

SO II - Conhecendo o Kali Linux



Tomaz Rocha - tomazrf@globo.com
Rafael Santos – rafaveira3@gmail.com

Kali Linux – Agenda

1 – O que é Kali Linux?

1.1 – Algumas ferramentas

2 – Um pouco de História...

2.1 – Offensive Security

2.2 – BackTrack 1,2,3,4,5

2.3 – Kali

3 – Ubuntu vs. Debian

3.1 - GNOME

4 – Processos

5 – Gerenciamento de aplicações

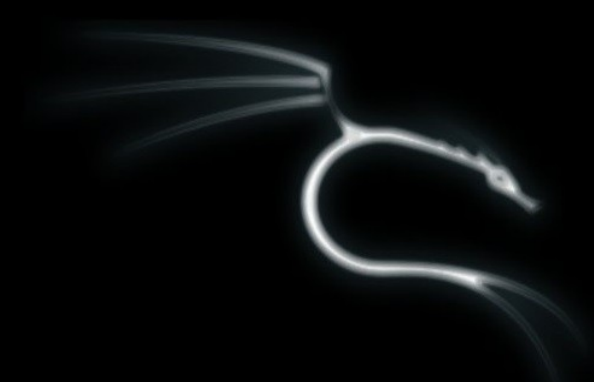
5.1 – Packagekit

5.2 – apt-get

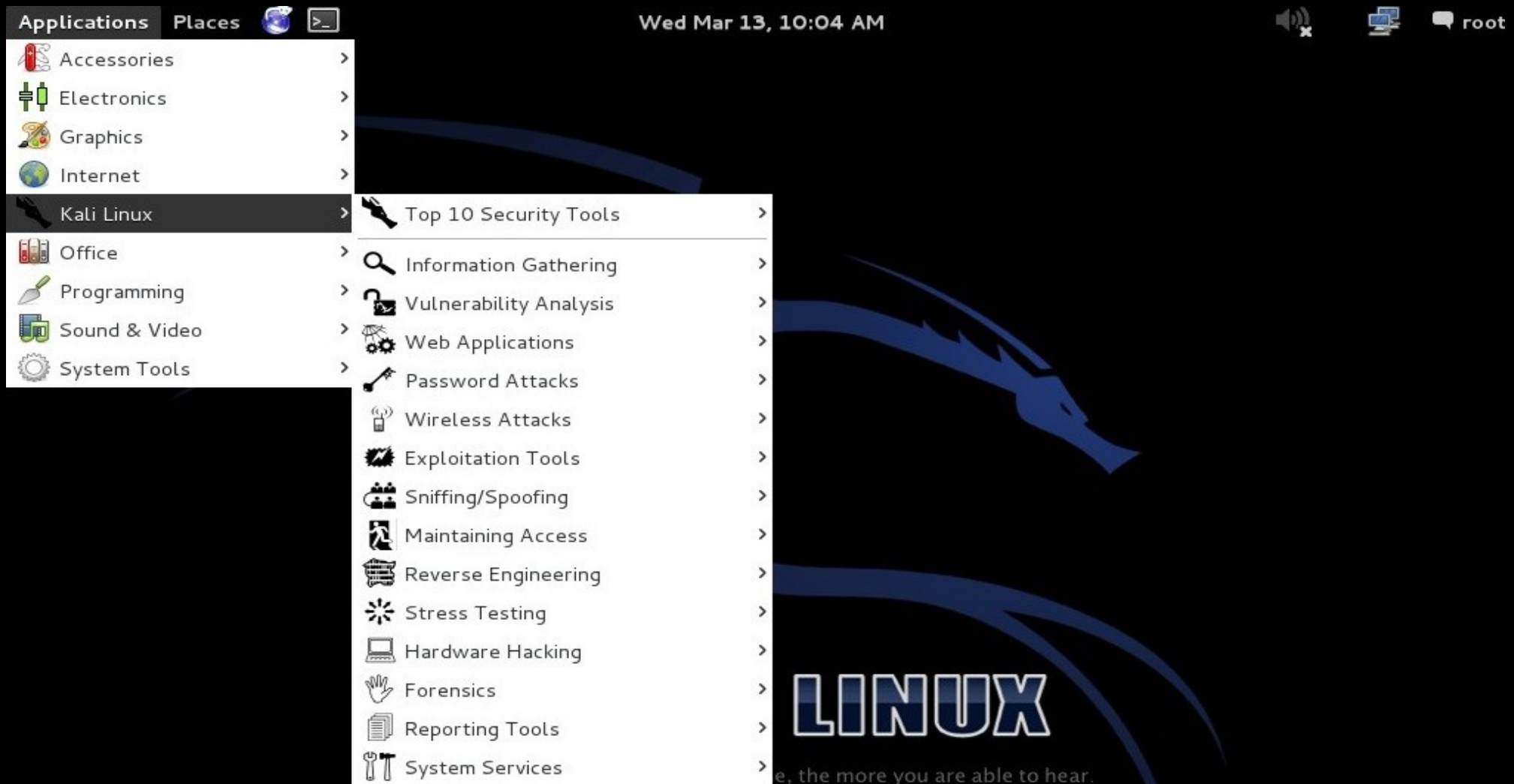
5.3 – Software Update

6 – Diretórios

7 – Outros SO

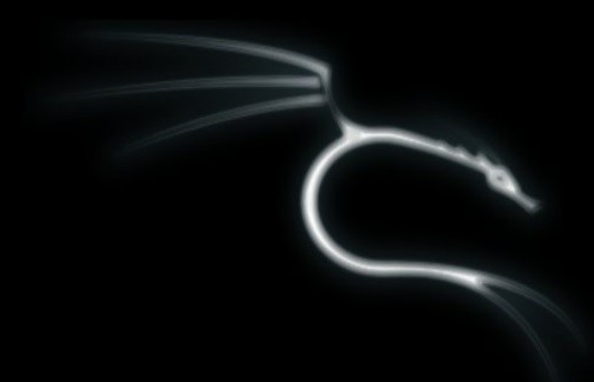


O que é Kali Linux?



“Kali Linux é uma avançada distribuição Linux especializada em Testes de Intrusão e Auditoria de Segurança.”

Algumas ferramentas

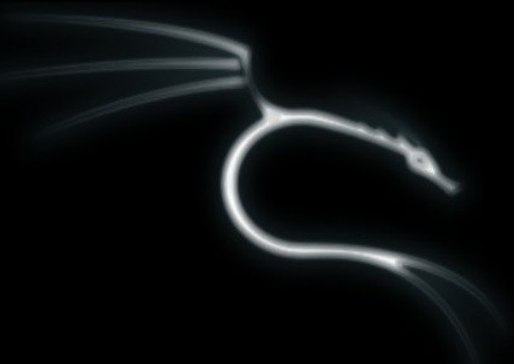


Um pouco de História...

OFFENSIVE
s e c u r i t y

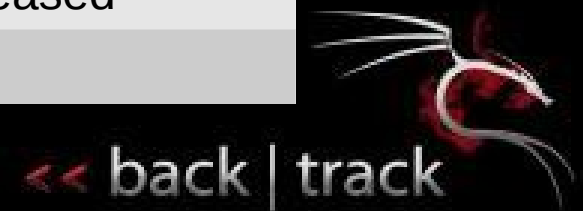


<https://www.offensive-security.com/>



Um pouco de História...

February 5, 2006	BackTrack v.1.0 Beta
May 26, 2006	First Release of BackTrack v.1.0.
March 6, 2007	BackTrack 2 final released
June 19, 2008	BackTrack 3 final released
January 9, 2010	BackTrack 4 final released
May 8, 2010	BackTrack 4 R1 released
November 22, 2010	BackTrack 4 R2 released
May 10, 2011	BackTrack 5 released
August 18, 2011	BackTrack 5 R1 released
March 1, 2012	BackTrack 5 R2 released
August 13, 2012	BackTrack 5 R3 released
March 13, 2013	Kali 1.0 released



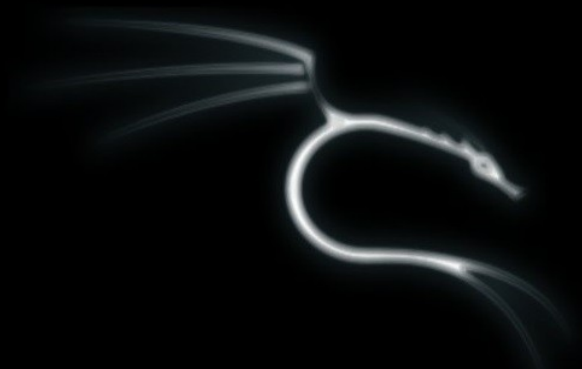
Ubuntu vs. Debian



A partir do BackTrack 4, os desenvolvedores passaram a usar o Debian ao invés do Ubuntu!



GNOME



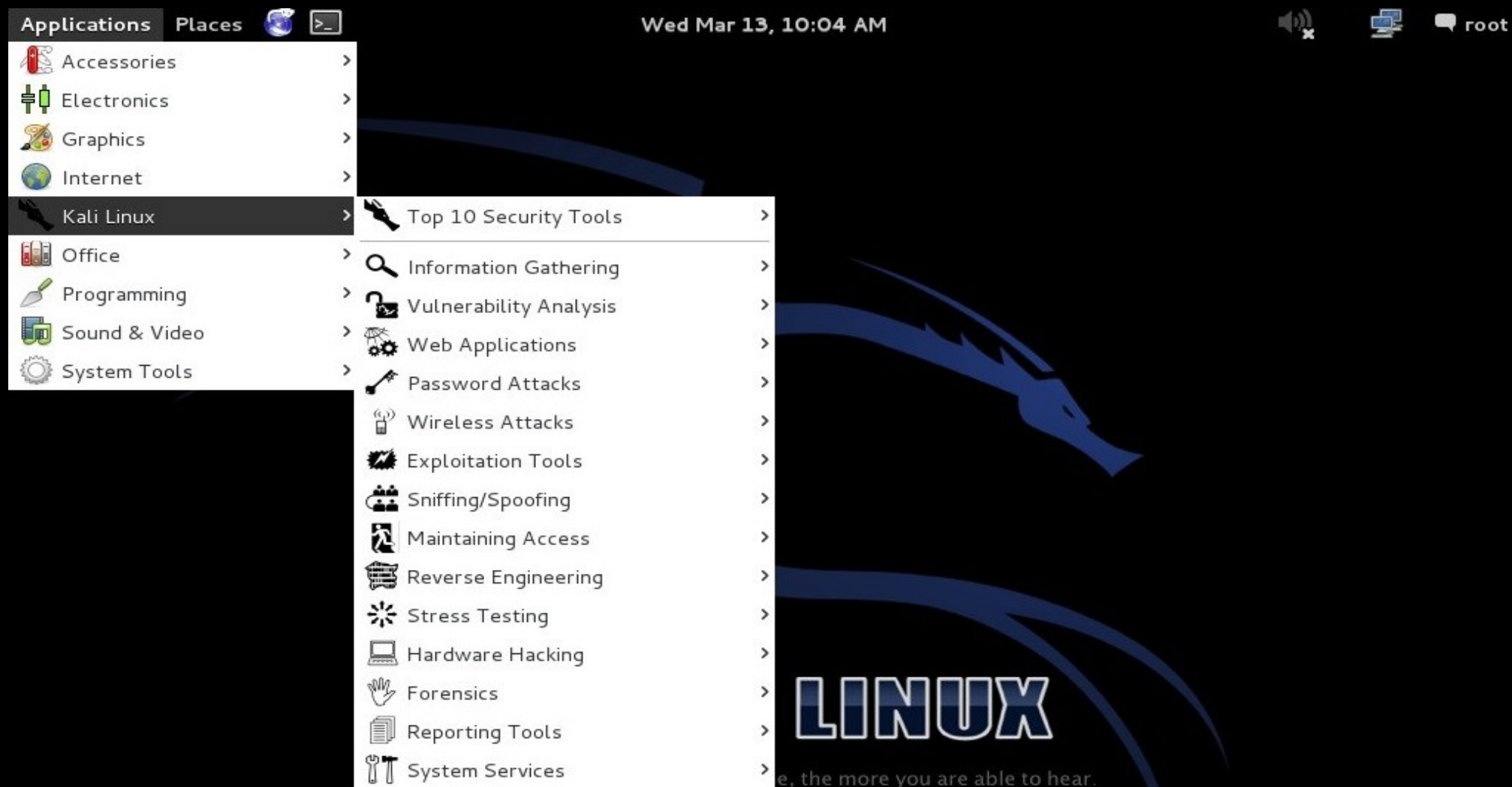
GNOME



- Criado em 1997 como uma resposta ao Windows 95;
- Enfatiza a usabilidade ao invés da configurabilidade;
- O projeto Gnome foi o primeiro a oferecer um desktop inteiramente livre para sistemas baseados em UNIX.



GNOME



Processos

```
top - 23:11:44 up 15 min, 2 users, load average: 0,59, 0,49, 0,37
Tarefas: 170 total, 1 running, 169 sleeping, 0 stopped, 0 zombie
%Cpu(s): 13,3 us, 4,6 sy, 0,0 ni, 79,6 id, 2,5 wa, 0,0 hi, 0,0 si, 0,0 st
KiB Mem: 3790768 total, 1791816 used, 1998952 free, 60220 buffers
KiB Swap: 9775100 total, 0 used, 9775100 free, 673684 cached
```

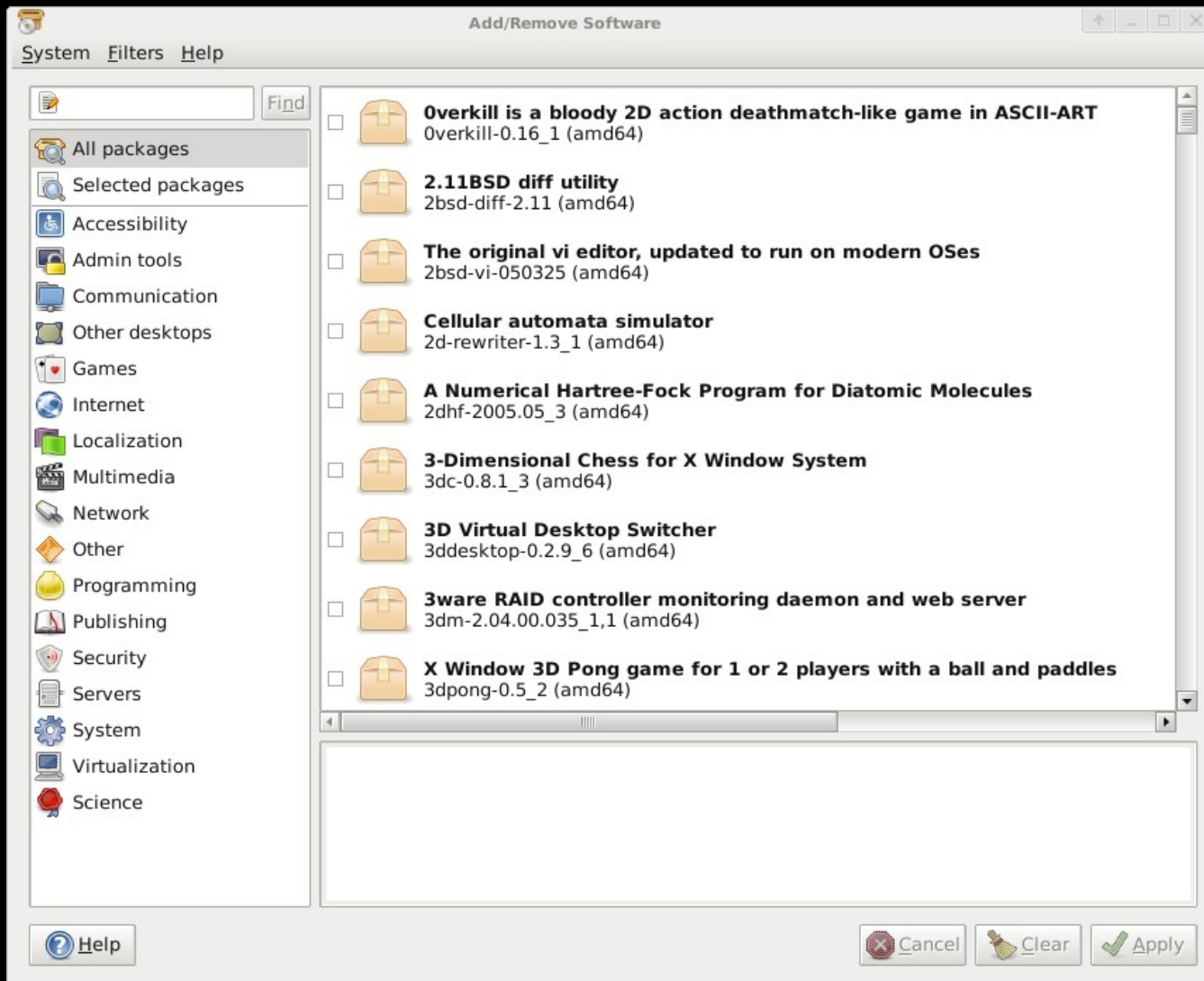
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2426	osvaldo	20	0	702m	107m	30m	S	5,0	2,9	0:31.64	chromium-browse
1713	osvaldo	20	0	1133m	106m	38m	S	4,7	2,9	0:17.69	compiz
1033	root	20	0	201m	35m	18m	S	3,7	1,0	0:26.29	Xorg
1566	osvaldo	9	-11	419m	6800	4316	S	3,3	0,2	0:12.87	pulseaudio
2143	osvaldo	20	0	1181m	181m	69m	S	2,7	4,9	0:21.81	soffice.bin
2340	osvaldo	20	0	1065m	174m	27m	S	0,7	4,7	0:21.91	chromium-browse
23	root	20	0	0	0	0	S	0,3	0,0	0:01.44	kworker/0:1
1067	tomcat7	20	0	1071m	76m	12m	S	0,3	2,1	0:05.43	java
2198	osvaldo	20	0	830m	106m	43m	S	0,3	2,9	0:15.87	chromium-browse
2555	osvaldo	20	0	589m	19m	12m	S	0,3	0,5	0:00.48	gnome-terminal
1	root	20	0	27052	2756	1360	S	0,0	0,1	0:01.04	init
2	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0,0	0,0	0:00.21	ksoftirqd/0
5	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	kworker/0:0H
7	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	kworker/u:0H



- Evita o desperdício de tempo;
- Kernel escalonador de processos;
- Limite de recursos por processo;
- Processos preemptivos.

Gerenciamento de aplicações

Packagekit



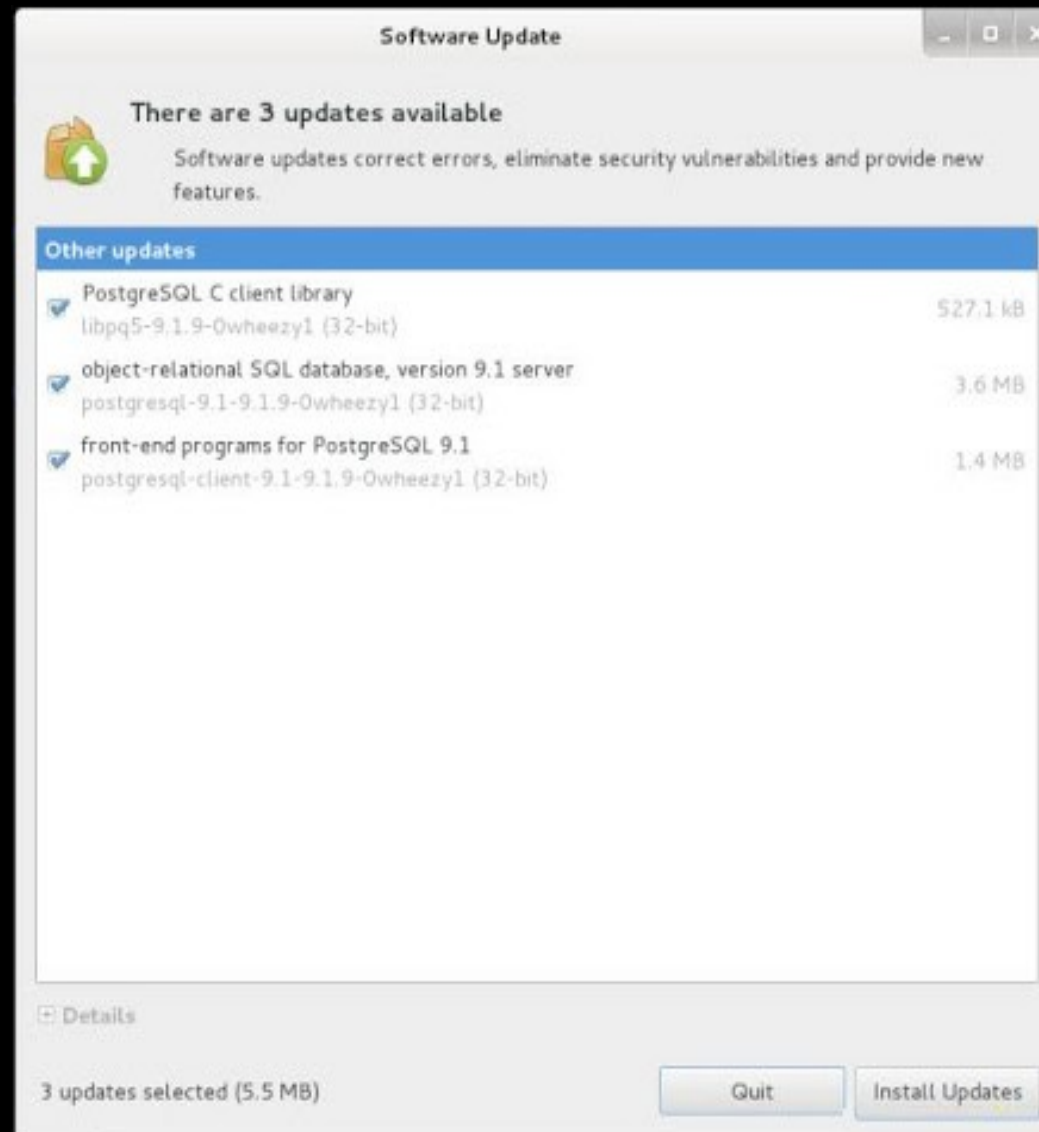
Gerenciamento de aplicações

apt-get

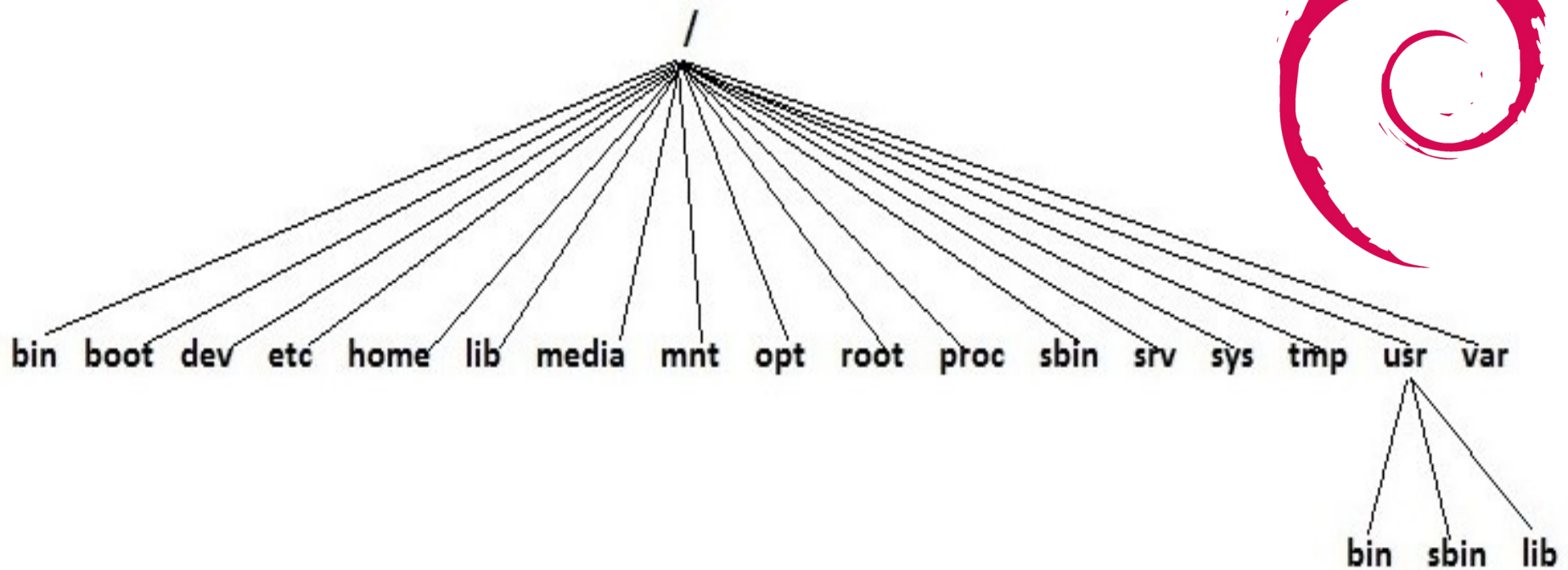
```
Terminal
File Edit View Terminal Tabs Help
roger@roger-desktop ~ $ sudo apt-get update
[sudo] password for roger:
Hit http://archive.ubuntu.com intrepid Release.gpg
Ign http://packages.linuxmint.com felicia Release.gpg
Hit http://security.ubuntu.com intrepid-security Release.gpg
Hit http://archive.canonical.com intrepid Release.gpg
Ign http://packages.linuxmint.com felicia/main Translation-en_US
Ign http://archive.ubuntu.com intrepid/main Translation-en_US
Get:1 http://packages.medibuntu.org intrepid Release.gpg [197B]
Ign http://packages.linuxmint.com felicia/upstream Translation-en_US
Ign http://security.ubuntu.com intrepid-security/main Translation-en_US
Ign http://archive.ubuntu.com intrepid/restricted Translation-en_US
Ign http://packages.medibuntu.org intrepid/free Translation-en_US
Ign http://archive.canonical.com intrepid/partner Translation-en_US
Ign http://packages.linuxmint.com felicia/import Translation-en_US
Ign http://security.ubuntu.com intrepid-security/restricted Translation-en_US
Ign http://archive.ubuntu.com intrepid/universe Translation-en_US
Hit http://archive.canonical.com intrepid Release
Ign http://packages.medibuntu.org intrepid/non-free Translation-en_US
Ign http://archive.ubuntu.com intrepid/multiverse Translation-en_US
Ign http://security.ubuntu.com intrepid-security/universe Translation-en_US
Get:2 http://packages.linuxmint.com felicia Release [7869B]
Hit http://archive.ubuntu.com intrepid-updates Release.gpg
Ign http://security.ubuntu.com intrepid-security/multiverse Translation-en_US
```


Gerenciamento de aplicações

Software Update



Diretórios



Relação com outros SO

Wine



Carregador de programas Windows no Wine

Microsoft Windows Compatibility Layer (Binary Emulator and Library)

★★★★☆ (67 avaliações)

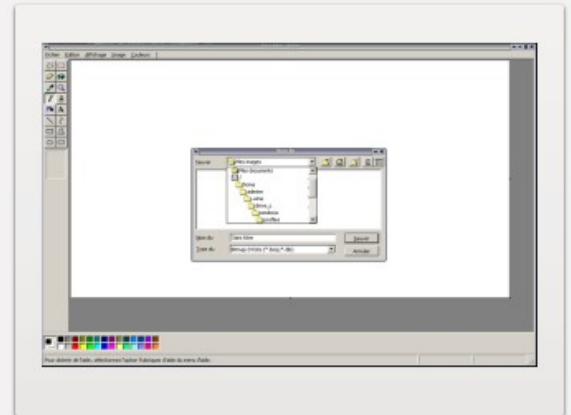
Gratuito

Instalar

Wine is a compatibility layer for running Windows applications on Linux. Applications are run at full speed without the need of cpu emulation. Wine does not require Microsoft Windows, however it can use native system dll files in place of its own if they are available.

This package includes a program loader for running unmodified Windows executables as well as the Wine project's free version of the Windows API for running programs ported from Windows.

[Página do desenvolvedor](#)





Dúvidas?



Obrigado!

Tomaz Rocha - tomazrf@globo.com
Rafael Santos – rafaveira3@gmail.com

Referências

- 1 - <https://www.offensive-security.com/community-projects/backtrack-linux/>
- 2 - <https://www.offensive-security.com/community-projects/kali-linux/>
- 3 - <http://www.kali.org/news/birth-of-kali/>
- 4 - <http://en.wikipedia.org/wiki/BackTrack>
- 5 - <http://br.docs.kali.org/introduction-pt-br/o-que-e-o-kali-linux>
- 6 - <http://www.debian.org/doc/>
- 7 - <http://www.gnu.org/licenses/gpl-faq.html#WhatDoesGPLStandFor>
- 8 - <http://debian-handbook.info/browse/pt-BR/stable/sect.filesystem-hierarchy.html>
- 9 - <http://www.vivaolinux.com.br/artigo/Estudo-sobre-os-tipos-de-gerenciamento-do-SO-Linux?pagina=5>