GUS
GRUPO DE USUÁRIOS SLACKWARE

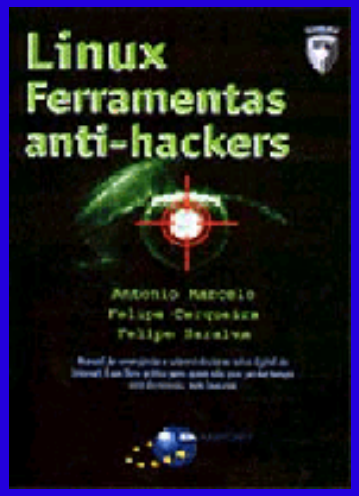
Primeiro Encontro LinuxChix e Slackware Brasil

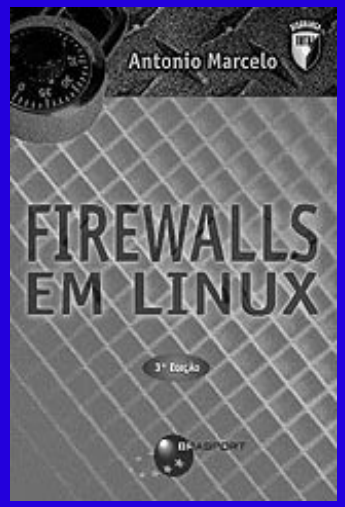
LKM ROOTKITS
Uma Visão Sobre o Assunto

Antonio Marcelo - Projeto IDSKIT
Amarcelo@plebe.com.br

LINUX CHIX .ORG .BR

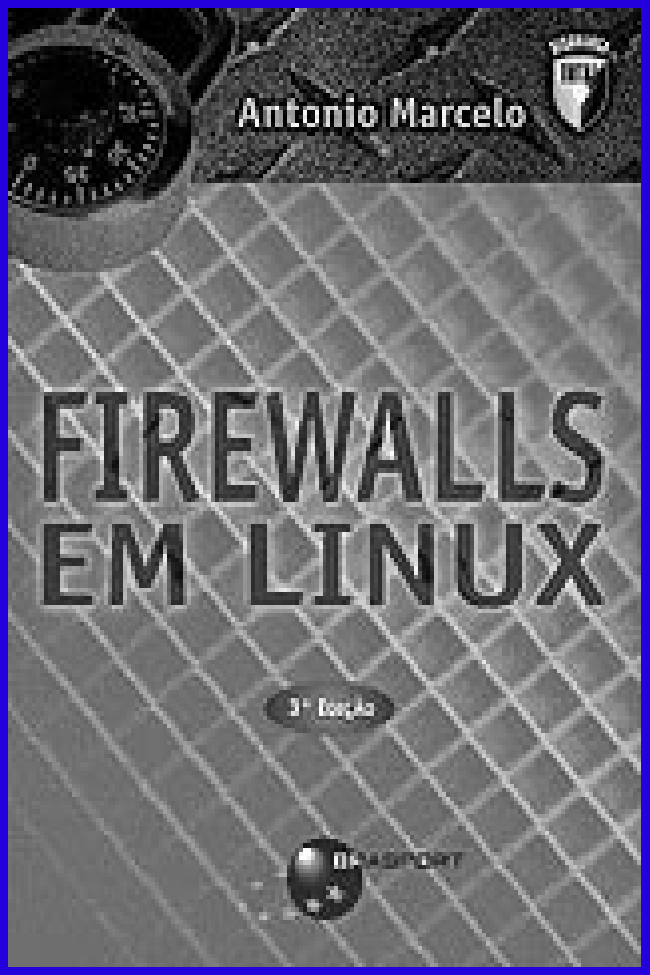
Livros do Publicados pelo Palestrante





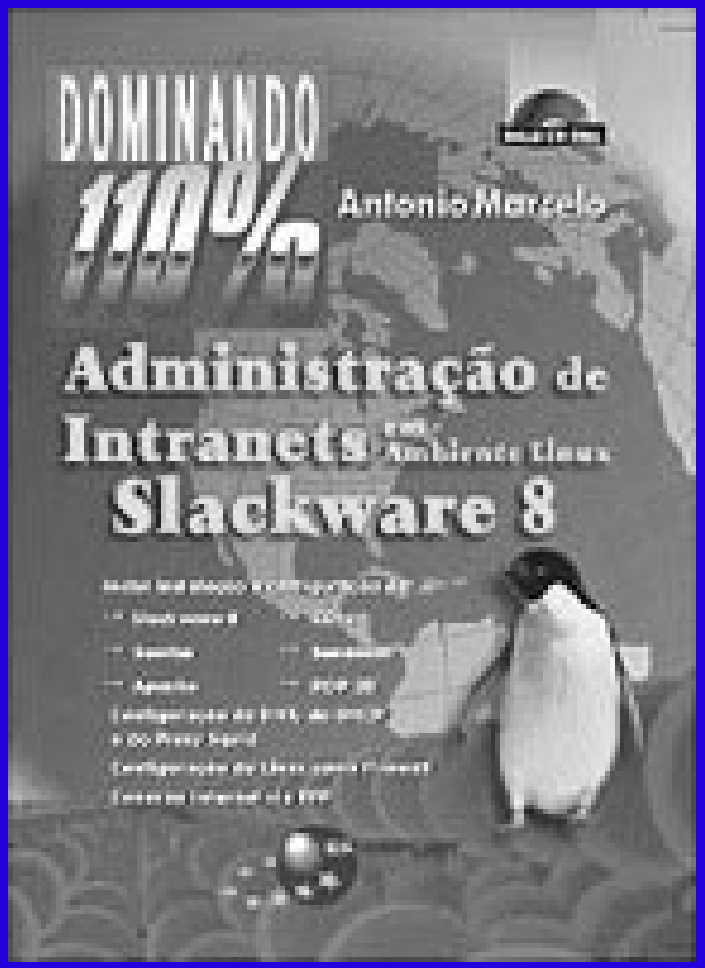
Novo !

Firewalls em Linux
3a. Edição



- Esta terceira edição traz novos recursos para o administrador implementar firewalls em Linux de maneira simples, direta e sem mistérios. É um guia extremamente prático, com muitos exemplos, que vai direto ao cerne da questão, pois a necessidade de um firewall em uma rede ligada à web é cada vez maior.

Administração de Intranets em Ambiente Slackware

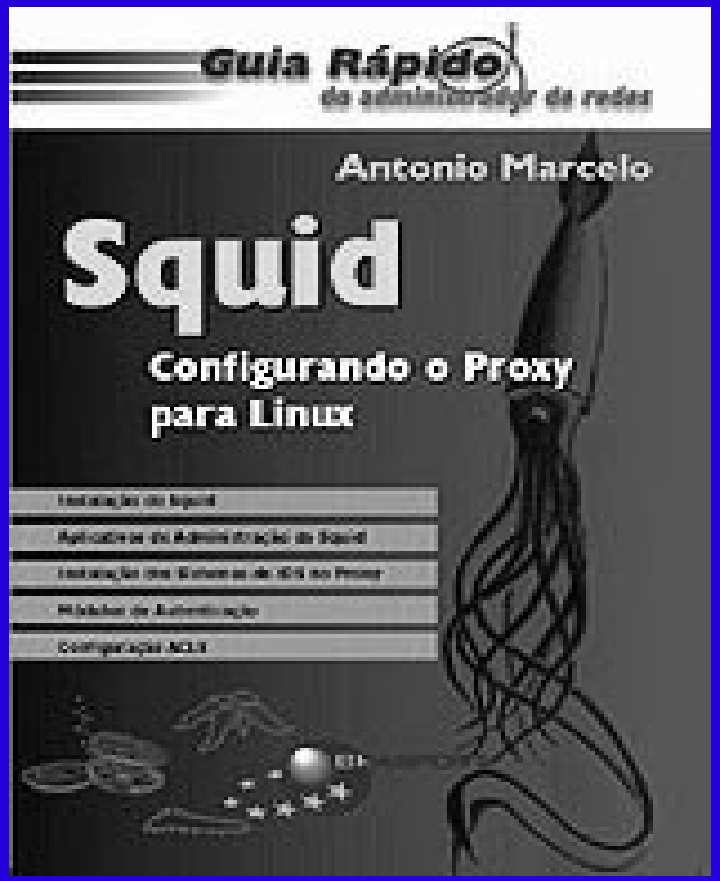


- O objetivo deste livro é servir de guia para a instalação de uma intranet, de forma prática, em pouco tempo e a baixo custo. É voltado para os administradores de rede que pretendem implementar em suas organizações o versátil ambiente operacional Linux.

APACHE

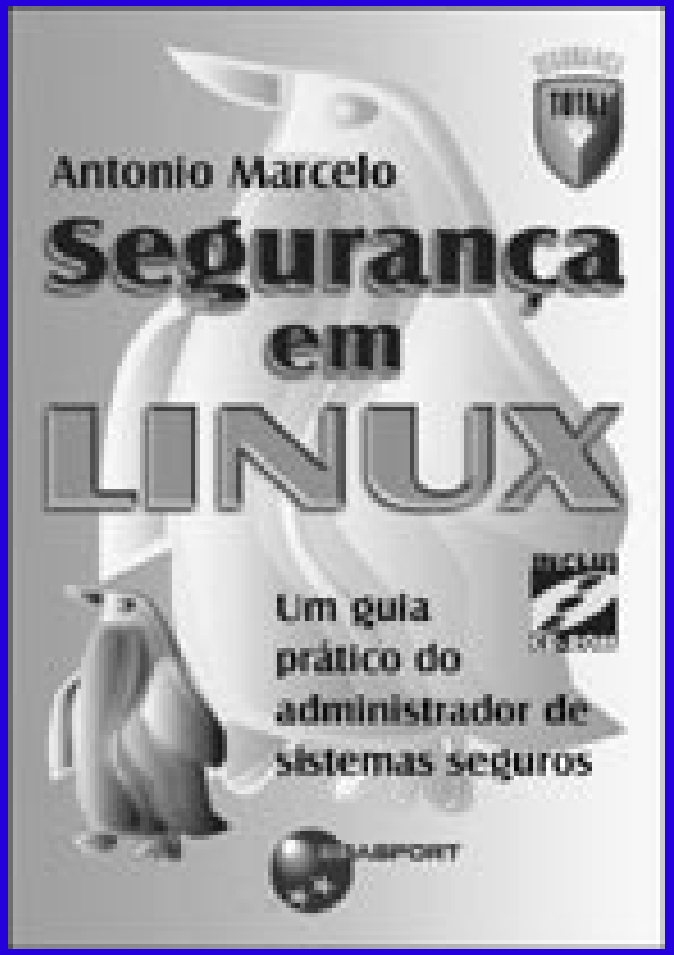
- Inaugurando a série Guia Rápido do Administrador de Redes, este livro apresenta o servidor web mais utilizado na Internet. O objetivo é mostrar aos administradores de rede como configurar o Apache de maneira simples em ambiente Linux.

SQUID



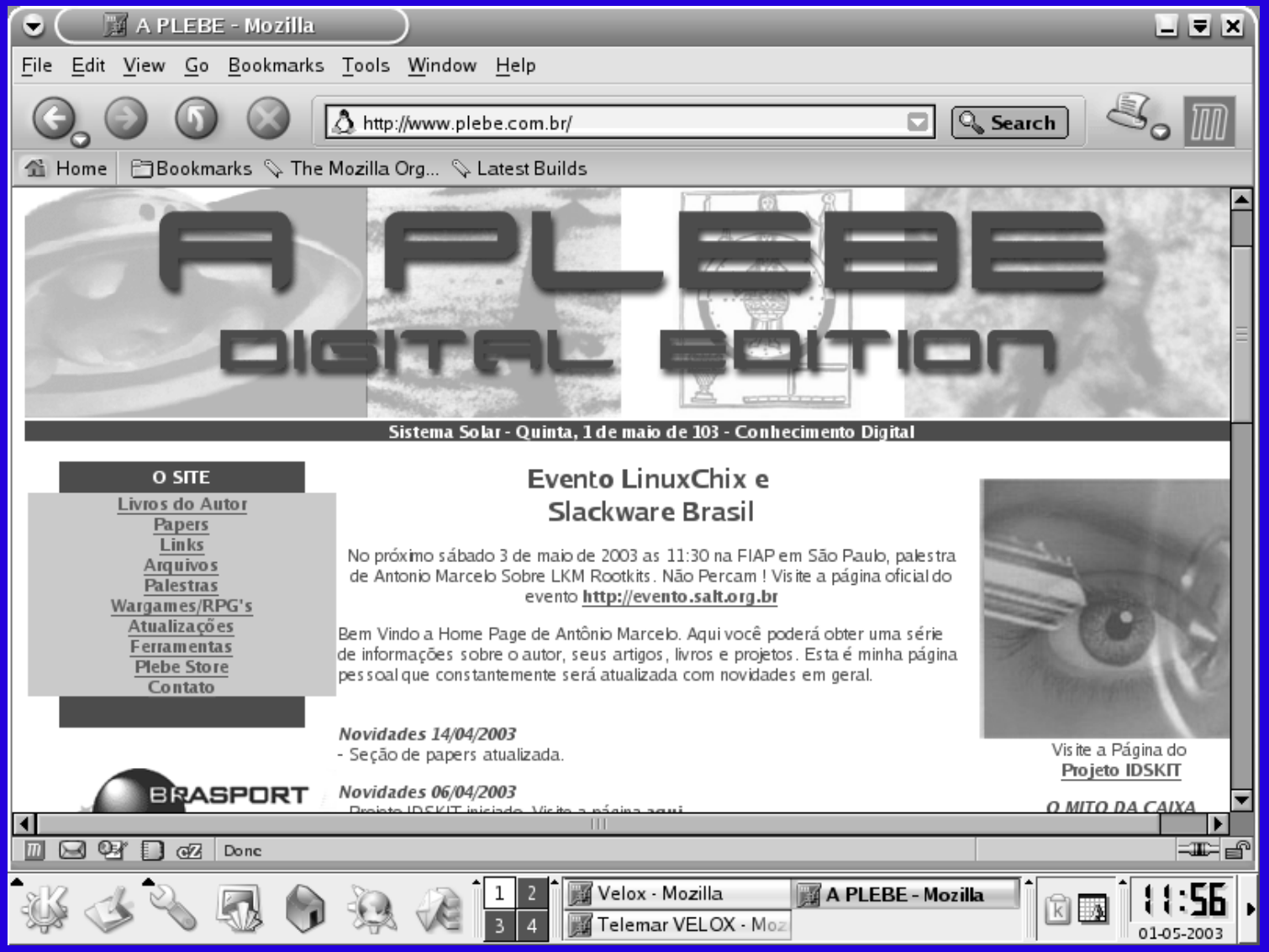
- Este é o segundo livro da série Guia Rápido do Administrador de Redes e tem como foco o Squid, o proxy mais utilizado na Internet e que consegue atender as mais diversas necessidades, seja em casa ou em ambientes de trabalho.

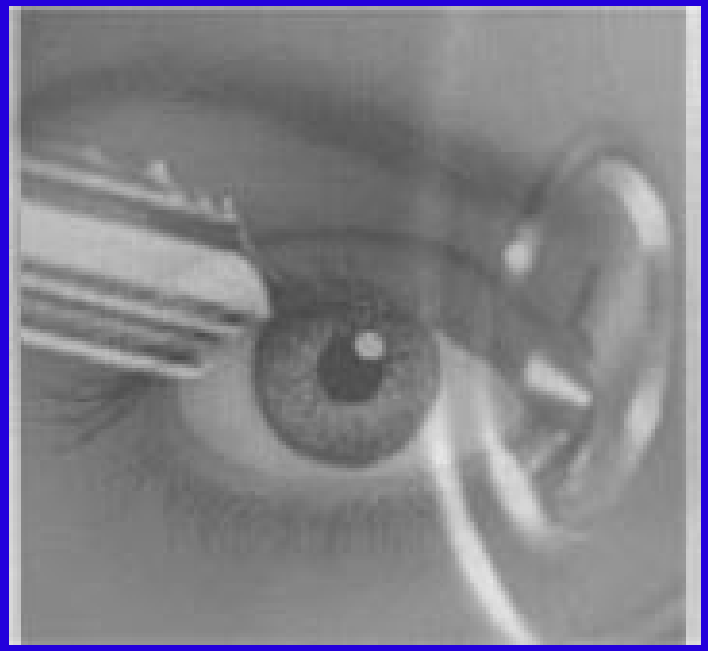
Segurança em Linux



- Novo livro da série Segurança Total que tem como objetivos mostrar uma visão prática para o Administrador de Servidores Linux. Cobrirá assuntos como : Firewalls, LSM, IDS, etc.
  Breve nas livrarias !

Página do Palestrante
http://www.plebe.com.br





LKM ROOTKITS
Uma Visão Sobre o Assunto

O que é um sistema seguro ?

- Podemos definir um sistema seguro como aquele que garante três necessidades básicas :
  - Integridade;
  - Confidencialidade;
  - Disponibilidade.

O que é uma Intrusão ?

- *Podemos definir como intrusão a ação que compromete os três princípios básicos da segurança : integridade, confidencialidade e disponibilidade.*

Taxonomia Básica de Ataques

- Scanners: tentativas de varreduras para descobertas de portas e serviços vulneráveis;
- Exploradores de vulnerabilidades : buffer overflows, stack overflows, heap overflows, integer overflows, format strings, scripts inseguros, vírus, worms, rootkits, etc.
- Hacking from Inside : ataques vindos dos próprios membros da estrutura interna da rede;

Taxonomia do Rootkit

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

Gerações de Rootkits

- Primeira Geração – GEN-I (LRK-5)
- Segunda Geração – GEN II (Knark)
- Terceira Geração – GEN III (Suckit)

Taxonomia GEN – I

- Nesta primeira geração os rootkits eram nada mais nada menos que programas de sistema modificados (trojans) ;
- Programas atacados (exemplos) :
  - Ifconfig;
  - Login;
  - inetd.

Profilaxia parao GEN-I

- Programas de auditoria de arquivos;
- Programa de auditoria de conexões;
- Programas de auditoria dos sistemas;
- Exemplos :
  - Tripwire;
  - Lstat.

GEN-II : LKM Rootkits

- Nesta segunda geração os rootkits deixaram de lado a preocupação de modificar programas do sistema e começaram a modificar atarvés de módulos de kernel (LKMs) as system calls do sistema;

Conceitos Básicos Importantes

" Sistema Operacional é a camada de software que cuida dos aspectos técnicos da operação de um computador. "
(Burges - A Short Introduction to Operating Systems)

O que é uma Syscall

- Qualquer tarefa importante de um sistema operacional envolve sempre uma grande porção de código de baixo nível. Por exemplo se quisermos criar um diretório em um disco rígido, teríamos de criar uam série de rotinas em Assembly ou em C ANSI para acessar os dispositivos e promover o devido controle no mesmo.
- Para evitar esta tarefa hercúlea, os projetistas de sistemas já criaram uma série de funções, ou melhor rotinas de baixo nível, que executam estas operações. Estas rotinas nós chamamos de systemcalls. Estas systemcalls interagem com o sistema e dizem exatamente o que ele deve fazer em uma determinada operação específica.

Uma chamada de Syscall

```
Mov    %ebx,%edx
mov   0x4(%esp,1),%ebx
mov    $0x1,%eax
int    $0x80
```

Loadable Kernel Modules

- Um LKM, ou melhor um módulo de kernel carregável (desculpem plea tradução), é um recurso que o kernel do Linux utiliza para aumentar suas funcionalidades. Com estes módulos é possível de maneira dinâmica carregar por exemplo módulos de uma placa de rede.

Taxonomia do GEN II

- Corrupção de um LKM para alteração de systema calls, assim modificando o sistema
- Permite ocultação de processos, arquivos, diretórios, modificação do /proc, etc.

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

extern void* sys_call_table[];

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

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

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

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

}
```

Profilaxia GEN II

- Compilação do Kernel sem suporte a LKM;
- Programas de auditoria do System.map;
- Auditoria de arquivos
- Programas exemplo : chkrootkit

GEN III – Private Syscall Rootkits

"/dev/kmem is your friend"

sd & devik

O KMEM

O linux possui um dispositivo conhecido como kmem (/dev/kmem), que possui o diretio de escrita e leitura somente pelo root. Este dispositivo abstrato tem como função traduzir a memoria virtual utilizada pelo kernel para a memória real (/dev/mem), ou seja o mesmo faz o endereçamento da memória real+swap

Taxonomia do GEN III

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

Profilaxia GEN III

- Proteçaão do kmem contra escrita;
- Programas de análise de execução de syscalls (auditor de intsruções)
- Programas de auditoria.

Conclusões

- GEN IV;
- Rumos Futuros;
- Técnicas de defesa importantes;
- Espaço aberto.