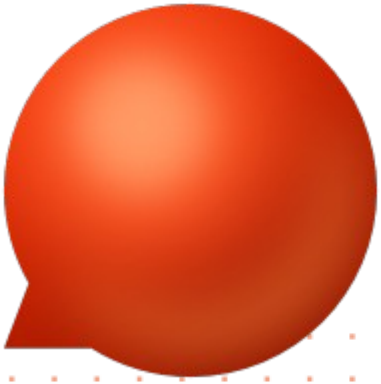
ubuntu



Segurança e riscos no Ubuntu Server

Autor:
Aprigio Simoes
aprigio@linuxstudent.com.br
http://www.aprigiosimoes.com.br

ubuntu-br
Comunidade Ubuntu Brasil

ubuntu

Bem-vindo ao Linux
Bem-vindo ao poder!

ubuntu-br
Comunidade Ubuntu Brasil

Aprígio Simões

ubuntu®

- Membro da Comunidade Ubuntu Brasil
- Líder do time regional Ubuntu BR RJ
- Instrutor e consultor UNIX e Linux
- Trabalho com TI a 14 anos.

Twitter:
@aprigiosimoes

Facebook:
fb.com/aprigiosimoes

IRC:
aprigio on irc.freenode.net

Google+:
gplus.to/aprigiosimoes

ubuntu-br
Comunidade Ubuntu Brasil

O que vamos ver

ubuntu®

- Introdução
- Ubuntu Server no seu ambiente de TI
- O custo de hardening para Windows e Linux
- Analise e correções de não-conformidades
- Boas práticas e o conceitos de segurança

ubuntu-br
Comunidade Ubuntu Brasil

Em uma galaxia distante ...

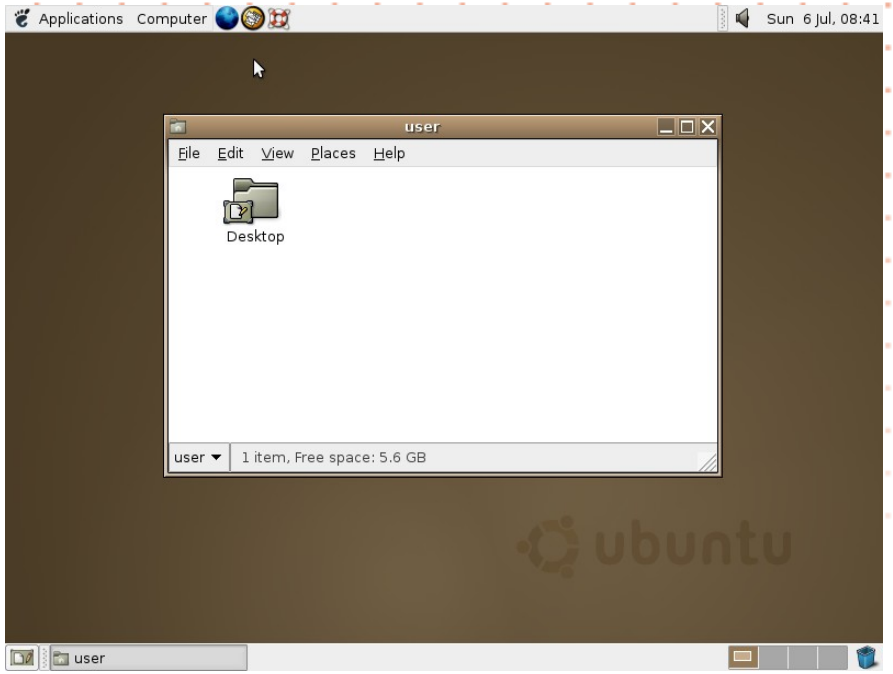
ubuntu®

- Em 1998 a Conectiva lança a versão 2 do seu sistema com o codnome de “Marumbi”, vendido em caixas em diversas lojas do pais, acompanhava um manual e o CD de instalação.
- Foi implementado pela Red Hat no Linux o sndconfig que insenta a compilação do kernel 2.0 para o sistema reconhecer a placa de som, basta selecionar a placa de som, editar o valor de entrada e saida, IRQ e os canais DMA. Em seguinda, será carregado o sample.au e você ouvirá a voz do Linus Torvalds pronunciando o nome “Linux” corretamente. SE, tudo der certo,o módulo sound.o estarão escritos no arquivo /etc/conf.modules e o seu som funcionará corretamente.

Em uma galaxia distante ...

ubuntu

- Em 26 de outubro de 2004 a Canonical lança o Ubuntu 4.10 com o nome de Warty Warthog, baseado na distribuição Debian Sid e nos seus repositórios. O seu suporte foi até 30 de abril/2006. A imagem acompanhava o Gaim 1.0, GIMP 2.0, GNOME 2.08, Mozilla Firefox 0.9, and OpenOffice.org 1.1.x, MySQL 4.0, PHP 4.3, Python 2.3 e kernel 2.6.8 com XFree86 4.3.



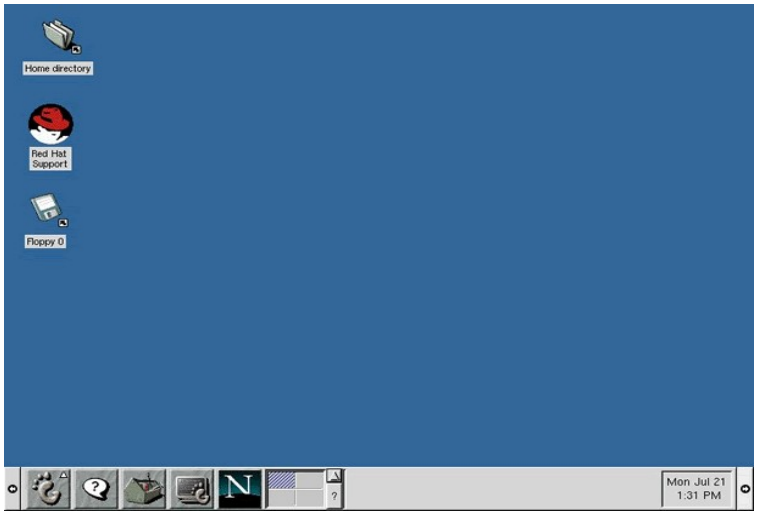
ubuntu-br
Comunidade Ubuntu Brasil

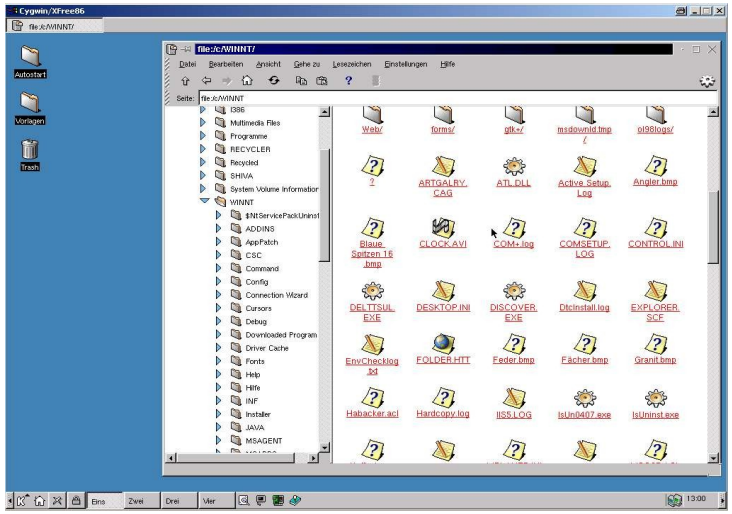
Você lembra?

- Em 12 de julho de 1998 foi anunciado o KDE 1.0 "Um Window Manager Integrado para sistemas operacionais Unix/Linux com a seguinte mensagem:

  “Nós estamos felizes em anunciar a disponibilidade da versão 1.0 do Ambiente de Trabalho K"

- O projeto GNOME foi criado em agosto de 1997 pelos mexicanos Miguel de Icaza e Federico Mena Quintero, como uma resposta ao Windows 95 e com lançamento para Linux em 1999 para Linux e BSD.





ubuntu-br
Comunidade Ubuntu Brasil

Mas e a segurança da sua distribuição,
você tem feito?

O mundo em 1988

ubuntu®

- **Morris Worm Virus**

  O primeiro worm que atraiu grande atenção foi o Morris Worm, escrito por Robert T. Morris Jr no Laboratório de Inteligência artificial do MIT. Ele foi iniciado em 2 de novembro de 1988, e rapidamente infectou um grande número de computadores pela Internet. Ele se propagou através de uma série de erros no BSD Unix e seus similares. Morris foi condenado a prestar 400 horas de serviços à comunidade e pagar uma multa de US$10.000

O mundo em 2013

ubuntu®

- **Vulnerabilidade no Kernel Linux**

  um bug que esteve presente entre as versões 2.6.37 e 3.9 foi corrigido já há algum tempo, mas não era considerado uma falha de segurança - só que agora foi demonstrado (via um exploit) que o mesmo bug permite que um usuário local alcance privilégio de root.

- **Linux/Cdorked**

  Atacantes estão utilizando o novo backdoor, para substituir o binário httpd ou apache2 do servidor por um outro, permitindo abrir um shell reverso na máquina ativado por uma requisição HTTP do tipo GET ao servidor e indicando onde o host deve se conectar para abrir o shell, permitindo controle remoto e total do servidor pelo atacante. O ESET também descreveu como o malware usa um segmento de memória compartilhado de 6 MB, permitindo acesso a leitura e escrita para todos os usuários neste segmento de memória, além de redirecionar requisições de clientes que queriam acessar o site para outras páginas que vão usar o blackhole.

Grandes problemas de segurança

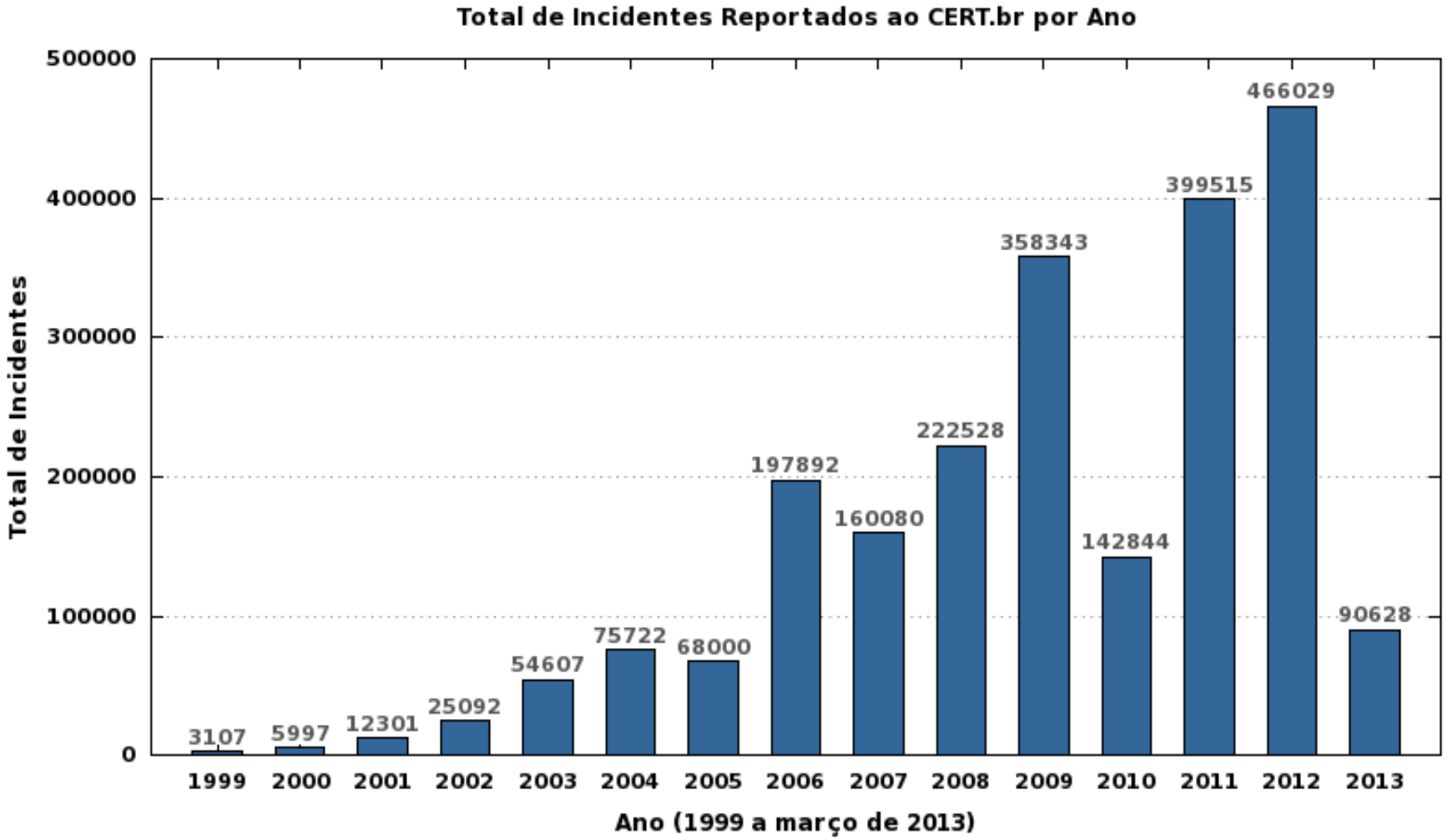
ubuntu®

- **Engenharia social**
- **Exploits**
- **SQL Injections**
- **DDoS (Distributed Denial of Service)**
- **Phishing**
- **Overflows de buffer**
- **Cross-site Scripting**
- **Spyware**
- **Cavalos de Troia**
- **Erros de configuração**

Estatísticas 2013

ubuntu

NIC BR Security Office (NBSO) - Estatísticas

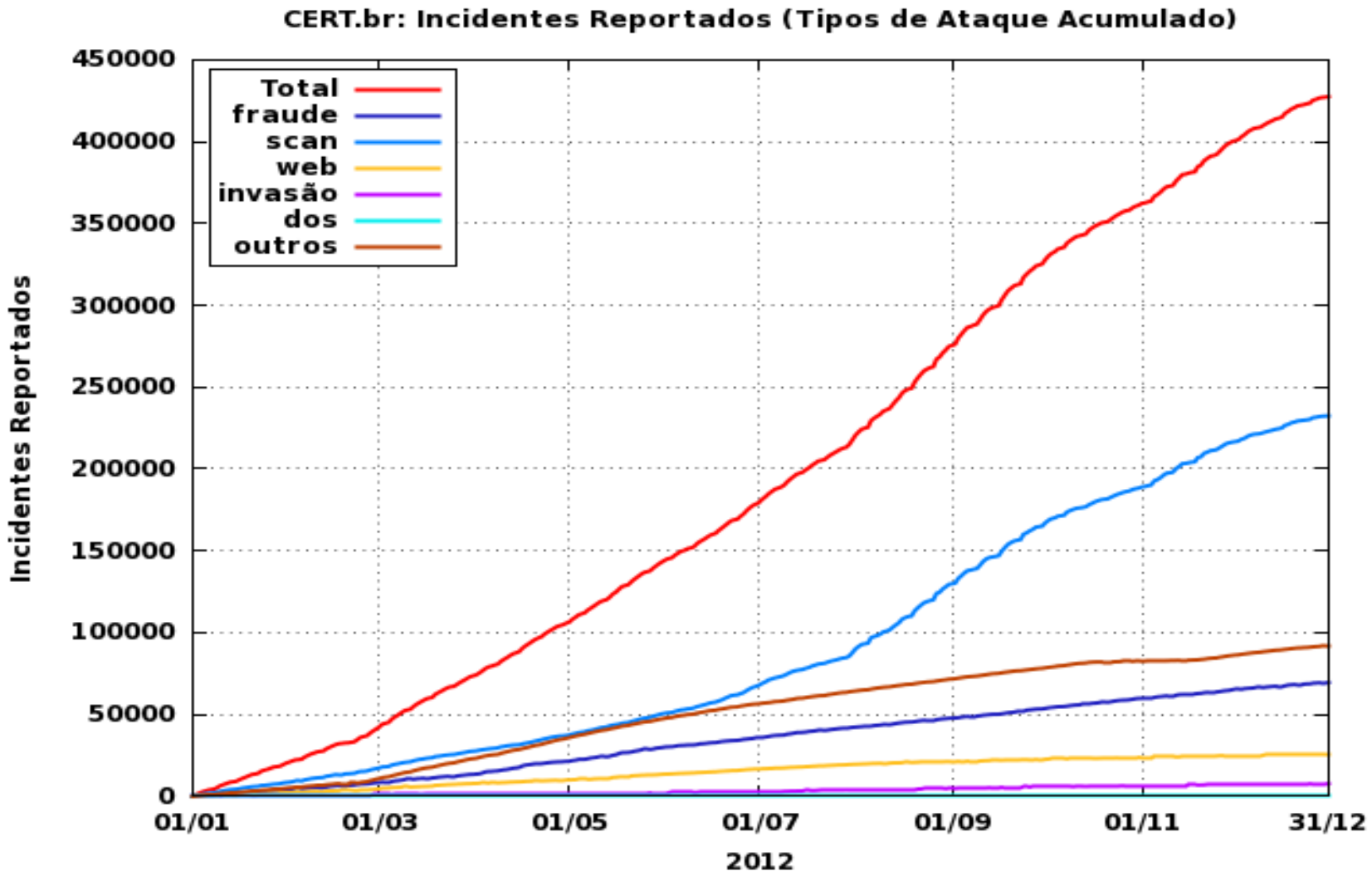


ubuntu-br
Comunidade Ubuntu Brasil

Estatísticas 2012

ubuntu®

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2012



ubuntu-br
Comunidade Ubuntu Brasil

ubuntu

Ubuntu Server

ubuntu-br
Comunidade Ubuntu Brasil

Ubuntu Server

ubuntu®

- Baseado no Debian
- Não utiliza interface gráfica
- Acompanha os lançamentos **LTS** e **interim**
- Homologações com fabricantes de hardware
- Serviço de monitoramento e agentes
- Suporte a RAID por Software e LVM
- Homologado a virtualizadores e a soluções de cloud
- Suporte a HBA e iSCSI como target e initiator
- Firewall descomplicado

debian

ubuntu-br
Comunidade Ubuntu Brasil

Pontos de Atenção

ubuntu®

- O seu servidor é homologado?
- Vai montar servidor de que?
- Seu servidor possui core suficiente para a sua solução?
- O seu Hypervisor possui template para o Ubuntu?
- Política de Backup?
- Usuários locais ou em base de dados?
- Vai fazer o Hardening teste servidor?

A essência da segurança

ubuntu®

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade

- **Não-conformidades**
- **Hardening**

ubuntu-br
Comunidade Ubuntu Brasil

Ubuntu Security Notices

ubuntu®

- Visualização WEB e RSS
- Ajuda ao administrador de sistema a entender as necessidades de atualizações de segurança.
- Equipe de segurança: security@ubuntu.com
- Atualizações via APT (servidor)

 # sudo unattended-upgrades

 # sudo apt-get dist-upgrade -o Dir::Etc::ARQUIVO_COM_REPOSITORIOS

ubuntu-br
Comunidade Ubuntu Brasil

Ubuntu security notices

Subscribe to the RSS feed

These are the Ubuntu security notices that affect the current supported releases of Ubuntu. These notices are also posted to the ubuntu-security-announce mailing list (list archive). To report a security vulnerability in an Ubuntu package, please file a bug, or contact security@ubuntu.com. You may also be interested in learning about Ubuntu security policies. For more details on a specific CVE or source package, please see the Ubuntu CVE Tracker.

You can also view the latest notices by subscribing to the RSS or the Atom feeds.

Show: All Release: Showing page 1 of 43 Next >

USN-1883-1: Linux kernel (OMAP4) vulnerabilities - 14th June 2013

Kees Cook discovered a flaw in the Linux kernel's iSCSI subsystem. A remote unauthenticated attacker could exploit this flaw to cause a denial of service (system crash) or potentially gain administrative privileges. (CVE-2013-2850) An information leak was discovered in the Linux kernel's crypto API. A local user could exploit this ...

CVE-2013-2850 CVE-2013-3076 CVE-2013-3222 CVE-2013-3223 CVE-2013-3224 CVE-2013-3225 CVE-2013-3234 CVE-2013-3235

USN-1882-1: Linux kernel (OMAP4) vulnerabilities - 14th June 2013

Ubuntu CVE Tracker

ubuntu®

- Banco de informações a vulnerabilidades
- Acompanhadas do MITRE CVE
- Dispõe de informação detalhada e acompanhamento a outros sites
- Informações para os repositórios: Main, Universe e Partner
- Pode ser acessado pelo site: http://people.canonical.com/~ubuntu-security/cve/

ubuntu

Ubuntu CVE Tracker

Introduction

Ubuntu tracks its security vulnerabilities via the Ubuntu CVE Tracker. This report is divided into the following sections:

Main (supported by Canonical Ltd)
Universe (supported by the Ubuntu community)
Partner (supported by upstream vendor)

Priority Color Key

Main

CVE	Package	Ubuntu 10.04 LTS (Lucid Lynx)	Ubuntu 12.04 LTS (Precise Pangolin)	Ubuntu 12.10 (Quantal Quetzal)	Ubuntu 13.04 (Raring Ringtail)	Ubuntu 13.10 (Saucy Salamander)	Links
CVE-2005-1080	openjdk-6	needed*	needed*	needed	needed	needed	Mitre LP Debian
CVE-2005-4890	shadow	needed*	needed*	needed*	needed*	needed*	Mitre LP Debian
CVE-2005-4890	sudo	needed*	not-affected*	not-affected*	not-affected*	not-affected*	Mitre LP Debian
CVE-2009-0801	squid3	needed	needed*	needed*	needed*	needed*	Mitre LP Debian
CVE-2009-1384	libpam-krb5	ignored	needed*	needed*	needed*	needed*	Mitre LP Debian
CVE-2009-4135	coreutils	needed*	needed*	needed*	needed*	needed*	Mitre LP Debian
CVE-2009-5080	groff	needed*	needed*	needed*	needed*	needed*	Mitre LP Debian
CVE-2010-0624	cpio	needed*	not-affected*	not-affected*	not-affected*	not-affected*	Mitre LP Debian
CVE-2010-0624	tar	needed*	not-affected*	not-affected*	not-affected*	not-affected*	Mitre LP Debian
CVE-2010-	nano	needed*	not-affected*	not-affected*	not-affected*	not-affected*	Mitre LP

Ambiente Linux vs Windows

ubuntu®

- **O Linux não pega virus**

  “ ... são bastante incomum” **(Charlie Harvey – GNU Project)**

- Windows possui 899894892392384923248989990 de vírus
- O Linux possui vários anti-vírus
- Vulnerabilidades são tratadas pela comunidade e mantenedor (não pragas)
- Se gasta mais tempo configurando o Windows e contratando soluções do que o Linux
- Correções não precisam de boot*

ubuntu-br
Comunidade Ubuntu Brasil

Segurança no Ubuntu

ubuntu®

- A segurança no Linux é binária
- Política de primeiro usuário
- Conta de root bloqueada
- Janelas de root
- Auditorias em logs
- AppArmor como padrão
- Repositórios de segurança isolados
- Suporte a aplicações de backup

Backup e situações de desastre

ubuntu®

- Plano de backup
- Suporte a dispositivos de fitas como DDS 4mm, 8mm, 3590, 3592, LTOx e novas soluções de arquivamento em Library.
- Backup local
- Backup remoto
- Diversos programas de backup

ubuntu

Algumas não-conformidades presentes no sistema Linux

ubuntu-br
Comunidade Ubuntu Brasil

Não conformidades presentes

ubuntu®

- Atualize o seu Ubuntu **SEMPRE**

  $ sudo apt-get update

  $ sudo apt-get dist-upgrade

- Serviços desnecessários

  # initctl list | less

  # service --status-all

ubuntu-br
Comunidade Ubuntu Brasil

Não conformidades presentes

ubuntu®

- Usuários como root?

  Verifique no /etc/passwd se existe mais algum usuário com o UID 0

  # cat /etc/passwd | cut -d “:” -f 1,3,5

- Use timeout de sessão e nunca deixe conectado

  Adicione em .bashrc ou profile

  TMOUT=600

  export TMOUT

Não conformidades presentes

ubuntu®

- Altere em no máximo 60 dias sua senha

  $ passwd

  # chage -M 60 praga

  (fixar no arquivo /etc/login.defs o PASS_MAX_DAYS)

- Verifique os grupos dos seus usuários

  # cat /etc/group

  # id usuario

  # groups usuario

ubuntu-br
Comunidade Ubuntu Brasil

Não conformidades presentes

ubuntu®

- Permissão do usuário comum de compilar

  Remover as permissões de outros do binário gcc

- Uso irrestritivo do cron e at

  Adicionar os usuários em /etc/cron.allow e /etc/at.allow

- Uso de políticas para o tcpwrappers

  Mapear todos os serviços e criar regras em /etc/hosts.allow e /etc/hosts.deny

Não conformidades presentes

ubuntu®

- Controle compensatórios

  /var/log/*

  /var/log/syslog (/var/log/messages)

  last

  lastlog

- Permissões dos arquivos de log incorretas

  Os arquivos devem estar com a permissão 640 (rw-r-----) e diretórios com 750 (rwxr-x---)

Não conformidades presentes

ubuntu®

- Permissões de /etc incorretas

  Os arquivos e diretórios não devem estar com permissões de leitura, escrita e entrada (arquivos: execução) para outros.

- Permissões indevidas com o bit-especial

  É necessário verificar se no sistema de arquivos existe algum arquivo executável com a permissão suid (analisar cada arquivo encontrado).

  # find / -user root -perm -4000 -print

Não conformidades presentes

ubuntu®

- Todo usuário deve ter o seu diretório

  *** Verifique o /etc/passwd (ou finger)**

  *** Verifique o /home**

- O usuário root não deve se conectar diretamente no terminal

  Verifique o /etc/securetty (para serial)

  Verifique o /etc/ssh/sshd_config

  PermitRootLogin = no

- Instalações devem separar /home e /tmp da raiz.

  Proteja a sua tabela de inodes.

ubuntu-br
Comunidade Ubuntu Brasil

Não conformidades presentes

ubuntu

- Umask deve ser restritivo

  Defina o umask em /etc/profile e proteja arquivos e diretórios

- Ah! Dá um chmod 777

  # userdel -r usuario

  Bloquear acessos dessa pessoa na empresa.

E não para ....

ubuntu®

- **Ausência de restrições nos compartilhamentos NFS**
- **Permissões de arquivos de auditagem do logrotate**
- **Sem restrições a numero máximo de tentativas de logins**
- **Ausência de restrições nos compartilhamentos pelo samba**
- **FTP anônimo permitido**
- **Ausência de proteção via chroot para o bind**
- **Vulnerabilidade de spoofing entre as interfaces**
- **Ausência da configuração de pacotes suspeitos (logmartians)**
- **Broadcast em ICMP sendo permitido**
- **Roteamento entre as interfaces habilitado desnecessariamente**

Investimentos na segurança

ubuntu®

- **Analise e trate com correções as não-conformidades**
- **Treinamentos em Linux**
- **Atualize sempre!**
- **Mantenha o Ubuntu Server nas versões LTS**
- **Se envolva com a comunidade Linux**
- **Leia fóruns**
- **Consulte Wiki**
- **Coma as documentações do mantenedor**
- **Consulte sites de segurança**

ubuntu-br
Comunidade Ubuntu Brasil

Mas fique tranquilo ....

ubuntu®

O Windows tem muito mais não-conformidades

ubuntu-br
Comunidade Ubuntu Brasil

Precisa de suporte?

ubuntu-br
Comunidade Ubuntu Brasil

Suporte da comunidade

ubuntu®

- Apoio às diversas necessidades de suporte dos usuários
- Alguns canais de suporte ativos:
  - IRC
  - Fórum Ubuntu Linux - PT
  - Listas de discussão
  - AskUbuntu
  - ubuntuforums
  - Help Ubuntu
  - Sites da comunidade

ubuntu-br
Comunidade Ubuntu Brasil

Suporte Canonical

ubuntu®

- Landscape
- Virtualização
- Cloud
- Migração
- Desktop
- Server
- OEM
- Acesse: http://www.canonical.com

ubuntu-br
Comunidade Ubuntu Brasil

Começe agora mesmo!

ubuntu®

http://www.ubuntu.com.br

Linux, Não trava, não da tela azul

Se jogar pro espaço,

Vira satélite ....

É o poder!

ubuntu-br
Comunidade Ubuntu Brasil

Dúvidas?

Apresentação de slides

ubuntu®

Baixe o Ubuntu Server

http://www.ubuntu.com

Autor:

Aprigio Simoes

aprigio@linuxstudent.com.br

http://www.aprigiosimoes.com.br

ubuntu-br

Comunidade Ubuntu Brasil