



Marta Vuelma  
Alfasys Tecnologia

# Hardening Linux Servers

# Quem?

Analista de Projetos na Alfasys Tecnologia

Atua na área de TI desde 1993

Experiência em treinamento em várias áreas para os mais diversos públicos desde 1995

Trabalha com Linux desde 2001

Possui Certificação LPIC-3

Graduanda em Segurança da Informação

Palestrante em eventos de âmbito nacional e regional

Membro atuante do Ubuntu-BR e ASL

# Agenda

- Apresentando fatos
- Obstáculos para a segurança
- O que é hardening
- Técnicas de hardening
- Perguntas

22/06/2011 19h19 - Atualizado em 22/06/2011 19h33

# Ataque hacker foi o maior já sofrido por sites do governo na internet

Servidores na Itália teriam sido ponto de partida para ação de grupo. LulzSecBrazil reivindicou autoria de ataque de 'negação de serviço'.

Do G1, em São Paulo

imprimir



O ataque hacker às páginas da Presidência da República, Portal Brasil e da Receita na madrugada desta quarta-feira (22) foi o maior já sofrido pela rede de computadores do governo brasileiro. De acordo com o Serviço Federal de Processamento de Dados (Serpro), o ataque - que não causou danos às informações disponíveis nas páginas - partiu de servidores localizados na Itália.

Para derrubar os sites, os hackers utilizaram sistemas que faziam múltiplas tentativas de acesso ao mesmo tempo, técnica batizada

PUBLICIDADE



Clique e faça uma busca na sua área:

- Administração
- Comercial e Vendas
- Educação
- Engenharia

Mais áreas

## Tecnologia e Games

- 30 JUN 07:00 **Tira-dúvidas: software do Windows no Mac e segurança de apps em Java**
- 07:00 **Miguel Nicoelis apresenta seu primeiro livro em São Paulo**
- 00:20 **Hackers atacam rede de comunicação da al-Qaeda**
- 29 JUN 20:01 **Assuntos do dia no Twitter - quarta-feira, 29/6/2011**



## TECNOLOGIA

COMPARTILHAR: [Facebook] [Twitter] [Google+] [Email] [Print] [Comentar] [Curtir] 16

# Funcionários da Petrobras confirmam dados obtidos de hackers

comentários 37

25 de junho de 2011 • 21h26 • atualizado às 21h30

NOTÍCIA

JORGE LOURENÇO

AAA [Print]

Funcionários da Petrobras confirmaram ao *Jornal do Brasil* que os dados obtidos pela reportagem, cedidos pela LulzSec Brasil, são reais. Os arquivos, divulgados na manhã deste sábado, revelam o nome completo, matrículas, chaves do sistema, endereços de e-mail e dados do servidor de 46 mil funcionários da empresa.

A assessoria de imprensa da Petrobras manteve a posição de que os servidores da empresa não foram comprometidos por qualquer invasão hacker e que vai investigar como esses dados vazaram. O arquivo da LulzSec mostra, inclusive, supostos dados pessoais de membros da alta cúpula da Petrobras, como do presidente José Sergio Gabrielli de Azevedo, do diretor de abastecimento, Paulo Roberto Costa e da diretora de Gás e Energia, Maria das Graças Foster.

Os funcionários com os quais o *Jornal do Brasil* conversou pediram para manter seus nomes em sigilo, mas lamentaram o fato de que a empresa não fez qualquer comunicado a respeito do vazamento de dados pessoais.

[mais notícias de internet »](#)

[JORNAL DO BRASIL](#)

[Jornal do Brasil](#)

## últimas

NOTÍCIAS FOTOS VÍDEOS

09h12 Justiça ordena registro de IP de perfis do Orkut pelo Google

06h31 Samsung quer proibir importação de produtos Apple nos EUA

04h36 Jornal: hacker violou e-mail de Dilma durante a campanha de 2010

[mais notícias »](#)



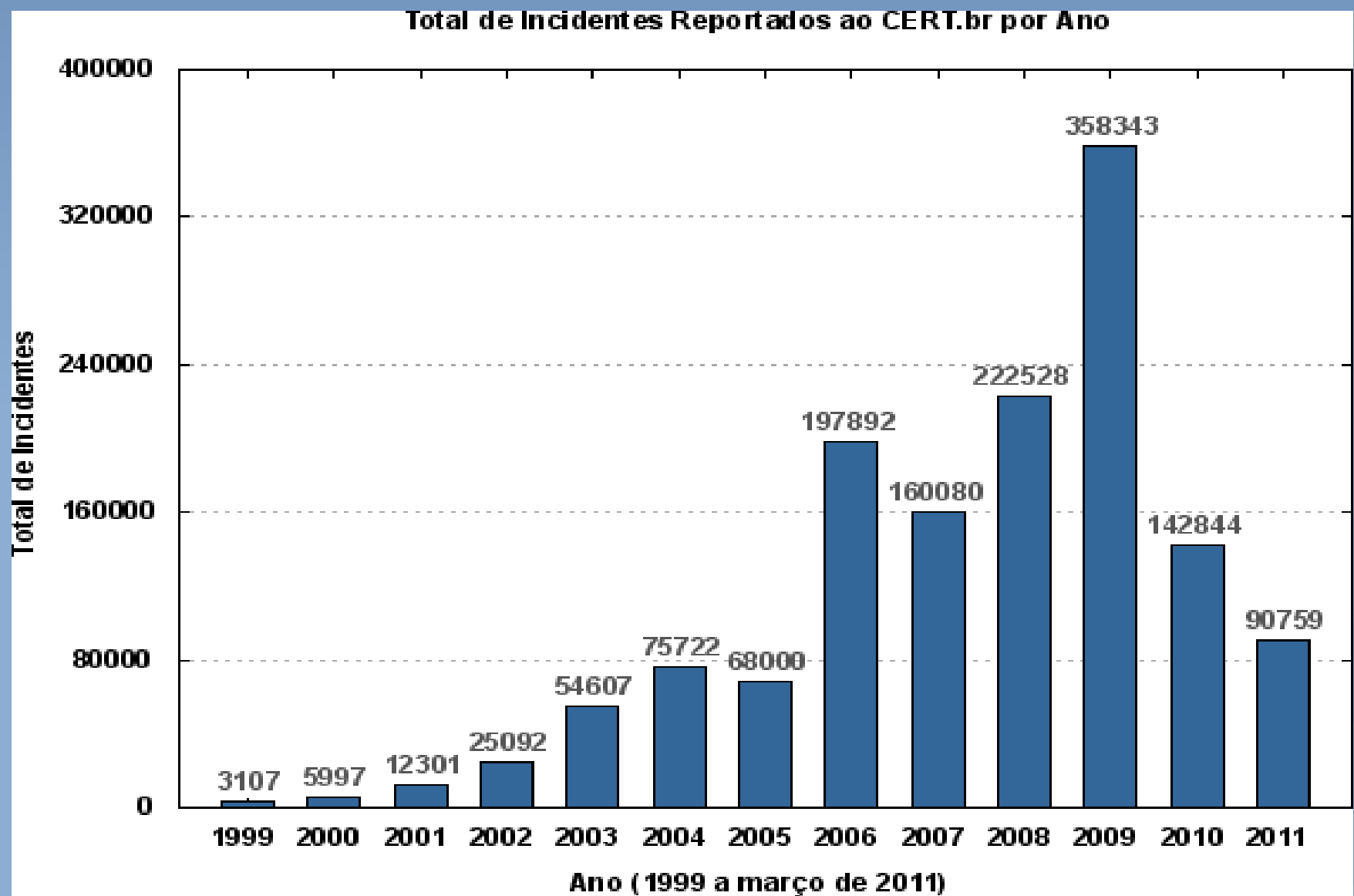
# Alguns fatos sobre segurança

- Os principais tipos de ataques reportados ao CERT.br e à outras instituições ocupadas em criar estatísticas sobre segurança são:
  - **SPAM** (só no primeiro trimestre de 2010, o número de registros ultrapassou os 10 milhões.
  - **Phishing** (aumento de 61% em um ano)
  - 30% dos ataques resultam em perda de dados

# Alguns fatos sobre segurança (cont.)

- A maioria destes ataques exploram vulnerabilidades conhecidas de servidores e estão sendo usados para atacar outros servidores.
- **Somente um firewall convencional** (stateful firewall) **NÃO** consegue proteger um servidor contra este tipo de ataque.

# Números



# Obstáculos para a segurança

- Segurança requer **planejamento**;
- Segurança requer **monitoramento permanente**
- Segurança requer **atualização constante**, tanto das ferramentas em uso quanto dos profissionais envolvidos.
- Já existem muitos padrões internacionais de segurança (como Sarbanes-Oxley, ISO, etc.) **MAS** a maioria das organizações possui mecanismos pobres de segurança e ausência quase que total de políticas e cultura de segurança.

# Obstáculos para a segurança (cont.)

- Os **usuários não estão preparados** para uso adequado dos recursos;
- Atualmente, o objetivo primário é *compartilhar e não proteger*;
- A segurança é um **processo permanente**. Não existem soluções do tipo “Instale-Esqueça”
- Muitos profissionais utilizam-se de **falsos conceitos de segurança** para montar suas redes.

# O que é hardening?

- É um processo utilizado em diversos níveis de recursos em servidores para proporcionar segurança mais completa e efetiva.
- A partir do momento em que conectamos um equipamento em uma rede, ele não está mais seguro. Isso inclui desde o processo de instalação até a liberação para produção.
- A ampla oferta de ferramentas para hardening de servidores, permite ao administrador montar o conjunto ideal de ferramentas para o seu cenário.

# O que é hardening? (cont.)

- As ferramentas disponíveis hoje para Linux oferecem um nível de segurança muito elevado para servidores e estações.
- A utilização das técnicas de hardening, somada a uma política de monitoramento e atualização constante, garante um nível de proteção muito alto.
- O objetivo do hardening de servidores é manter os intrusos o mais longe possível pelo maior período de tempo com múltiplas camadas de segurança.

# Nível 0

- A segurança de um sistema começa na instalação.
- Um servidor só pode ser considerado seguro se o processo de instalação utilizou-se das seguintes técnicas de hardening:
  - Fontes de instalação confiáveis e verificados com a chave GPG do desenvolvedor;
  - Após a instalação, deve ser gerada uma base de informações sobre o sistema de arquivos que será utilizada como matriz para detecção de alteração dos binários e arquivos de configuração após a conexão do servidor no ambiente de risco.

# Nível 0 (cont.)

- Ferramentas como o Tripwire\* ou AIDE oferecem o nível de controle necessário para monitorar alterações no sistema de arquivos.

```
aide --check.
```

```
AIDE found differences between database and filesystem!!
```

```
Start timestamp: 2010-01-06 14:41:17
```

```
Summary:
```

```
Total number of files=4145,added files=0,removed  
files=0,changed files=1
```

```
Changed files:
```

```
changed:/etc/hosts
```

```
Detailed information about changes:
```

```
File: /etc/hosts
```

```
Permissions: -rw-r--r-- , -rwxr-xr-x
```

# Hardening para o SO

- ✓ Tudo que não é explicitamente permitido deve ser proibido.
- ✓ **Não esqueça o básico:**
  - ✓ Troque as senhas default de serviços;
  - ✓ Use senhas complexas;
  - ✓ Desinstale ou desabilite software desnecessário;
  - ✓ Mantenha o SO sempre atualizado;
  - ✓ Documente a instalação para permitir uma recuperação rápida em caso de falhas.

# Hardening para o SO (cont.)

- ✓ Apague contas de usuários não usadas e restrinja o acesso de contas do sistema (`nobody`, `guest` e qualquer outra conta usada pelo sistema deve ter `/bin/false` como default shell no arquivo `/etc/passwd`);
- ✓ Mantenha os logs habilitados e verifique-os periodicamente.
- ✓ Utilize preferencialmente um servidor de logs para armazenar os registros do servidor e mantê-los a salvo de invasores (`rsyslog` é uma das melhores opções pois utiliza `ssl`)

# Hardening para o SO (cont.)

- Utilize ferramentas para verificar se o servidor está realmente seguro antes de colocá-lo em produção (scanners de porta – nmap, por exemplo, sniffers – tcpdump ou wireshark, entre muitos outros);  
`nmap -p0- -v -A -T4 host`
- Faça o download de pacotes de software de fontes confiáveis e verifique com a chave GPG fornecida pelo desenvolvedor.  
`rpm --checksig nome_pacote`

# Hardening para o sistema de arquivos

- Em ambientes críticos, isole os arquivos do sistema em partições somente leitura, o que reduz muito o risco de comprometimento:

`/bin, /lib, /sbin, /usr` - somente leitura

`/var, /usr/var, /home` - escrita

`/opt, /usr/local` - somente leitura

`/etc, /usr/local/etc` - escrita

Todo o resto (/) - somente leitura

- Considerar a necessidade de planejamento de atualizações para este caso.

# Hardening para o sistema de arquivos (cont.)

- Certifique-se que não existem arquivos com SUID, SGID ou sem proprietário:

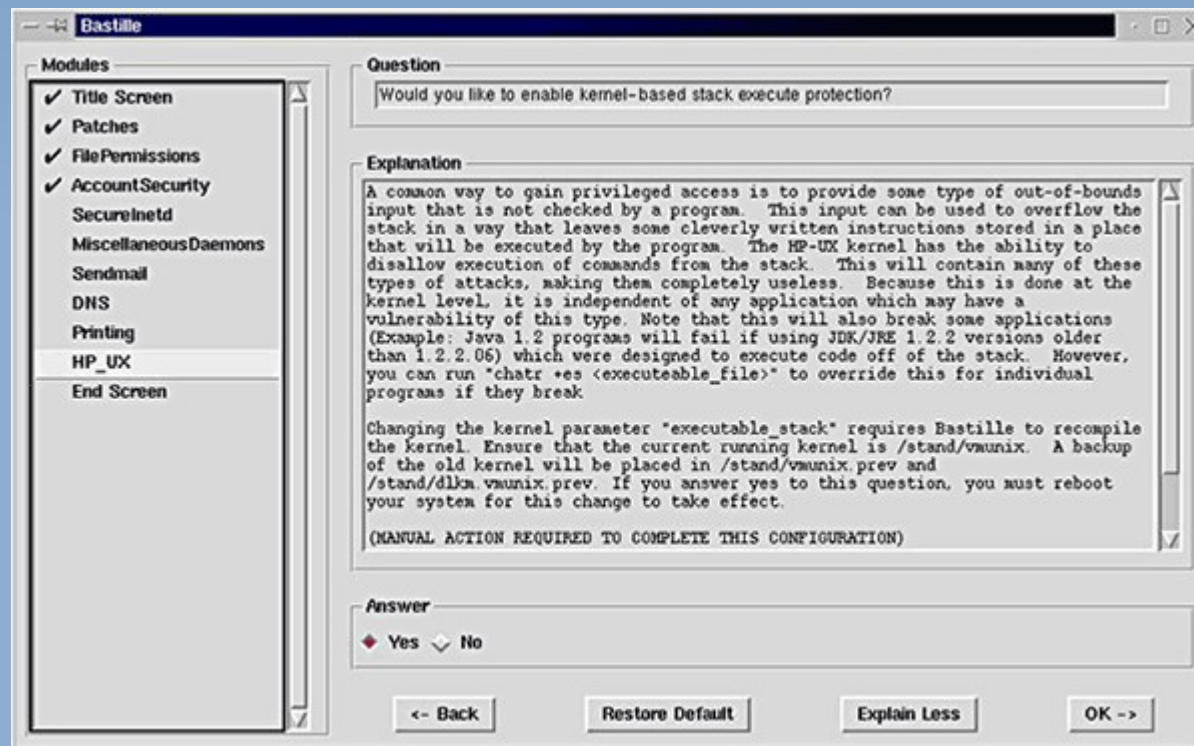
```
find / \( -perm -004000 -o -perm -002000 \) -type  
f -print
```

```
find / -nouser
```

```
find / -nogroup
```

# Ferramentas de conformidade

- Após todos os ajustes requeridos para o SO e sistema de arquivos, deve ser aplicada uma ferramenta que avalie o estado atual em conformidade com a expectativa de segurança. A figura mostra uma tela do Bastille.



# Hardening para rede

- O login remoto do root e de outros usuários privilegiados deve ser desabilitado: configure e utilize o sudo;
- Configure cada servidor com o seu próprio firewall (filtro de pacotes, stateful firewall e firewall de aplicação);
- Um firewall de aplicação permite suprir a carência deixada pelos firewalls stateful que não conseguem avaliar além do binômio protocolo/porta (o netfilter pode utilizar o patch I7-filter)

# Hardening para rede (cont.)

- Feche todas as portas abertas que não estão sendo usadas e monitore-as periodicamente.

```
netstat -lut
```

- Todos os serviços publicados devem ser executados em ambiente chroot.
- Sempre que possível, restrinja o número de hosts que acessam os serviços públicos.
- Utilize uma DMZ para isolar servidores que precisam ter serviços na Internet.

# Hardening para rede (cont.)

- Monitore os logins no servidor com alertas no momento em que eles são realizados. A possibilidade de não perceber um comprometimento em um servidor que não é acessado frequentemente é muito grande.
- Inclua a seguinte linha no bashrc do sistema:

```
echo 'Login efetuado' `hostname` `date`  
`who` | mail -s "Login efetuado  
`hostname` `who | awk '{print $5}'`"  
suporte@dominio
```

# Gerenciamento e continuidade

- A complexidade dos serviços e o número de itens que precisam ser monitorados exige ferramentas específicas que colem informações e gerenciem alertas como:
  - Nagios
  - Shinken
  - Zabbix (entre outros)
- Não existe segurança sem plano de contingência e recuperação. Para isto, documentação e backup são cruciais.

# Referências

- [www.isc.org](http://www.isc.org)
- [www.cgi.br](http://www.cgi.br)
- [www.cetic.br](http://www.cetic.br)
- [www.antispam.br](http://www.antispam.br)
- [www.cert.br](http://www.cert.br)
- [www.websense.com](http://www.websense.com)
- [www.antiphishing.org](http://www.antiphishing.org)
- [www.netcraft.com](http://www.netcraft.com)

# Contato

- [marta.vuelma@gmail.com](mailto:marta.vuelma@gmail.com)
- [marta@alfasys.com.br](mailto:marta@alfasys.com.br)
- [www.alfasys.com.br](http://www.alfasys.com.br)
- [martavuelma.wordpress.com](http://martavuelma.wordpress.com)

# Perguntas



**Obrigada!**

The background features a light blue gradient with several overlapping, semi-transparent blue squares of various sizes and orientations, creating a modern, abstract design.