-93A8-26CDB98B05A8&displaylang=en

Microsoft Windows NT Server 4.0, Terminal Server Edition, Service Pack 6

Cai a máscara da violência

Por: Maurício Martins

Mas só para quem tem estômago forte

É difícil fazer uma crítica de um filme tão polêmico quanto *Irreversível*. Presente na Mostra de Cinema de São Paulo do ano passado, ele está de volta em 2003, tamanho o interesse que gerou no público.

Vemos violência no cinema, na TV, na vida real, enfim, em todo lugar atualmente. Mas a violência explícita, da forma que é mostrada no filme, com a trilha executada, os movimentos de câmeras e a iluminação não-convencional usadas, acaba por provocar um sentimento totalmente diferente nos espectadores. Não é como se víssemos a morte de mais uma das centenas de vítimas de Arnold Schwarzenegger no cinema. Desta vez, somos realmente jogados na parede: ISSO é a violência, ISSO é um assassinato, ISSO é um estupro.

Agora todos viram, todos sentiram. Alguns não agüentaram, tiveram que sair do cinema. Outros conseguiram continuar, a maioria com a nítida certeza de ter visto cair uma máscara do mundo ocidental: a do herói assassino.

Dá pra entender claramente por que *Irreversível* é tão polêmico. Talvez seja o filme mais angustiante e explicitamente violento já feito. Mas, por outro lado, é o longa que todos os súditos de George W. Bush, em todo o planeta Terra, precisam ver nos dias de hoje.

O avesso da Inglaterra

Por: João Marinho

Coração humano inicia saga de imigrantes ilegais

Depois de *Irreversível* e *Demonlover*, nada mais justo do que resenharmos um outro filme que também traz o submundo e o sexo entre os temas tratados: *Coisas belas e sujas*.

Coisas mostra o avesso da aristocrática Londres e trabalha com o que ocorre nos becos da metrópole. Drogas, sexo, trabalho semi-escravo e xenofobia (aversão aos estrangeiros) aparecem com cores fortes.

A história começa quando um imigrante ilegal encontra um coração humano em uma privada, no hotel em que trabalha à noite. O acontecimento bizarro serve como ponto de partida para contar o dia-a-dia nada fácil de quem vai para a Europa em busca de uma vida melhor e encontra um ambiente hostil e subumano. Mais do que recomendado.

Coisas belas e sujas (Inglaterra, 2002)
Direção: Stephen Frears
Elenco: Audrey Tautou, Chiwetel Ejiofor, Sergi Lopez

Globalização e não-lugar

Por: João Marinho

Filme traz personagens cruéis em trânsito livre

Marc Augé, antropólogo francês, descreveu um dos fenômenos mais pungentes de nosso tempo: a importância dos não-lugares. Em sua teoria, não-lugares são espaços não-identitários e semelhantes que evocam o anonimato, a fluidez e o livre trânsito. São opostos aos lugares no sentido antropológico, que são marcados pela tradição, pela cultura particular, pelas relações sociais, etc. Na prática, diz Augé, nós transitamos entre os dois conceitos, mas os ícones atuais são os não-lugares.

Os não-lugares – aeroportos, rodovias, hotéis, etc. – também são trabalhados em outras áreas do saber, além da filosofia, como no filme francês *Demonlover*

Demonlover é uma empresa que, junto a outra chamada Mangatronics, quer licenciar os animes pornográficos em 3-D produzidos pela TokyoAnime, que irá fundir-se com a Volf.

A negociação é permeada de espionagem corporativa, promovida tanto pela Mangatronics quanto pela Demonlover. No meio do caminho, aparecem personagens amorais e impiedosos, que estão em constante trânsito pelo globo.

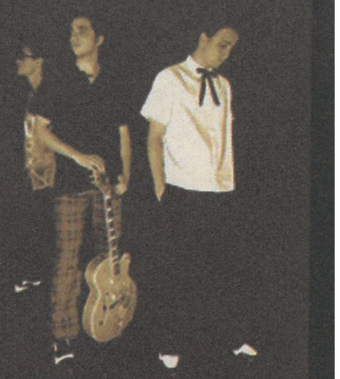
Além disso, estão todos tão fartos de "verem tudo" que cenas de estupro, games violentos, etc. já não causam reação. Qualquer semelhança conosco, ou com a obra de Augé, não é mera coincidência.

Demonlover (França, 2002)
Direção: Olivier Assayas
Elenco: Connie Nielsen, Charles Berling, Chloë Sevigny

Nos tempos da brilhantina

Por: Maurício Martins

Sapatos Bicolores querem invadir São Paulo



Brasília, para variar, está com uma cena musical efervescente. A capital do Brasil da nunca, e o rock por lá está mais aceso do que em muitas das maiores cidades do

Agora é a vez do rockabilly. E uma das principais forças locais, nesse estilo, está querendo expandir seus horizontes para o sul. São os "Sapatos Bicolores", que recentemente estiveram em São Paulo para apresentações. O grupo foi formado em 2001 por André Vasquez, guitarrista nascido no Rio Grande do Sul. Completam a banda o baixista PC e o baterista Caio. Lançaram um EP, chamado "Prafrentex", pelo selo Monstro Discos e começaram a ser notados na cena underground.

O rockabilly do grupo se destaca por não ser nem um pouco puro, pois mistura muito de country, Beatles e influências de bandas como Grafórreia Xilarmônica (como confirma o próprio guitarrista). O show é cheio de energia e muito dançante, sob o comando do front man André.

Aliás, sua guitarra é um show à parte. Fazendo jus ao legado de Brian Setzer (guitarrista e vocal líder dos Stray Cats), o som do seu instrumento nos transporta de volta aos anos 60, e desenha escalas e melodias inesperadas e divertidas.

Mas a banda só está começando, e ainda pode melhorar muito, principalmente se deixar o seu show mais enxuto. No começo de 2004, os Sapatos lançarão seu primeiro disco completo, e com certeza estarão pelo sul para promovê-lo. Força para eles. E que não se deixem levar pelo caminho fácil do sucesso via MTV e afins. Como nos disse André: "o mais importante, bem mais do que ficar famoso, é estar ao alcance dos nossos fãs".

Samba, suor e música eletrônica

Livro conta a história da música eletrônica tupiniquim

Por: Marcelo Barbão

Finalmente, a música eletrônica começa a virar gente grande no nosso País. Depois de conquistar as pistas nacionais, ganhando festivais próprios e cavando espaço nas rádios e TVs, chegou a hora de estudar sua história. Esse é o objetivo do livro *Todo DJ já Sambou*, da jornalista Cláudia Assef, que pesquisou, em apenas quatro meses, a trajetória da música eletrônica, desenvolvida no Brasil a partir dos anos 50.

Claro que o critério aqui de música eletrônica é bastante amplo. A autora começa contando que, nos anos 50, houve a transição dos bailes com orquestra para as festas com vitrolas elétricas – lembrando que a primeira equipe de som chamava-se Orquestra Invisível e se apresentava atrás de uma cortina.

É a descoberta dessa pré-história da música eletrônica que nos faz entender o título do livro. Afinal, nesses bailes cinquentões, a música que rolava era o samba. Até chegar aos DJs e às subdivisões da música eletrônica como encontramos hoje, existiram os famosos anos 70, com suas discotecas e coletâneas de hits que ficaram famosas. Nessa época, grande parte dos artistas e grupos era armação de gravadoras, como Gretchen, Harmony Cats e outros esquecidos pelo tempo.

No Brasil, o quente eram as discos, como Banana Power e Hippopotamus. Até a Globo lançou a novela Dancin'Days na época, que causou escândalo com a cena da dança na qual a Sônia Braga insinuava levemente que ia tirar a calça ou algo assim – coisa que poderia passar na Sessão da Tarde dos dias atuais.

Hoje em dia, o mundo techno é sofisticado. Muitos DJs brasileiros são respeitados internacionalmente, a tradicional MPB começa a se abrir, unindo tambores com picapes, e os festivais/raves se multiplicam pelo País. Nada melhor, portanto, que conhecer como tudo chegou a esse ponto.

Todo DJ já Sambou
Cláudia Assef
Editora Conrad
R$ 25

Guia do CD H4CK3R 13

Confira os principais destaques do sombrio CD da H4CK3R 13

Destaque: *Sentry Firewall CD-ROM 1.5.0*

Segurança sem instalação

Reiniciando uma máquina com o CD desta edição no drive, você irá rodar o Sentry Firewall. Ele é uma distro GNU/Linux baseada no Slackware 9.0 que possui os principais pacotes (confira abaixo) de segurança, e uma performance como nó de servidor e IDS (Intrusion Detection System) que não deixa nada a desejar se comparado com as opções comerciais de mercado. O Sentry não vem com nenhuma interface gráfica, o que garante maior agilidade e leveza para rastrear redes maiores via HTTP, FTP, SFTP ou SCP. Você também não vai encontrar nenhum script para automatizar tarefas de configuração: tudo deve ser feito "na unha". Mas isso não quer dizer que seja difícil deixá-lo perfeitamente adaptado às suas necessidades.

Principais pacotes presentes no Sentry Firewall CD

Snort IDS
Scanlogd
iptables
IProute2
OpenSSH e OpenSSL
Zebra
NMap
net-snmp
Webmin
E daemons para Apache, Sendmail, Squid, Perl e BIND

Requisitos mínimos

Computador com processador x86 Intel ou compatível com drive de CD-ROM
BIOS com suporte ao boot via CD no padrão El Torito
Pelo menos 32MB de memória RAM

Importante

Não esqueça do usuário e senha padrão do sistema:
Usuário: sentry e **Senha**: SENTRY – **Usuário:** root e **Senha:** sentry

*Para obter mais informações sobre as outras versões do Sentry Firewall, acesse o site oficial (*www.sentryfirewall.com*), e para saber mais sobre o processo de configuração, leia em *http://www.sentryfirewall.com/files/howto/*

Categoria: *Registro*

Faxina gratuita

O registro do Windows guarda informações sobre cada arquivo que você cria, move e remove. Isso deveria ser bom para restaurar documentos apagados acidentalmente ou desinstalar de vez programas indesejados. Mas o que acontece é um acúmulo de lixo e informações inúteis que deixam o sistema pior do que já é. Para resolver isso, bastaria usar o Linux, mas também é possível gerenciar e editar os arquivos de registro. Foi por isso que selecionamos softwares que realizam essa importante tarefa – e, o melhor, quase todos são freeware. Confira:

Regmon 6.06 (NT/2000/XP): Monitore o acesso ao registro do Windows. Pode detectar erros e até mesmo a atividade de vírus, trojans e outros programas de códigos maliciosos. Obs.: Apenas para Windows NT/2000 e XP

RegKey Backup 1.0: Faz o backup e recupera chaves e subchaves do Registro do Windows. Mesmo não sendo um editor de registro, é uma ferramenta fácil de usar para recuperar chaves que foram modificadas por programas ou web sites

MV RegClean 3.1: Este utilitário permite que você cheque e/ou remova os itens inválidos encontrados. Todas as remoções realizadas poderão ser restauradas por um arquivo de backup undo*.reg

DiamondCS Registry Prot 2.0: Protetor e monitor do registro do Windows. Faz com que você analise a presença de intrusos tentando alterar seu computador. Mostra em tempo real quais chaves foram incluídas ou modificadas e permite voltar ao original, sem mudanças

Reg Cool 2.408: Férramenta de edição de Registro com interface similar à do Explorer. Na esquerda, existem as chaves de registro baseadas em hierarquia de floresta; na janela à direita, é possível visualizar os valores individuais de cada chave. Possui sistema de busca booleano para localização de valores e chaves específicas. Inclui opção para comparação de registros

Registrar Lite 2.00: Gerenciador de registro do Windows. Pode realizar todas as operações de alteração, verificação e visualização do registro do Windows nas máquinas da rede, faz backups, realiza procuras, entre outras opções. Possui o comando undo para que você não faça estrago nas máquinas. Quando roda em Windows 2000 e NT, permite acesso às opções de segurança e permissões

Win/crypto: Este arquivo de texto explicará como decriptar senhas no Windows 9x armazenadas no registro em .doc, .ascii e formato de palmpilot

NT REG: Sistema de driver para o Linux que entende o formato do registro do Windows NT. Com ele você pode pegar arquivos do Windows NT e montá-los no Linux

Ms Decripter: Decripte passwords do MSN pelo registro

Rm Toolkit: Dá acesso ao registro das propriedades de video, etc

NT Reg Pack: Ajuste o registro do seu Windows NT 4.0 com as configurações sugeridas pela Webtrends Security Analyzer.

Cain: Ferramenta para a recuperação de senhas do Windows 95/98. Recupera senhas de logon, dial-up, entre outras

Chron: Esta ferramenta determinará o nível do serviço de update de todas as máquinas de Windows NT sob domínio do NT

Anna Klean: Aplicação de console para remover o worm Anna Kournikova do registro

Categoria: *Trainers*

Ganhar é bom. Roubar é melhor!

Ok, tem gente que não gosta nem um pouco desta categoria, mas ela é como todas as outras que estão no CD: você pode fazer bom uso dela ou fazer besteira.

Recomendamos que você use os trainers para melhorar suas habilidades no jogo e não sacanear os outros. De qualquer forma, veja a lista completa de trainers e cheaters desta edição:

Halo: Combat Evolved: Munições, health, escudo e flahlight infinitos

Freedom Fighters: Munições, health e carisma infinitos para você sair detonando

Max Payne 2: The Fall of Max Payne: Você terá bullet time, health e munições infinitos, entre outras opções

Mace Griffin: Bounty Hunter: Obtenha munição infinita e o máximo de energia possível

Western Outlaw: Wanted Dead or Alive: Munições infinitas e invulnerabilidades para facilitar a sua jogatina

Warlords 4: Tenha opções especiais, como ganhar mais ouro e mana

Commandos 3: Destination Berlin: Você poderá habilitar opções para deixar o seu personagem com health infinito, invisibilidade, entre outras

Command & Conquer: Generals - Zero Hour: Tenha dinheiro e poderes ilimitados

WarCraft 3 (Mission Unlocker): Deixa você escolher qualquer missão do jogo, mesmo as não disponíveis

Test Drive 6: Este trainer permite que você tenha dinheiro ilimitado no jogo

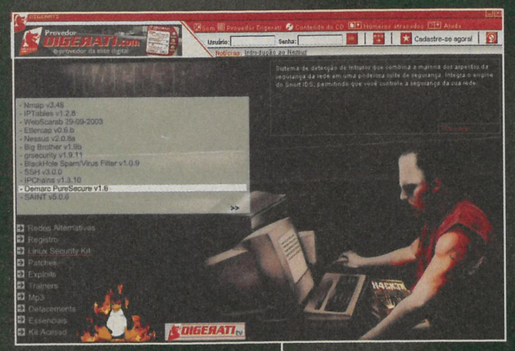
Alone in the Dark 4: Trainer que habilita munições e vidas infinitas e itens para salvar o jogo infinitas vezes

Championship Manager 4: Obtenha mais dinheiro para poder gerenciar melhor o seu time

Hitman 2: Silent Assassin: Com este trainer, você poderá salvar infinitas vezes, além de ter health e munições infinitas, entre outras opções.

Silent Hill 2: Director's Cut: Tenha força infinita, 99 balas para a sua pistola e outras 99 para a sua shotgun

Tony Hawk's Pro Skater 4: Este trainer irá permitir que você multiplique sua pontuação por 100 e remova o tempo do jogo



Categoria: *Linux Security Kit*

Mantenha-se invulnerável

Juntamos as ferramentas de segurança para Linux mais conceituadas em uma só categoria. Dá para dizer que ficou como um kit de primeiro socorros para quem lida com proteção de redes, criptografia e detecção de intrusos. São os essenciais do mundo hacker. Confira alguns dos destaques principais a seguir:

Nmap v3.48: Escaneia redes extensas rapidamente, mas trabalha melhor com hosts únicos. O Nmap utiliza os pacotes IP em caminhos originais para determinar quais hosts estão disponíveis na rede, quais serviços estão oferecendo, qual sistema operacional estão executando, qual tipo de pacote de filtro/firewall estão usando, além de outras opções

IPTables v1.2.8: Firewall em nível de pacotes. Funciona por meio da comparação de regras para saber se um pacote tem ou não permissão para passar. Também pode ser usado para modificar e monitorar o tráfego da rede, fazer NAT (masquerading, source nat e destination nat), redirecionar e marcar pacotes, modificar a prioridade de pacotes que chegam/saem do seu sistema, contar bytes, etc.

Ettercap v0.6.b: Sniffer, interceptador e logger de rede para as LANs. Suporta operação passiva e ativa dos protocolos (mesmo que sejam códigos como SSH e HTTPS), verifica se você está com a LAN trocada ou não, injeta dados para manter a conexão estabelecida, entre outras opções

Nessus v2.0.8ª: Verificador de falhas de segurança. Identifica problemas e sugere soluções ao comando dos cliques de mouse. Checa vulnerabilidades de backdoors e se o sistema está seguro de ataques denial of service ou similares

Snort v2.02: Software capaz de gerar uma análise em tempo real da performance do tráfego e dos pacotes logados no IP da rede. Também pode analisar a performance do protocolo, que pode ser usado para detectar uma variedade de ataques e invasões, como a saúde das portas rastreadas e os ataques CGI

SSH v3.0.0: Programa para logar em outro computador pela rede. Executa comandos em uma máquina remota e move arquivos de uma máquina para outra

IPChains v1.3.10: Esta ferramenta se destina a fazer a filtragem de pacotes que percorrem a rede

chkrootkit v0.41: Detector de presença de rootkits em sistemas baseados em Unix

AirSnort v0.2.2ª: Ferramenta para redes wireless que recupera chaves encriptadas. Opera passivamente, monitorando transmissões e garantindo que os pacotes cheguem ao seu destino

Categoria: *Patches*

Atualizar é questão de sobrevivência

Confira a lista com todos os patches e correções de segurança que selecionamos para o CD desta edição

Debian: Freesweep packages fix buffer overflow
Debian: hztty packages fix buffer overflows
Debian: ipmasq packages fix insecure packet filtering rules
Debian: libmailtools-perl packages fix input validation bug
Debian: New marbles packages fix buffer overflow
Debian: New webfs packages fix buffer overflows
Debian: OpenSSH buffer management fix
Debian: OpenSSL packages correct DoS
Debian: Openssl095 packages fix DoS
Debian: sendmail packages fix buffer overflows
Debian: Tomcat4 packages fix DoS
Red Hat: Apache e mod_ssl packages fix security vulnerabilities
Red Hat: MySQL packages fix vulnerability
Red Hat: SANE packages fix remote vulnerabilities
SuSE: lsh packages fix remote code execution
SuSE: MySQL packages fix remote code execution
SuSE: Openssl packages fix remote denial-of-service
SuSE: sendmail packages fix local/remote privilege escalation
MS Security Bulletin: MS03-039
MS Security Bulletin: MS03-040
MS Security Bulletin: MS03-041
MS Security Bulletin: MS03-042
MS Security Bulletin: MS03-043
MS Security Bulletin: MS03-044
MS Security Bulletin: MS03-045
MS Security Bulletin: MS03-046
MS Security Bulletin: MS03-047

H4CK3R

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

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, Andreza S. Francisco, Andressa Nozue
Colaboradores
Toniclay Andrade Nogueira, Othon Marcelo Nunes Batista, Antonio Marcelo, Piter Punk, Frederico Argolo, Marcos Velasco, Glauco S. Moraes e Fernando Giannacari
Revisão
Elizabeth Paik e Silvia Almeida
Departamento Multimídia
Design e Programação: Alexandre Diniz
Conteúdo: Juliano Barreto, João Henrique e Marcelo Quiñónez
Vídeo: Felipe Madureira
Departamento de Internet
Tarcila Broder, Carlos Sivalli Ignatti e Aleksandro Botelho

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

Mais uma publicação da DIGERATI especialista na comunidade digital digerati.com

Digerati Comunicação e Tecnologia Ltda
Rua Haddock Lobo, 347 – 12º. Andar
CEP 01414-001 Sao 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