

Trabalho de Sistemas Operacionais

Distribuição: Kali Linux



"The quieter you become, the more you are able to hear."

("Quanto mais quieto você se torna, mais você é capaz de ouvir .")

Porque ele foi criado ?

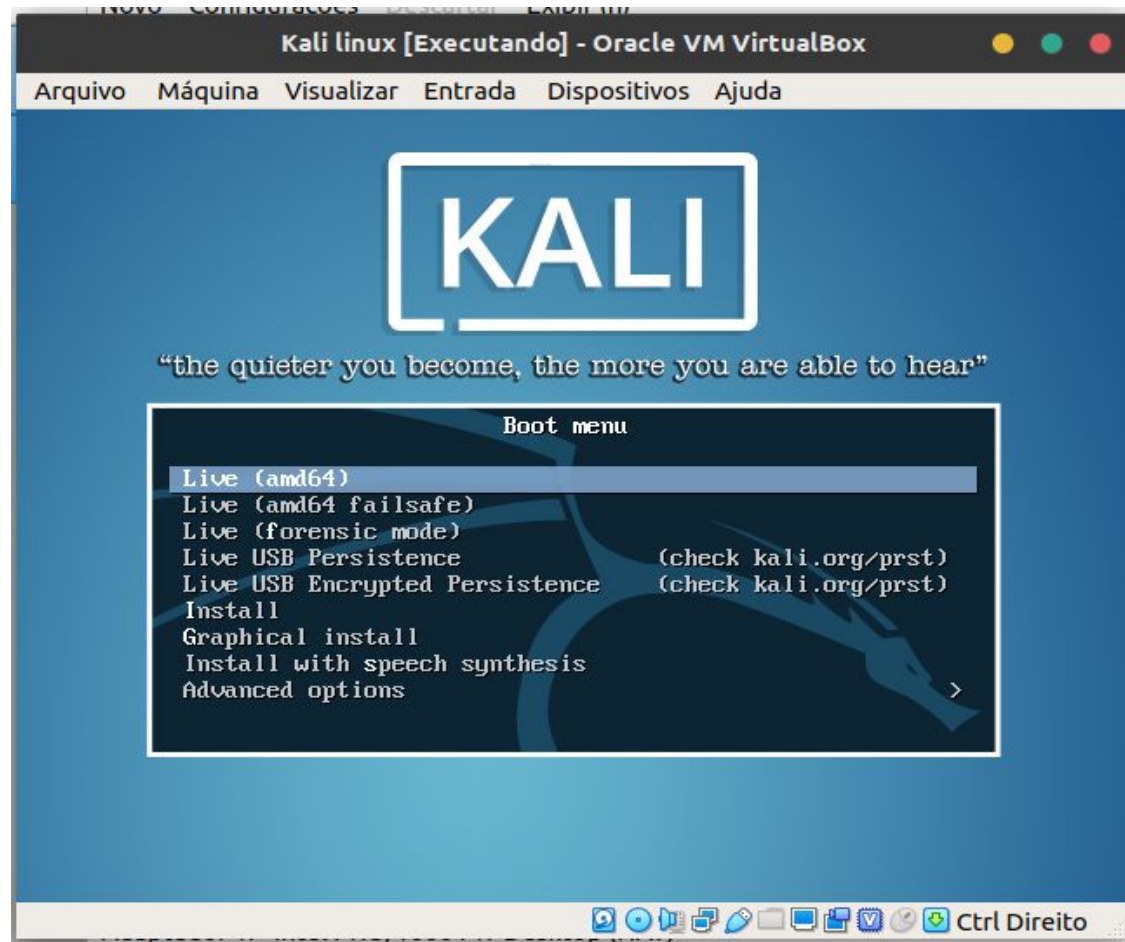
- Conceituado como “nova geração” das ferramentas de teste de penetração em redes de computadores, o Kali Linux tem maior robustez e estabilidade operacional;
- Kali Linux foi criado pela Offensive-Security;

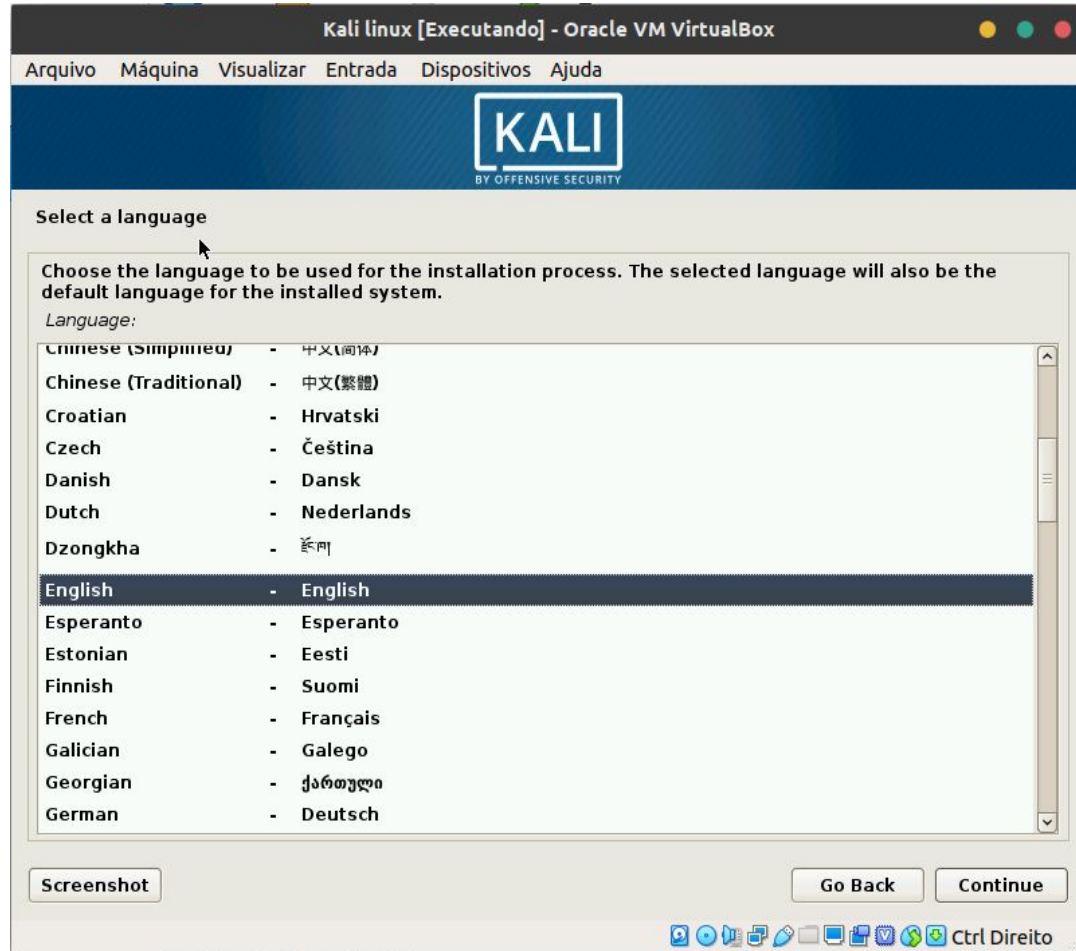
Versões do Kali Linux:

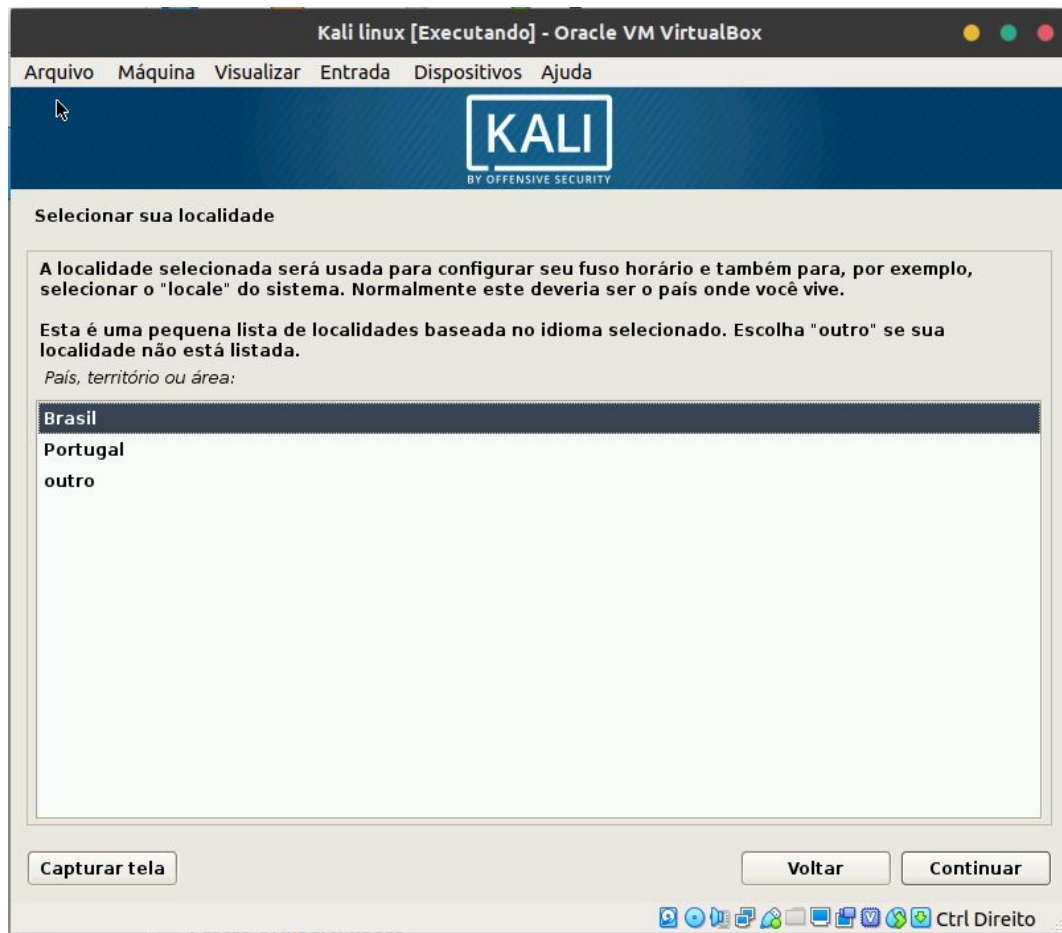
- **Kali 1.0.9** – 25th August, 2014 – BugFix release including installer and a set of tool updates and package fixes.
- **Kali 1.0.8** – 22nd July, 2014 – EFI Support for our “full” ISOs and a set of tool updates and package fixes.
- **Kali 1.0.7** – 27th May, 2014 – Kernel 3.14, tool updates, package fixes, Kali Live Encrypted USB Persistence.
- **Kali 1.0.6** – 9th January, 2014 – Kernel 3.12, cryptsetup nuke option, Amazon AMI, ARM build scripts.
- **Kali 1.0.5** – 5th September, 2013 – BugFix rollup. LVM Encrypted installs, Software Defined Radio (SDR) tools.
- **Kali 1.0.4** – 25th July, 2013 – BugFix rollup. Penetration testing tool additions and updates.
- **Kali 1.0.3** – 26th April, 2013 – BugFix rollup. New accessibility features. Added live Desktop installer.
- **Kali 1.0.2** – 27th March, 2013 – Minor BugFix release and update roll-up.
- **Kali 1.0.1** – 14th March, 2013 – Minor BugFix release (USB Keyboard).
- **Kali 1.0.0** – 13th March, 2013 – Initial release, “moto”.

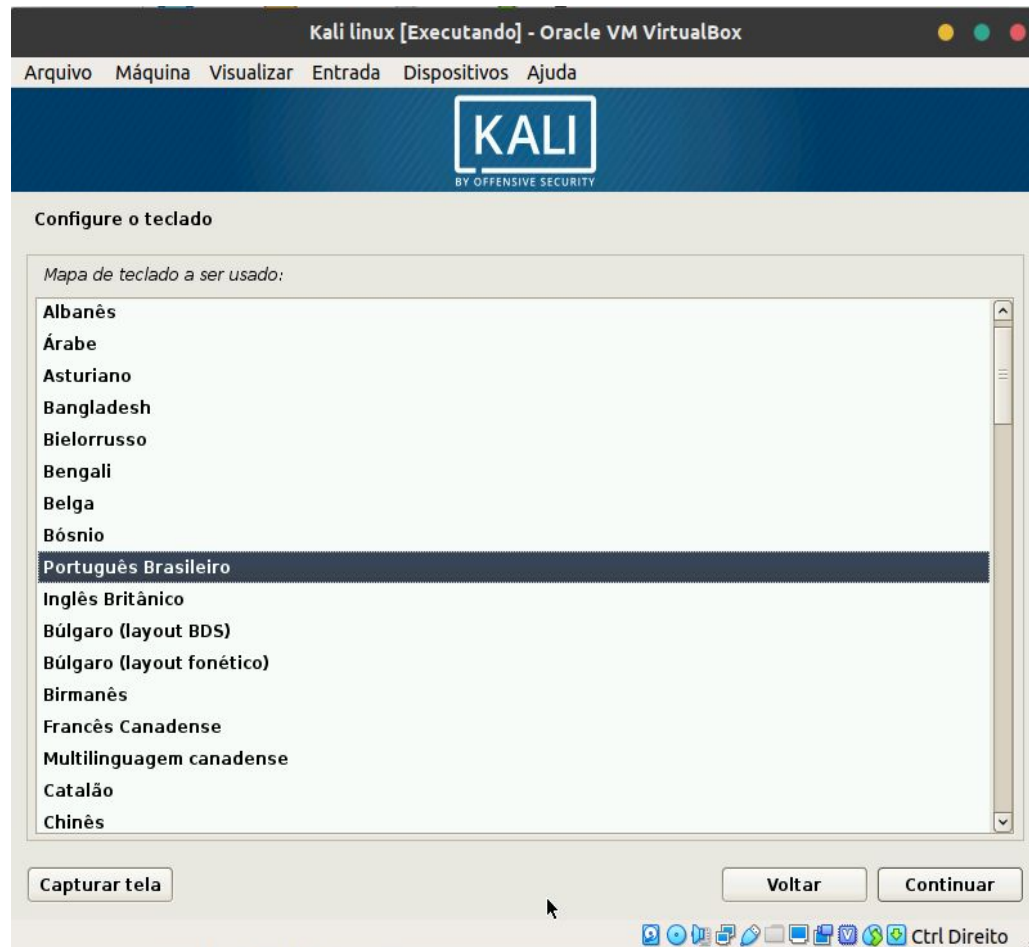
- **Kali 2019.1a** – 4th March, 2019 – Minor BugFix release (VMware Installer).
-
- **Kali 2019.1** – 18th February, 2019 – The First **2019 Kali Rolling** release. Kernel 4.19.13, GNOME 3.30.2
 - **Kali 2018.4** – 29th October, 2018 – The Fourth **2018 Kali Rolling** release. Kernel 4.18.0, GNOME 3.30.1
 - **Kali 2018.3** – 27th August, 2018 – The Third **2018 Kali Rolling** release. Kernel 4.17.0, GNOME 3.28.2
 - **Kali 2018.2** – 30th April, 2018 – The Second **2018 Kali Rolling** release. Kernel 4.15.0, GNOME 3.28.0
 - **Kali 2018.1** – 6th February, 2018 – The first **2018 Kali Rolling** release. Kernel 4.14.12, GNOME 3.26.2
 - **Kali 2017.3** – 21st November, 2017 – The third **2017 Kali Rolling** release. Kernel 4.13, GNOME 3.26
 - **Kali 2017.2** – 20th September, 2017 – The second **2017 Kali Rolling** release. Kernel 4.12, GNOME 3.25.
 - **Kali 2017.1** – 25th April, 2017 – The first **2017 Kali Rolling** release. Kernel 4.9, GNOME 3.22.
 - **Kali 2016.2** – 31st August, 2016 – The second **Kali Rolling** release. Kernel 4.6, GNOME 3.20.2.
 - **Kali 2016.1** – 21st January, 2016 – The first **Kali Rolling** release. Kernel 4.3, GNOME 3.18.
 - **Kali 2.0** – 11th August, 2015 – **Major release**, “safi”, now a rolling distribution, major UI changes.
 - **Kali 1.1.0a** – 13th March, 2015 – No fanfare release fixing kernel ABI inconsistencies in the installers.
 - **Kali 1.1.0** – 9th February, 2015 – **First dot release** in 2 years. New kernel, new tools and updates.

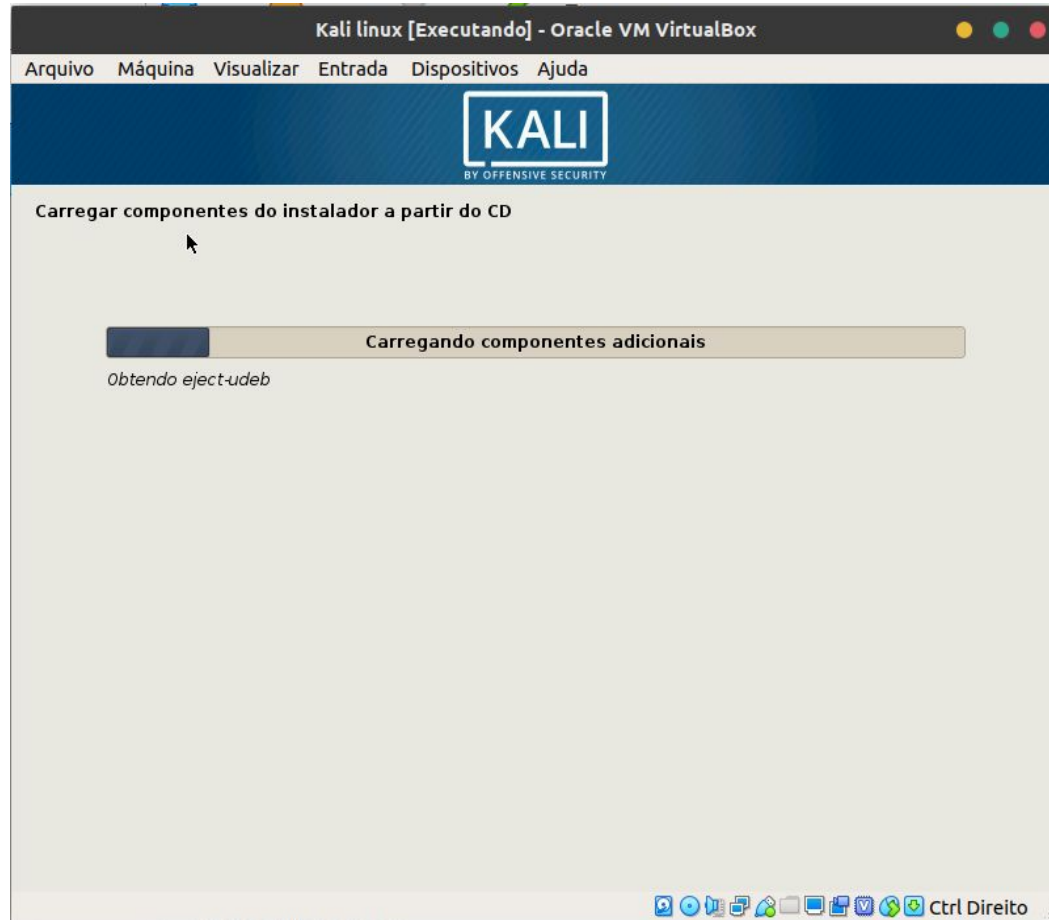
Instalação

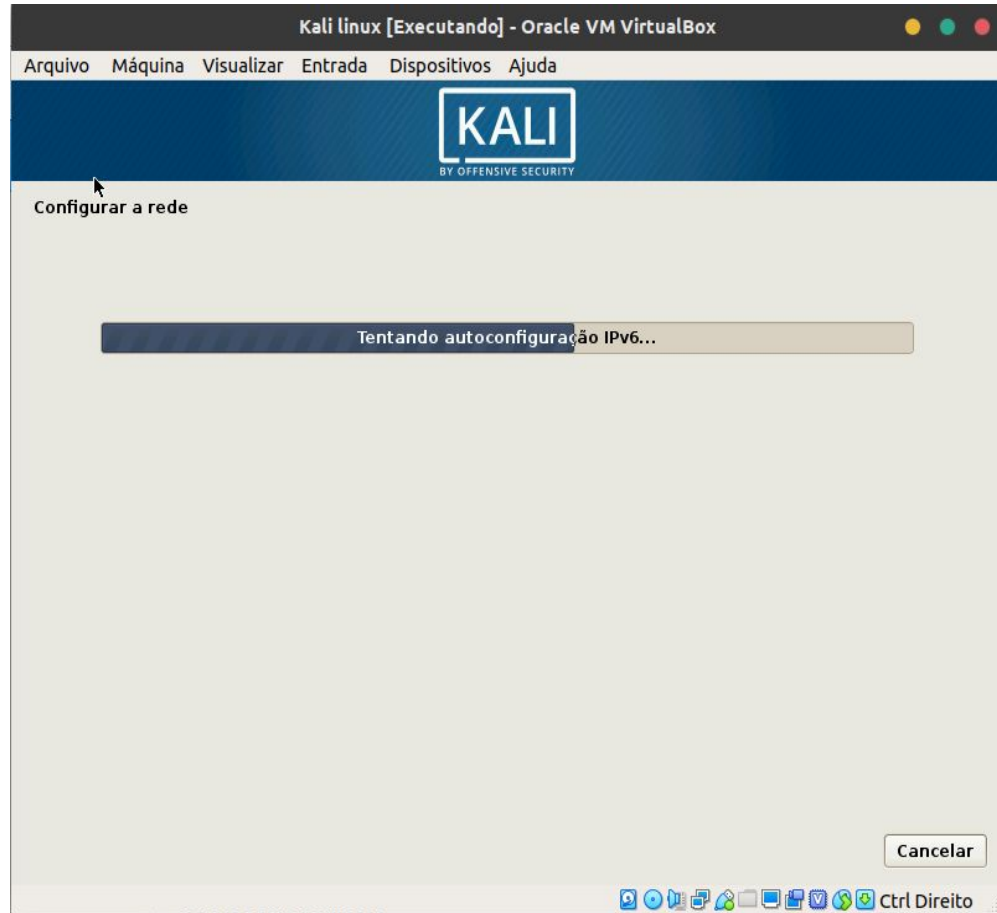


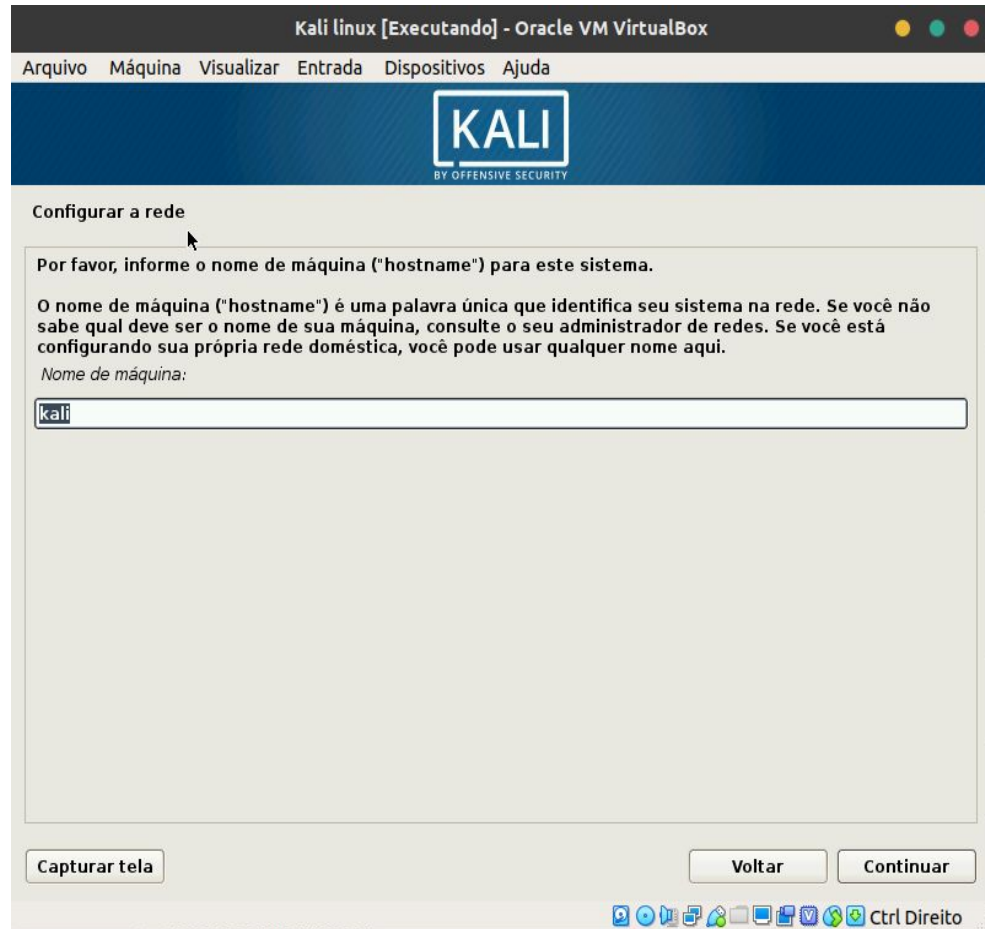


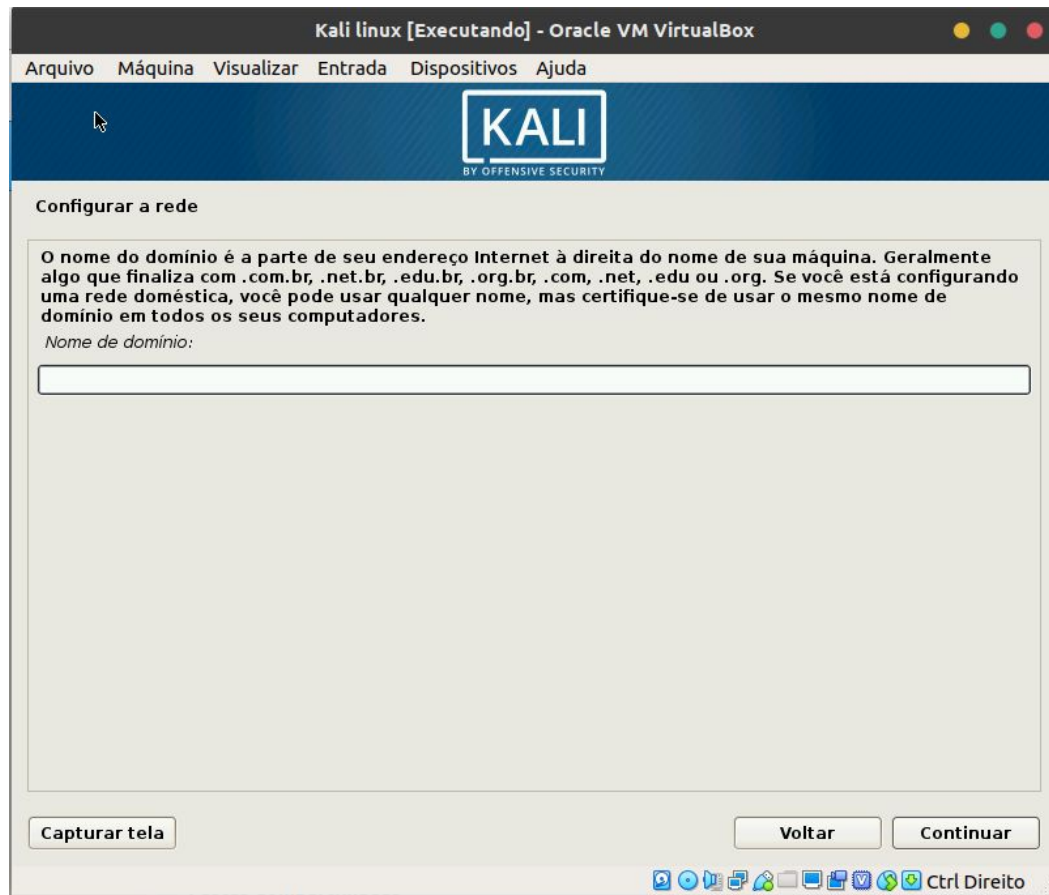


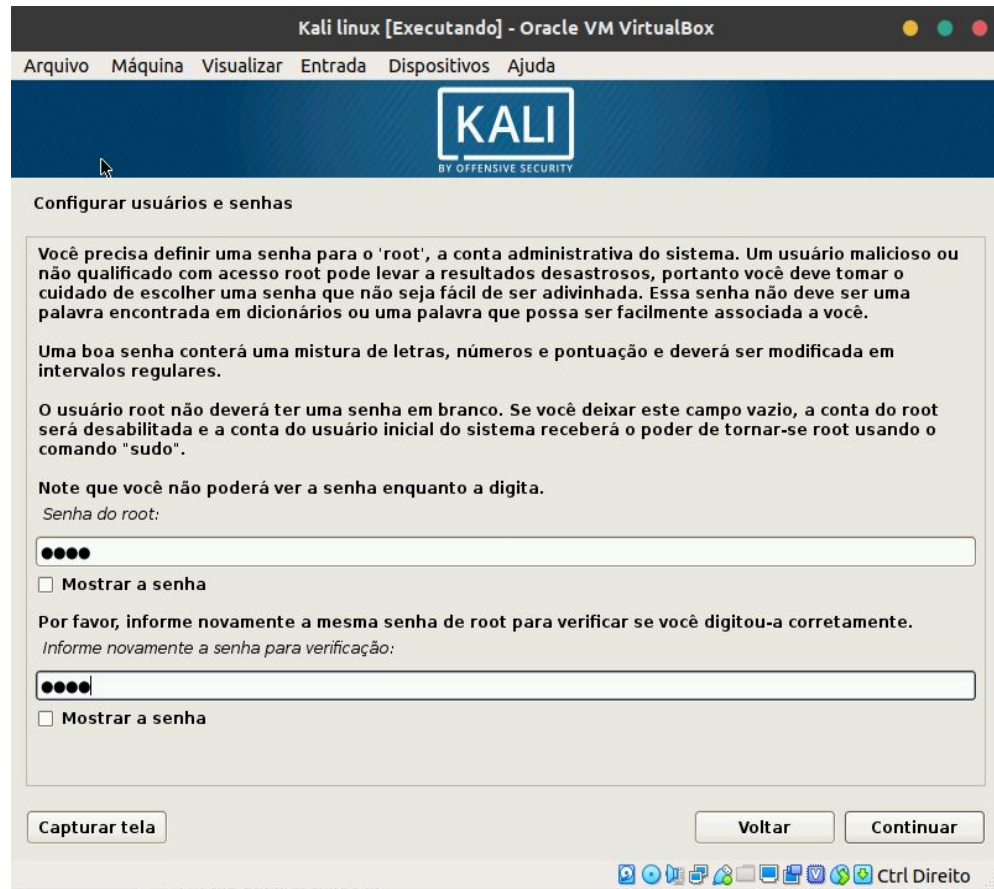


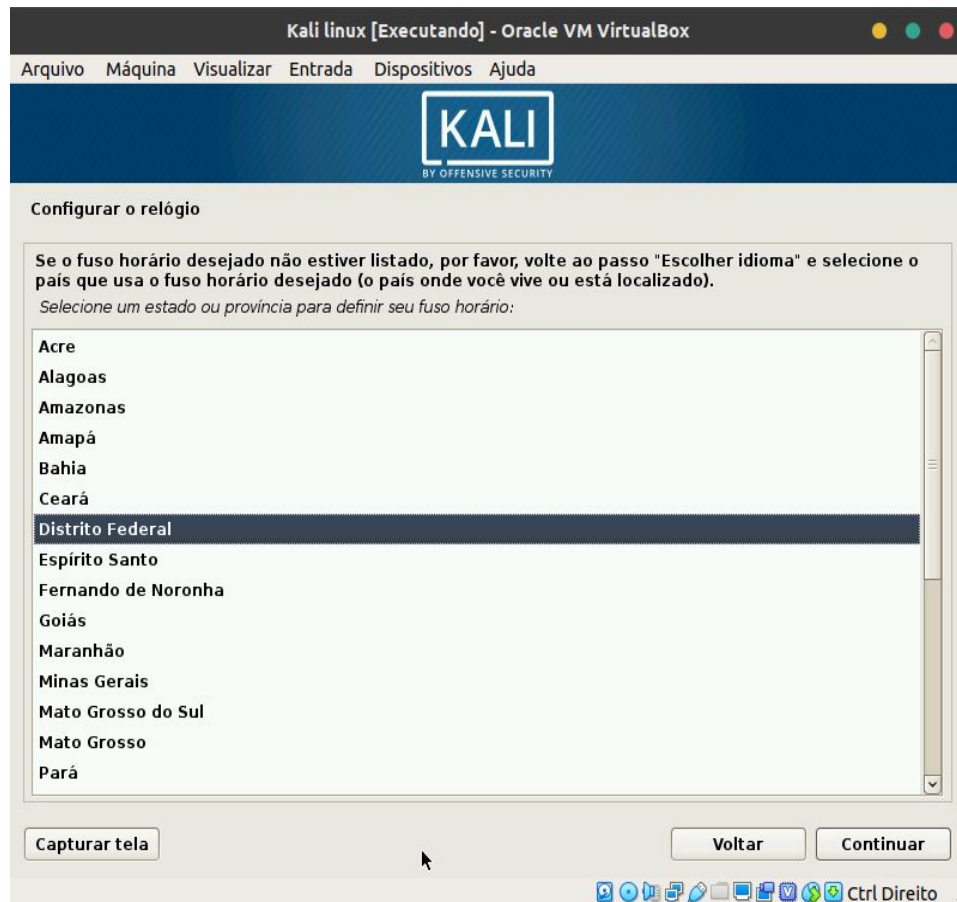


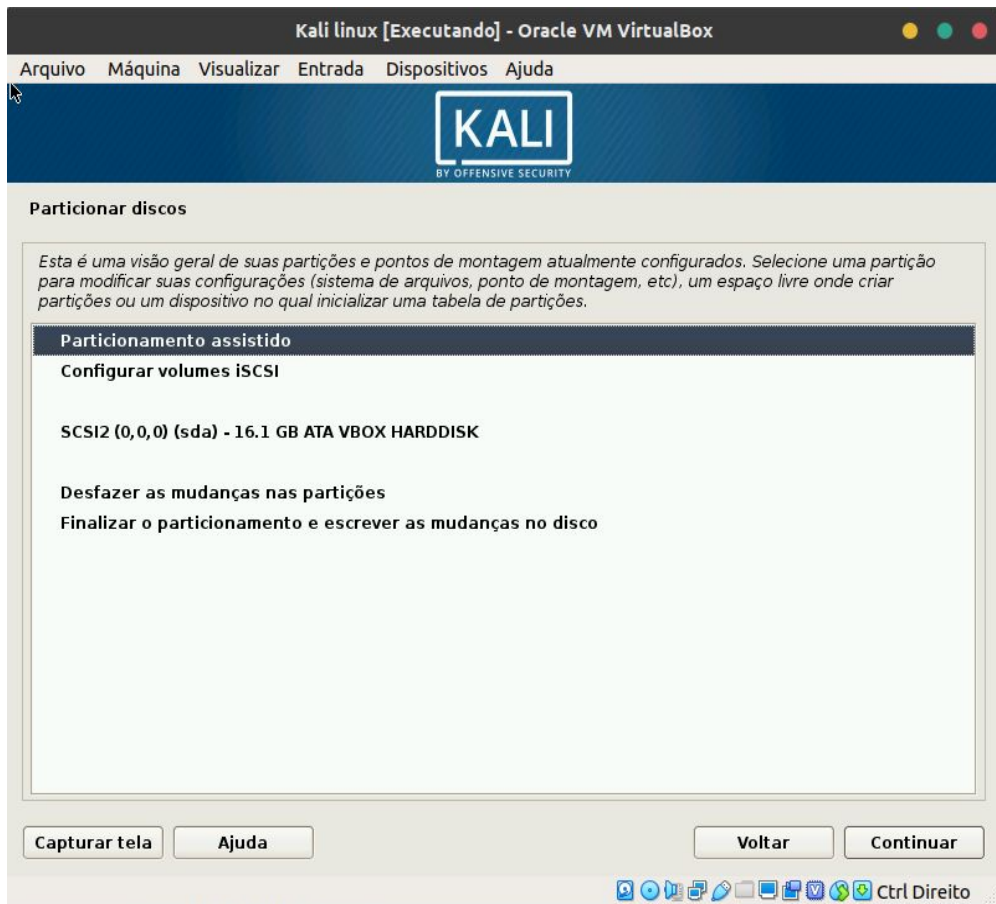


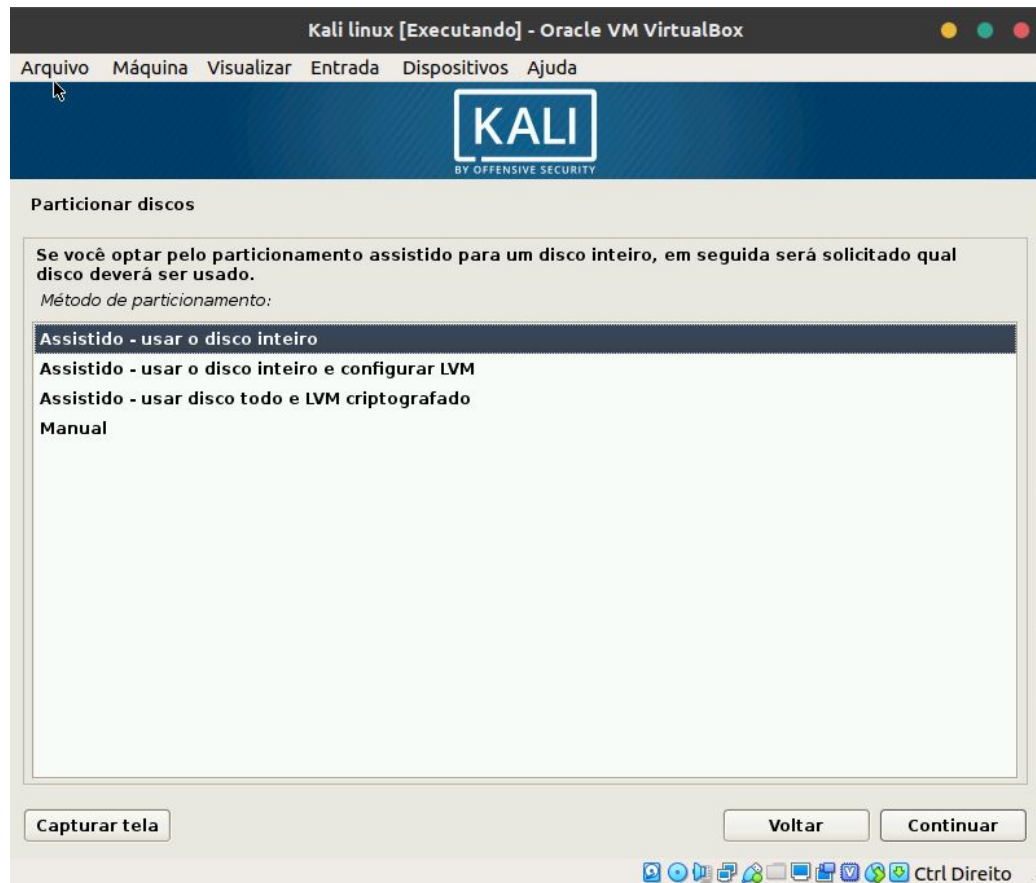


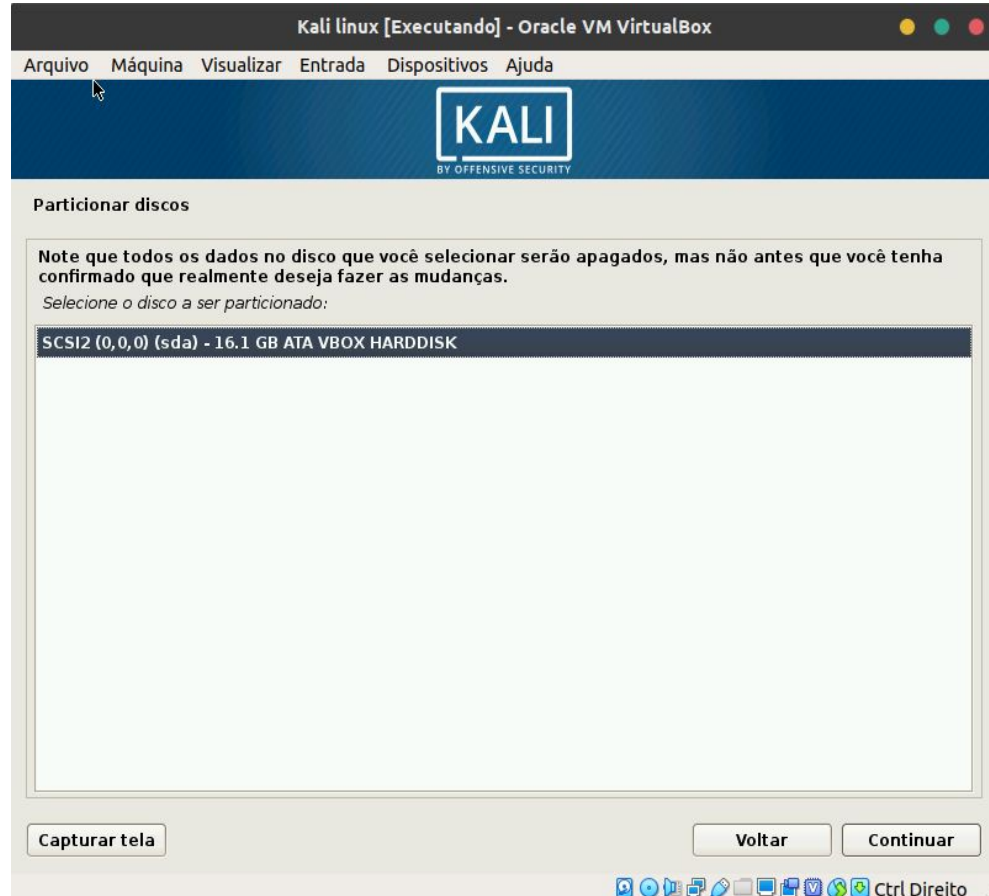


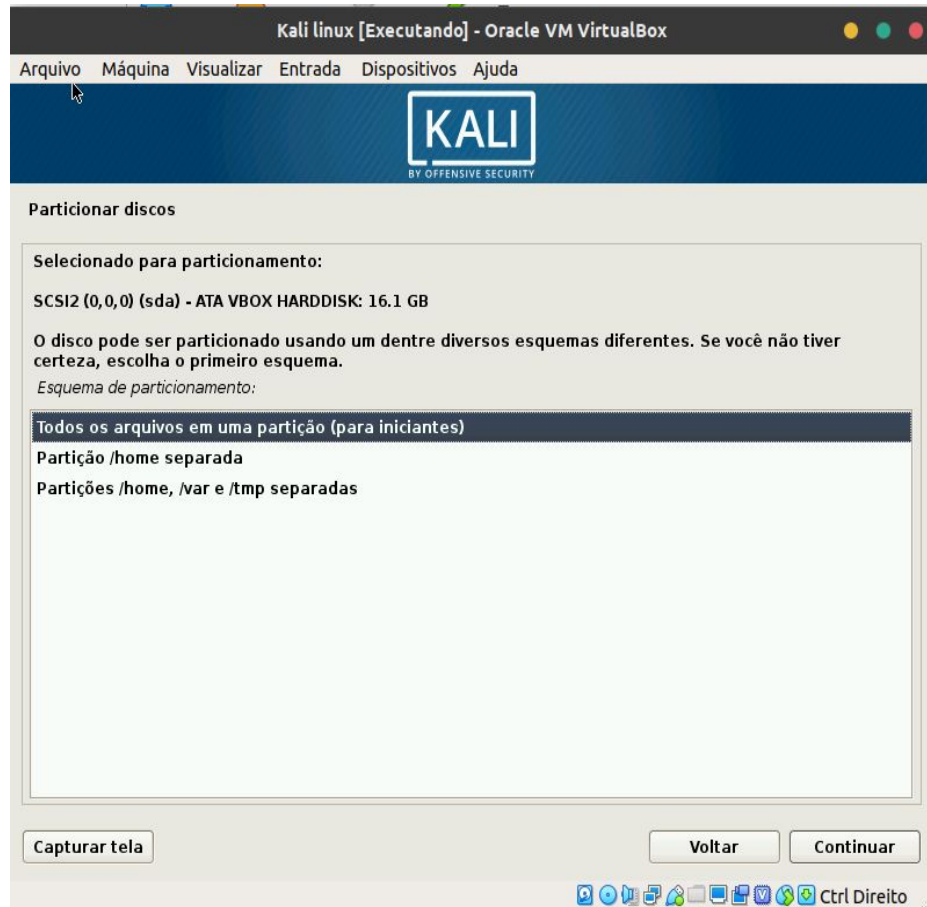


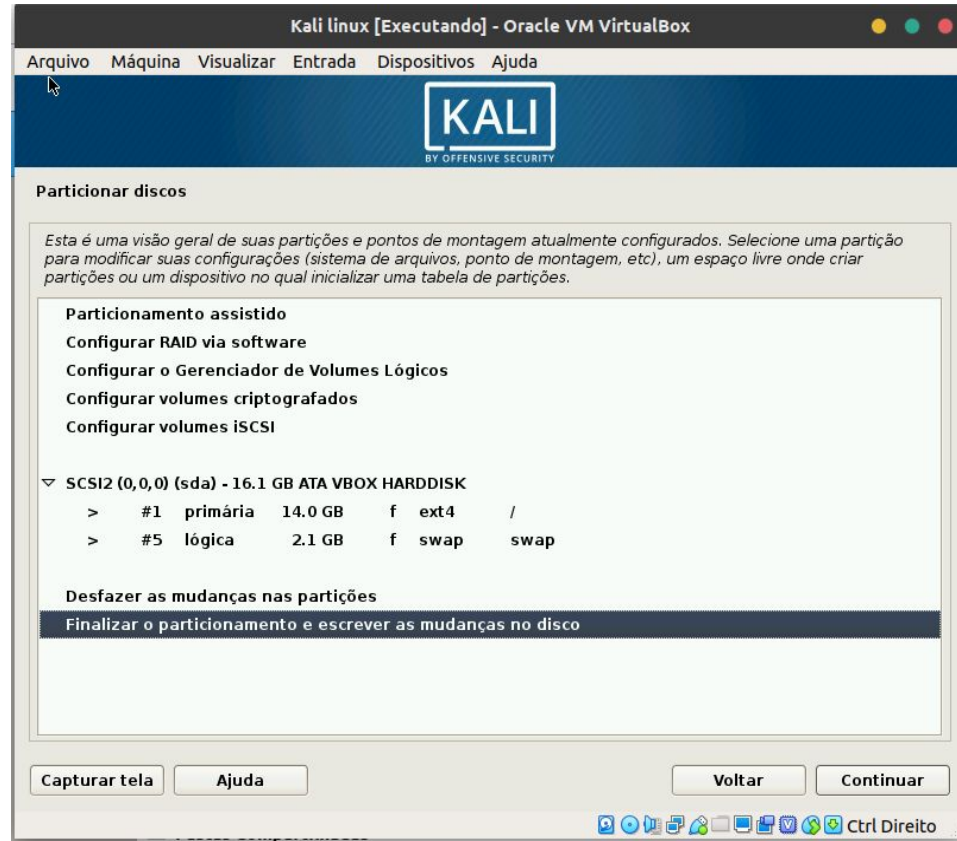


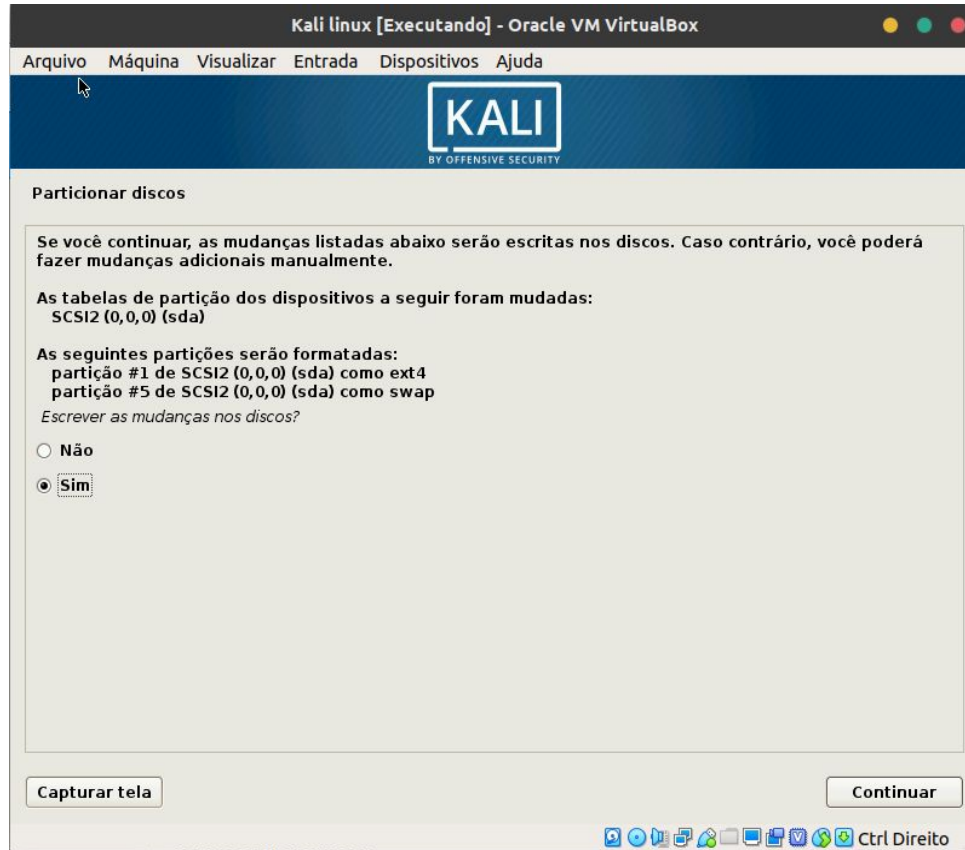


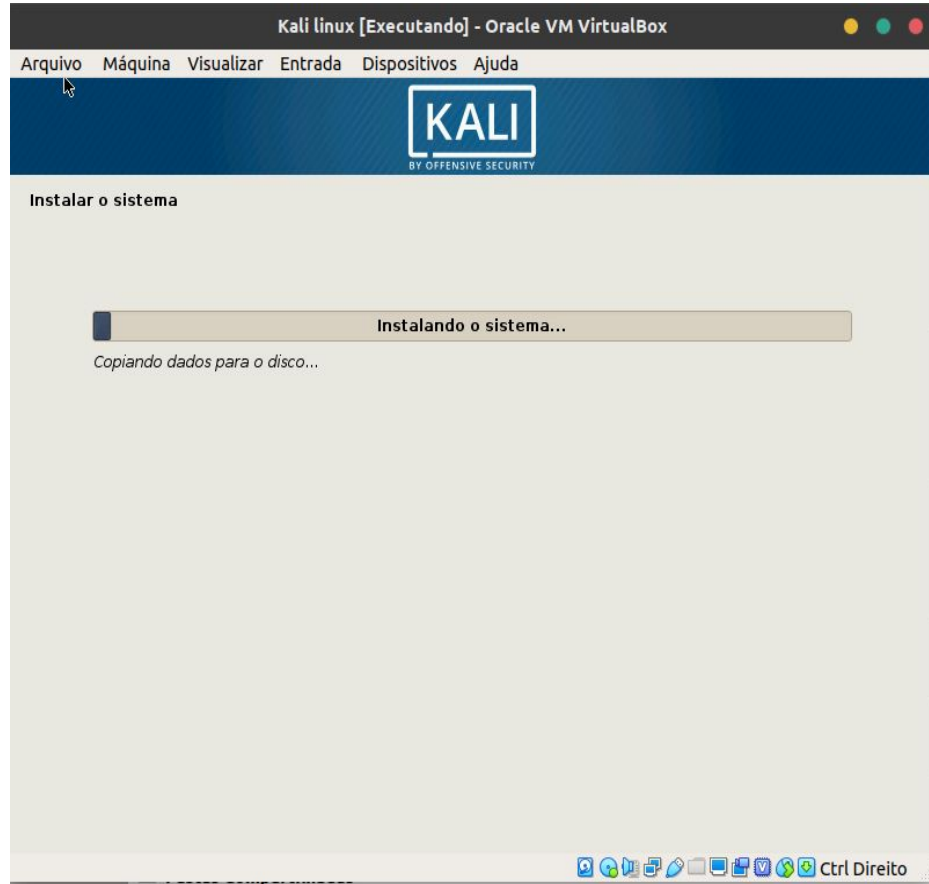


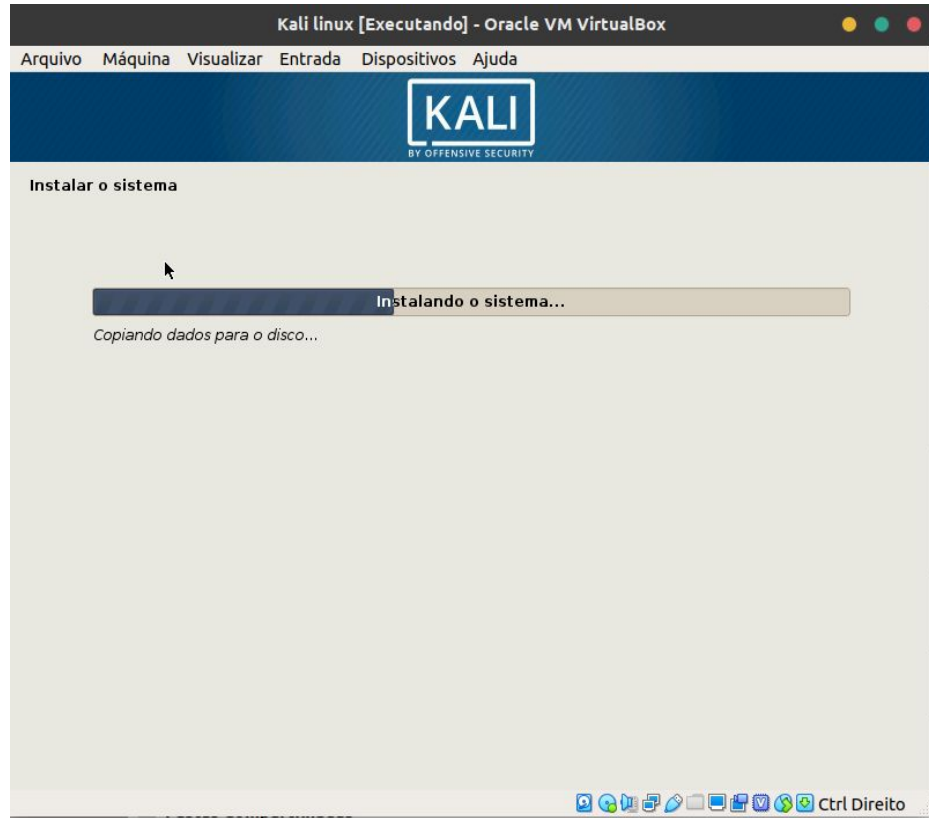


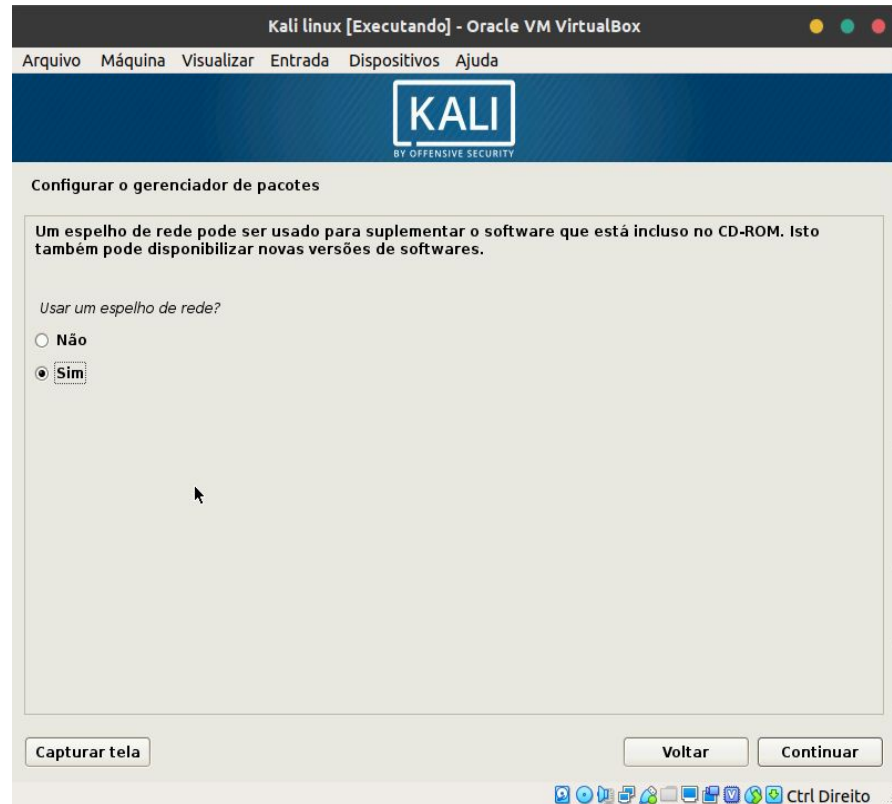


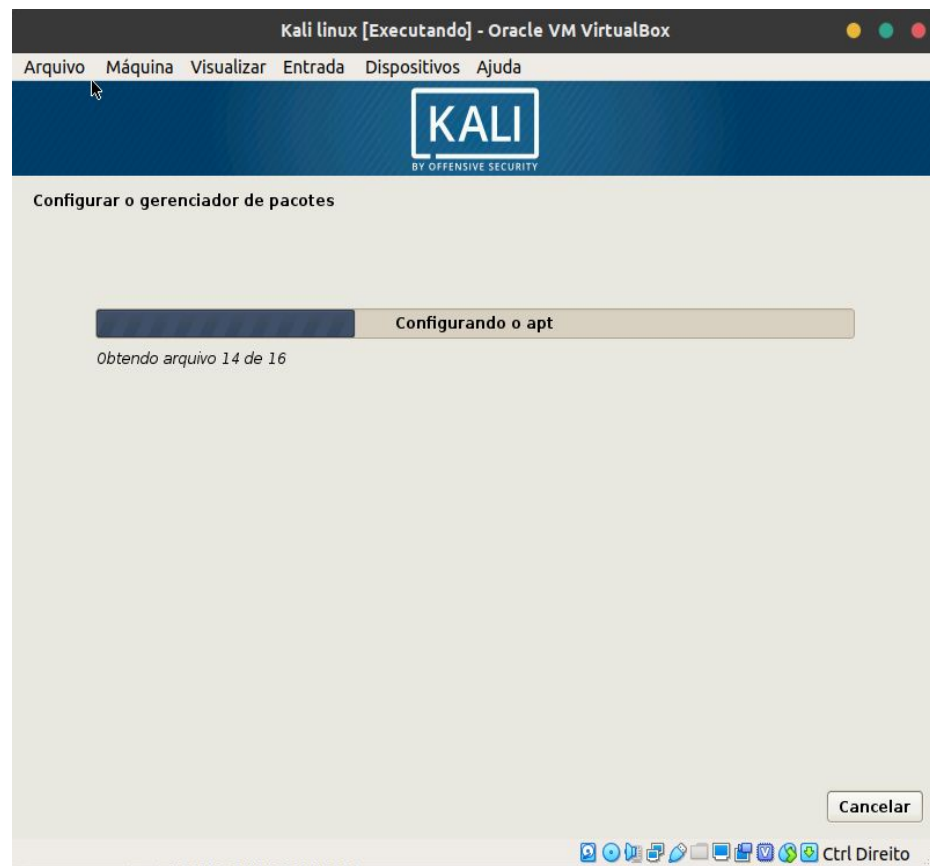


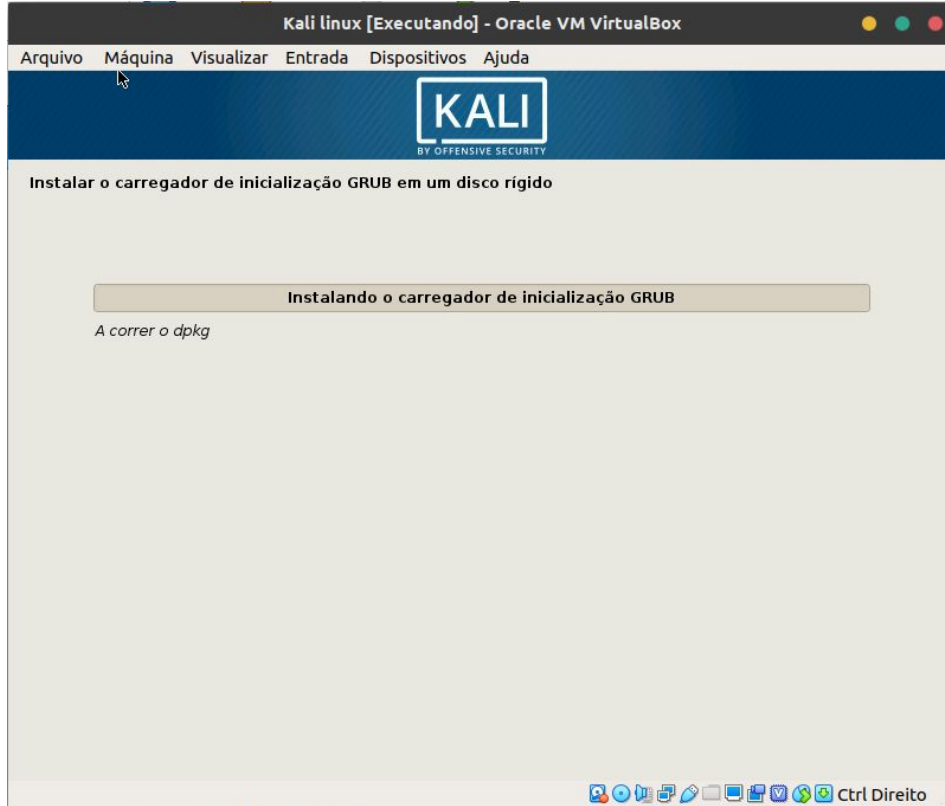


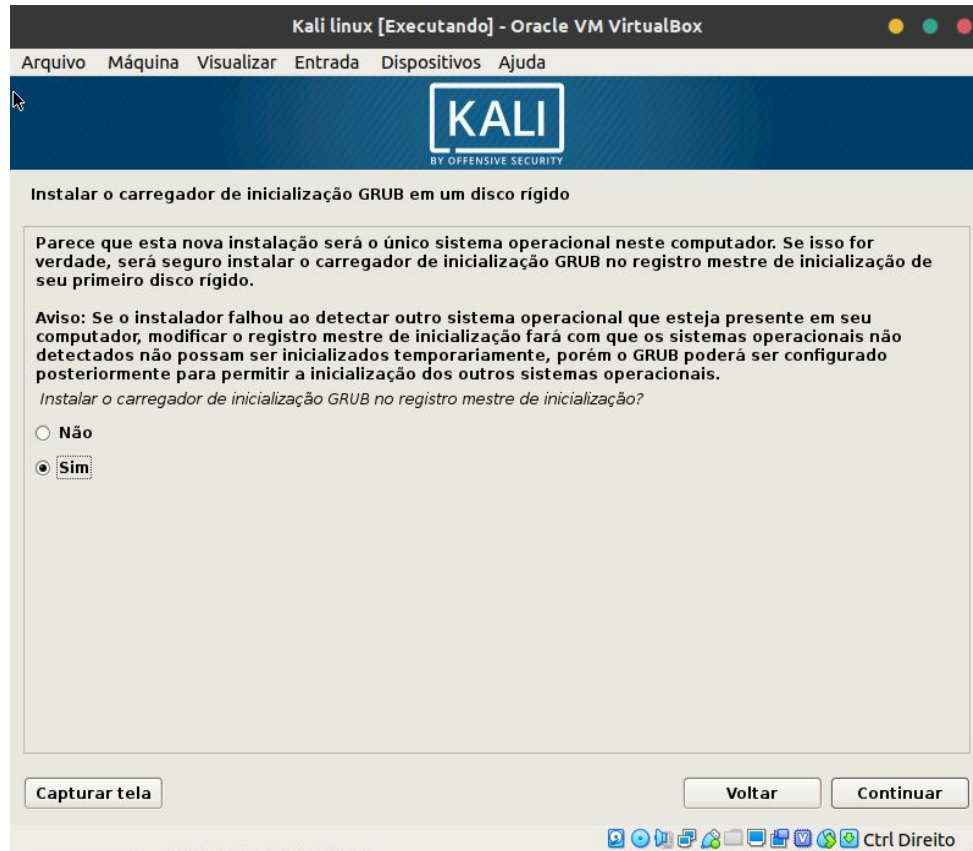


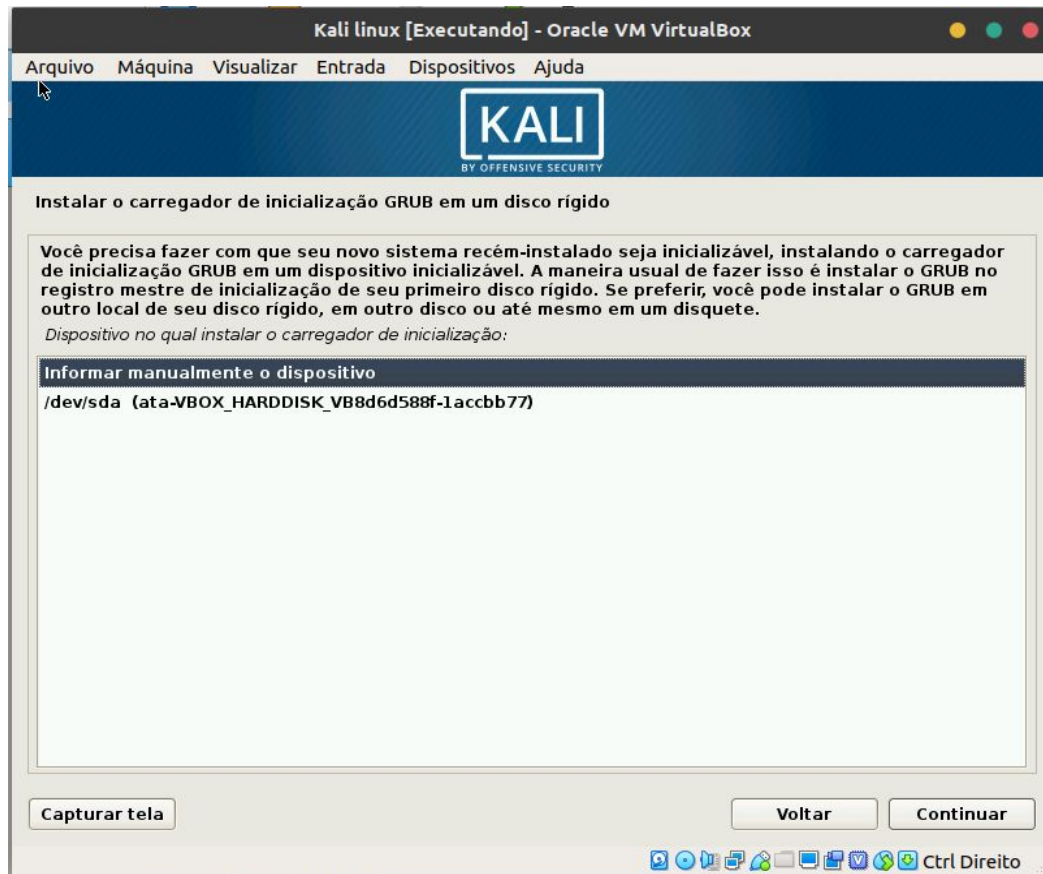


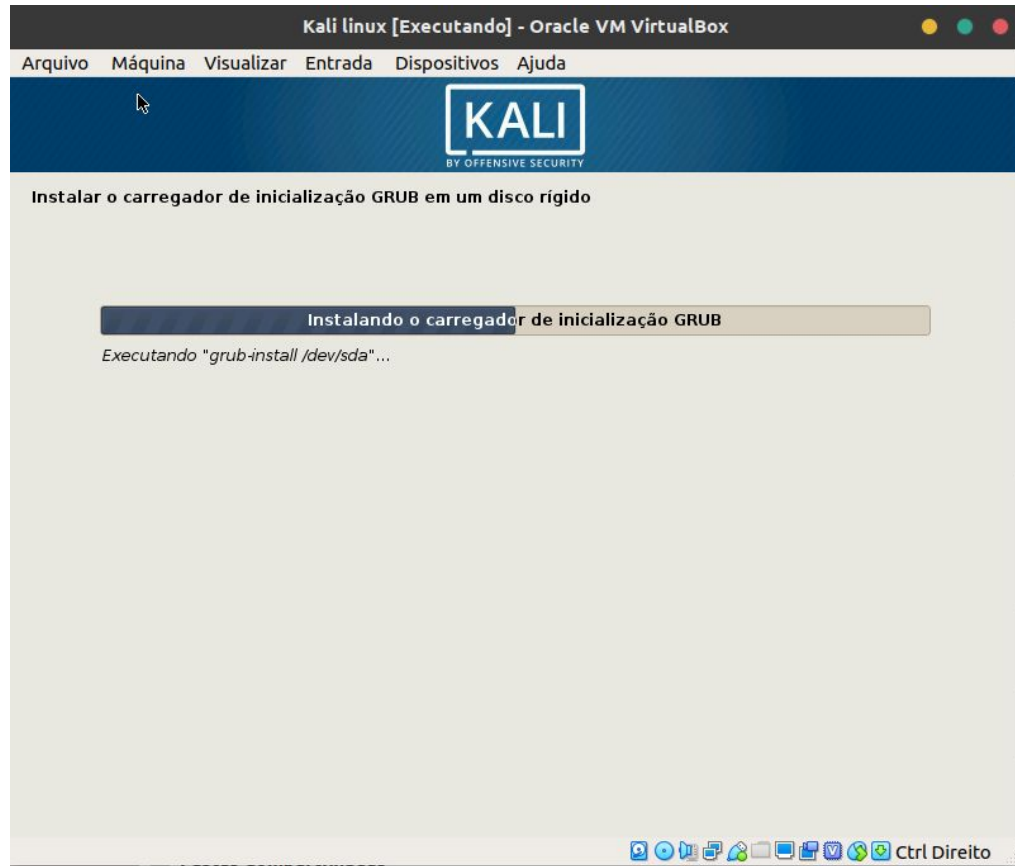


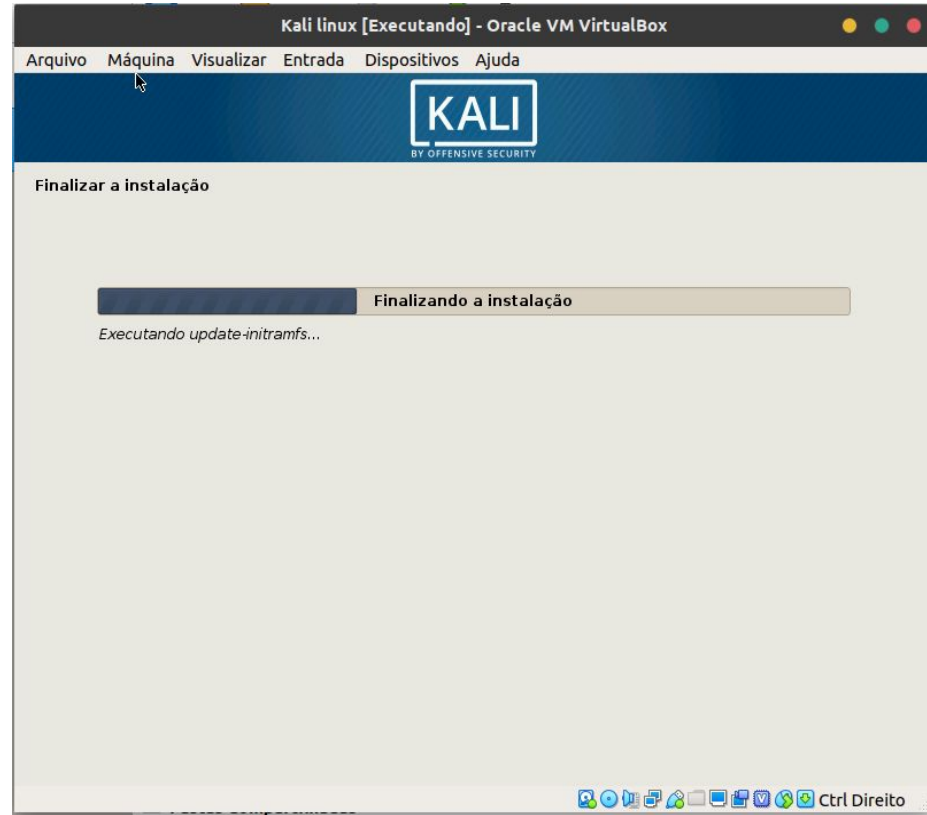


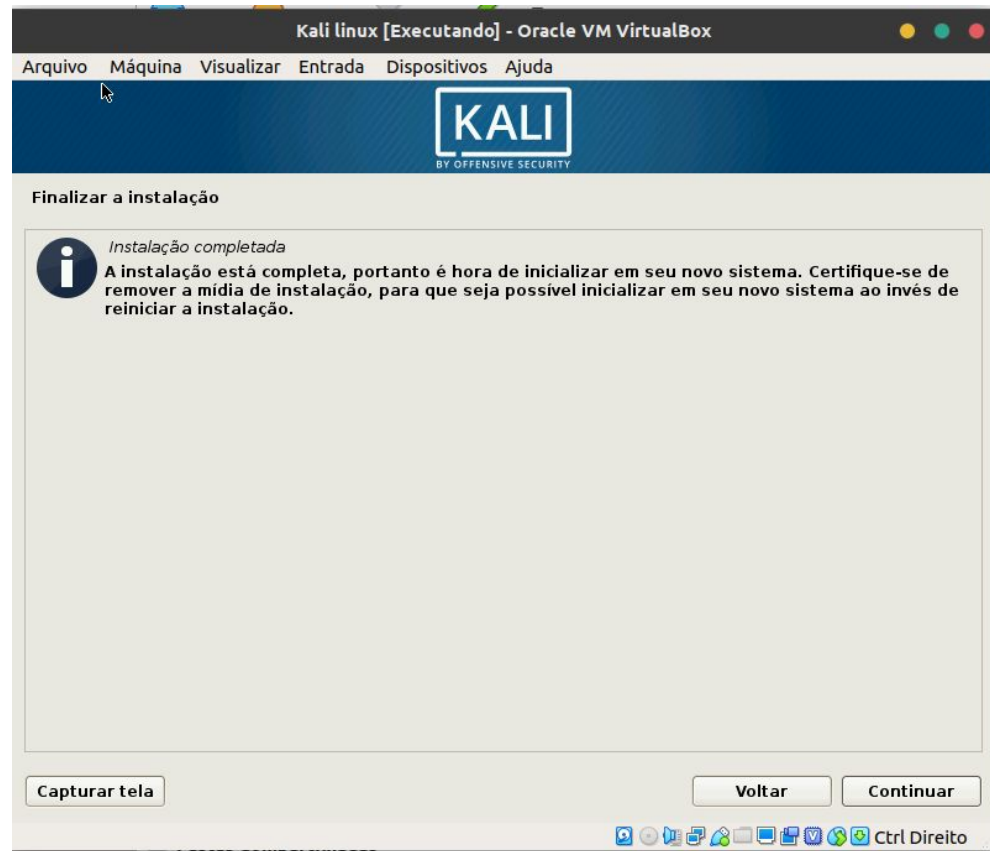


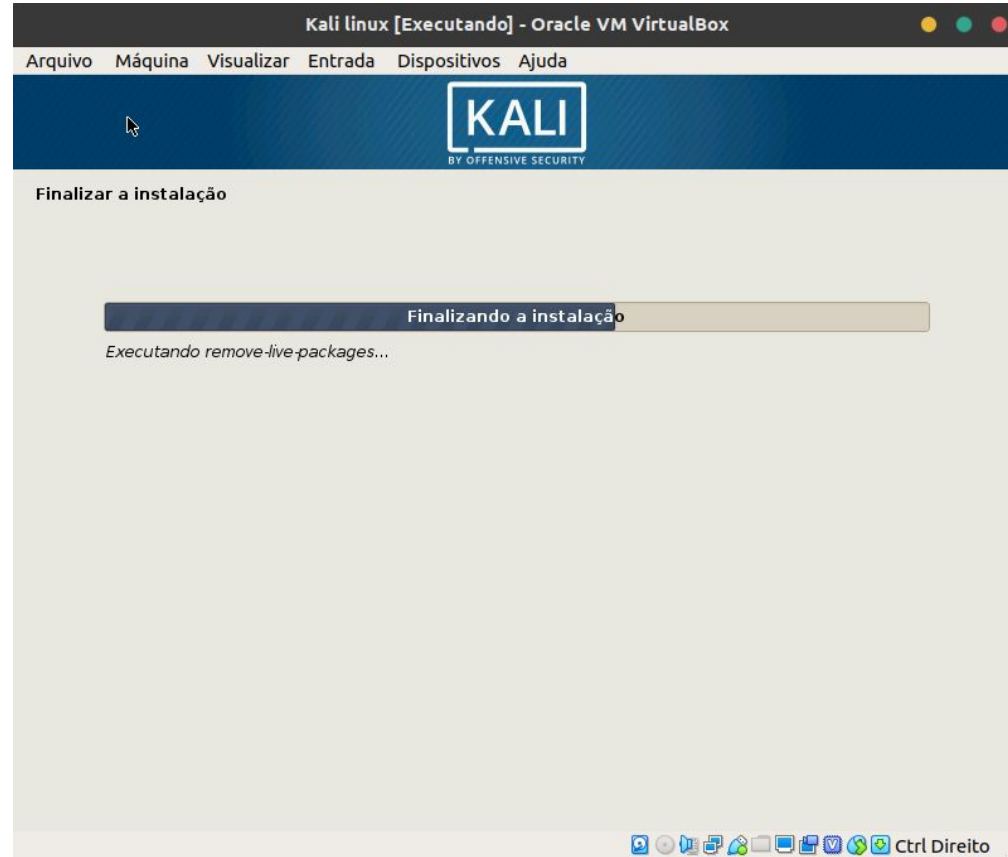


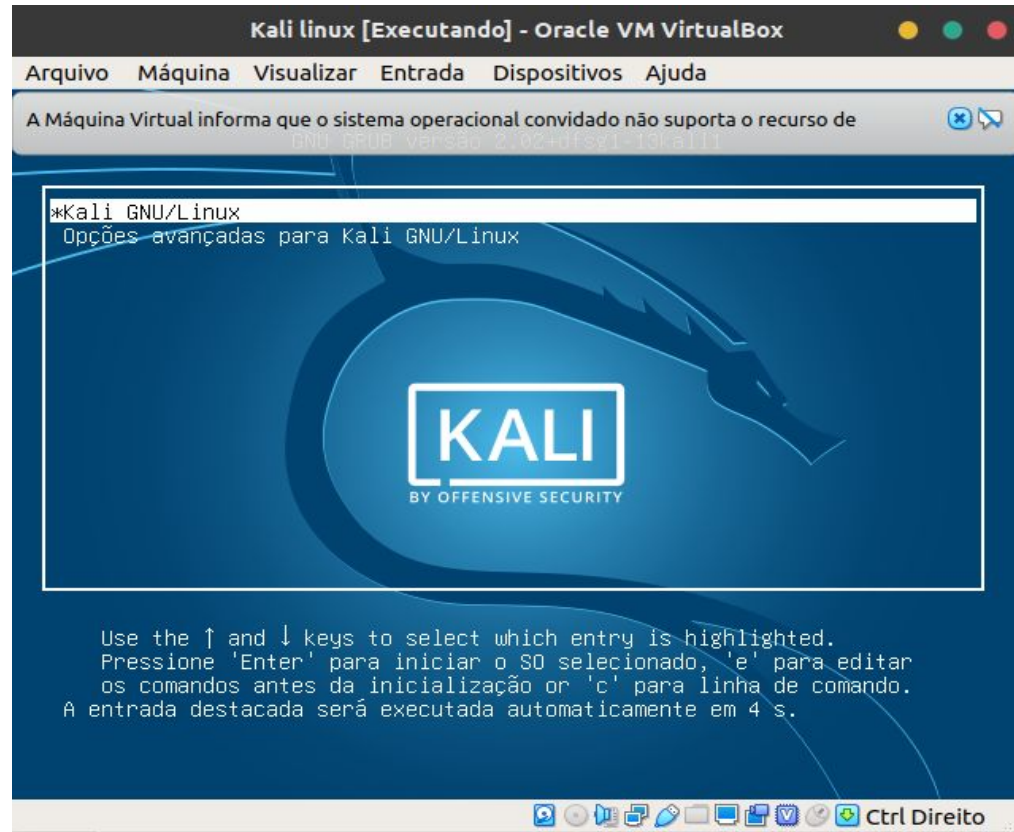


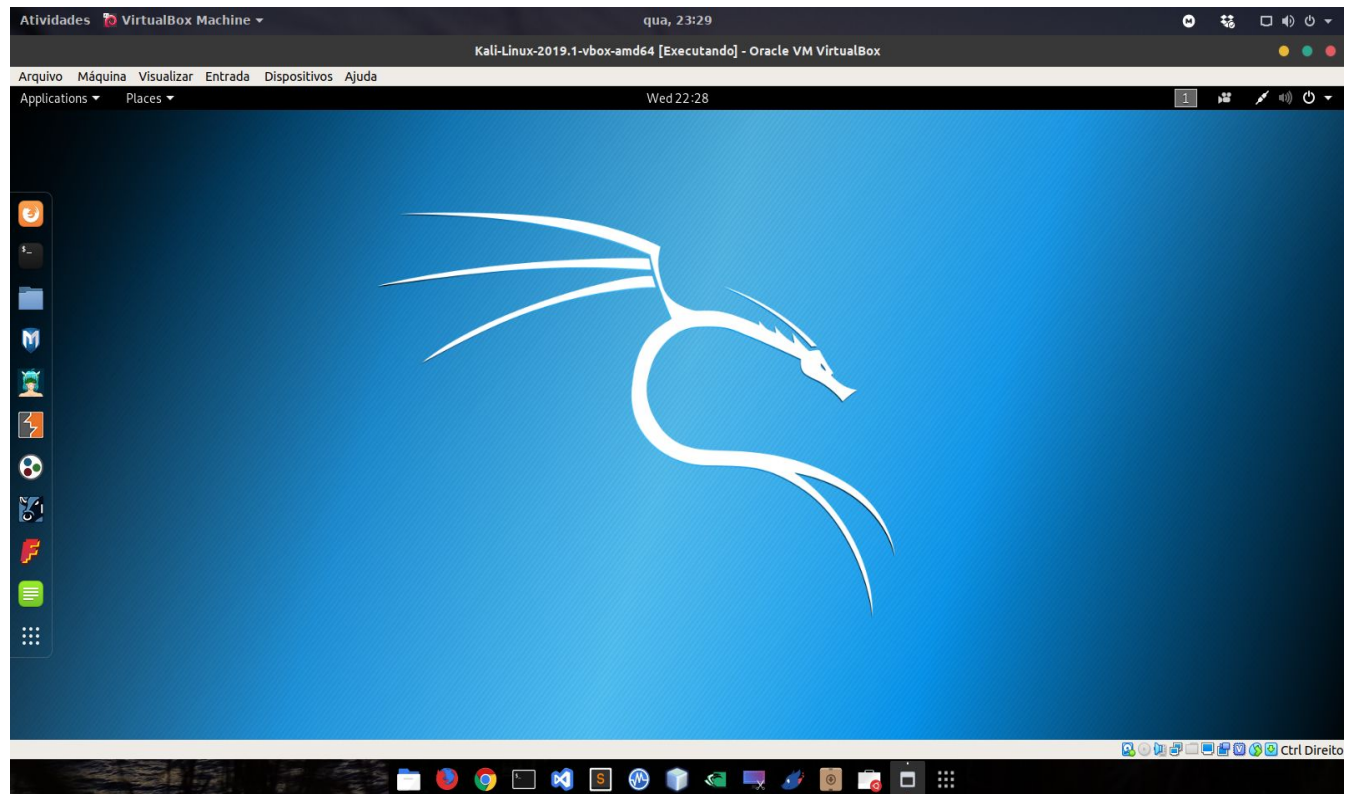












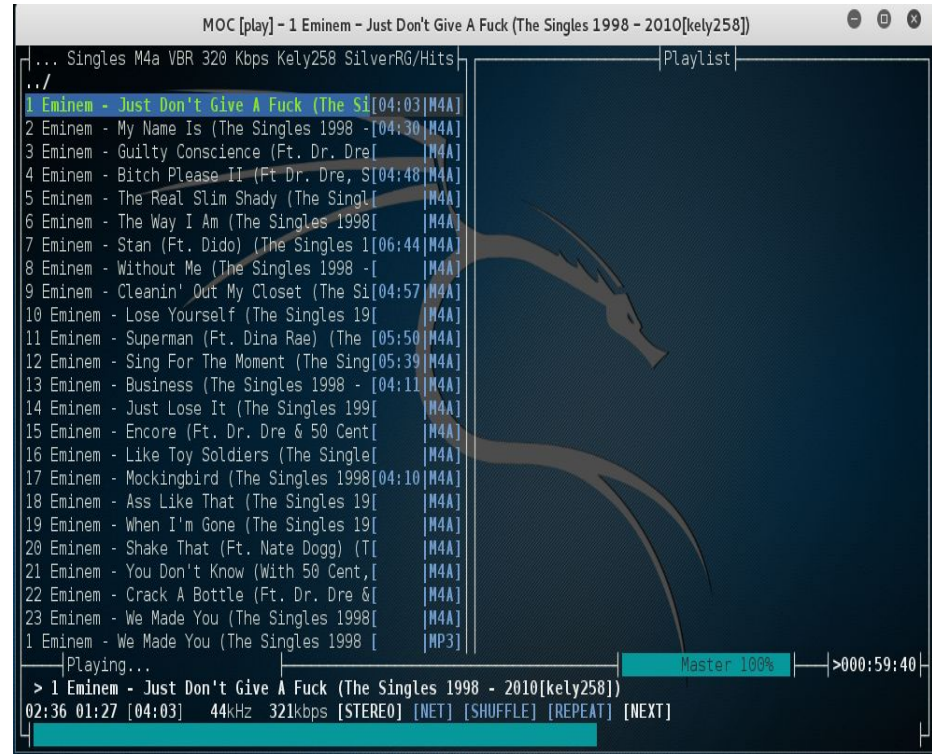
Informações importantes:

- Interface Gráfica: Gnome;
- É uma interface bonita;
- Apresenta um pouco de lentidão;



Acesso ao terminal:

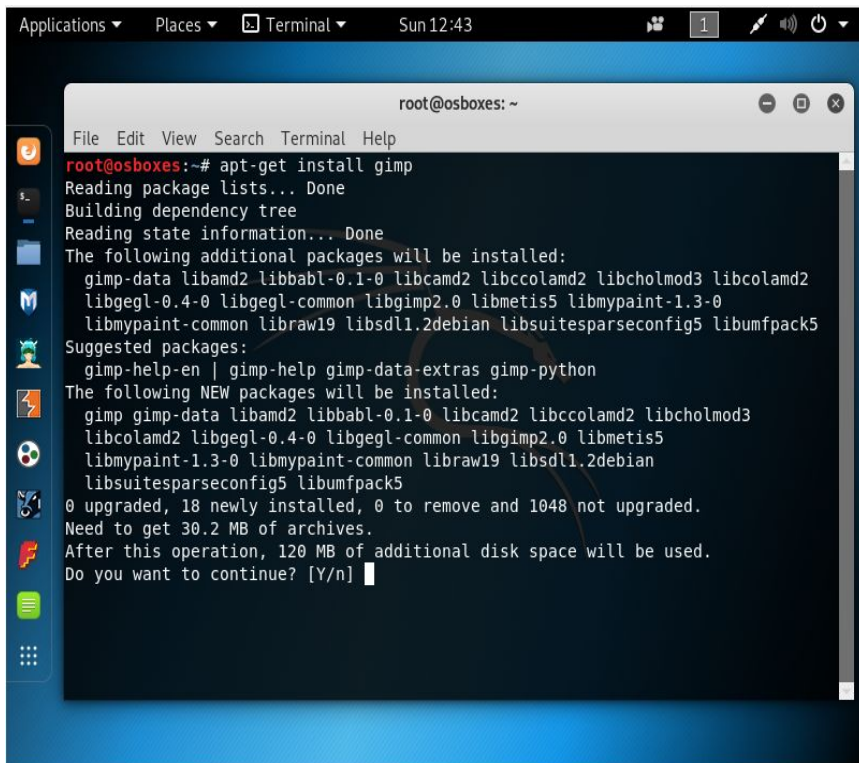
- Ctrl + Alt + T;
- Menu de favoritos;
- Menu mais aplicativos;
- Botão direito, abrir terminal;



Gerenciador de pacotes:

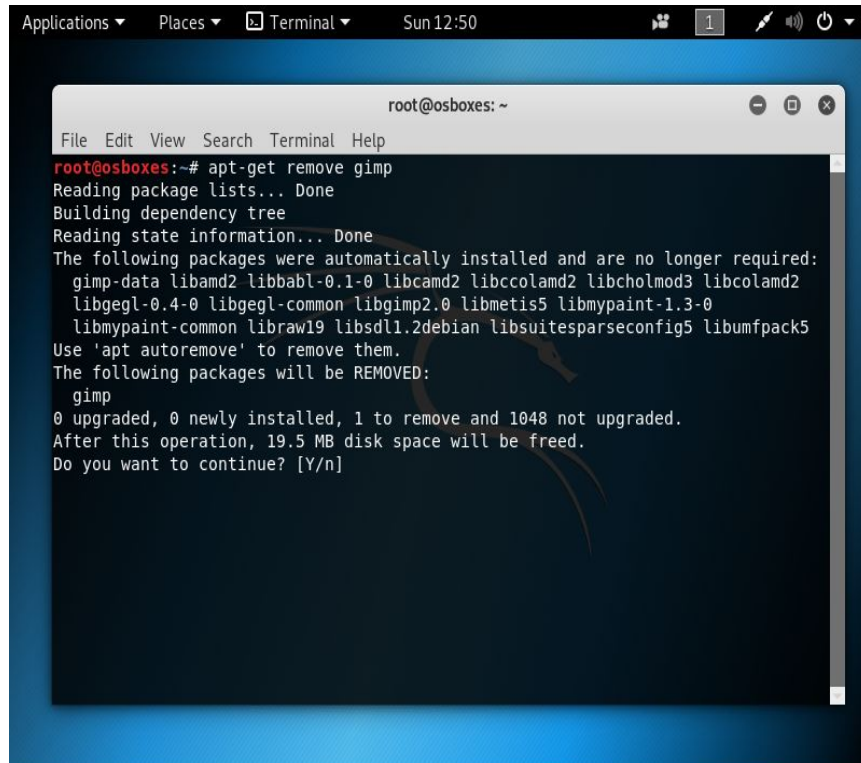
- Apt(Advanced Packaging Tool);

Instalação/desinstalação pelo terminal



A terminal window titled 'root@osboxes: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'apt-get install gimp' and its output. The output indicates that several additional packages will be installed along with gimp, lists them, and shows the disk space requirements. The prompt 'Do you want to continue? [Y/n]' is visible at the bottom with a cursor.

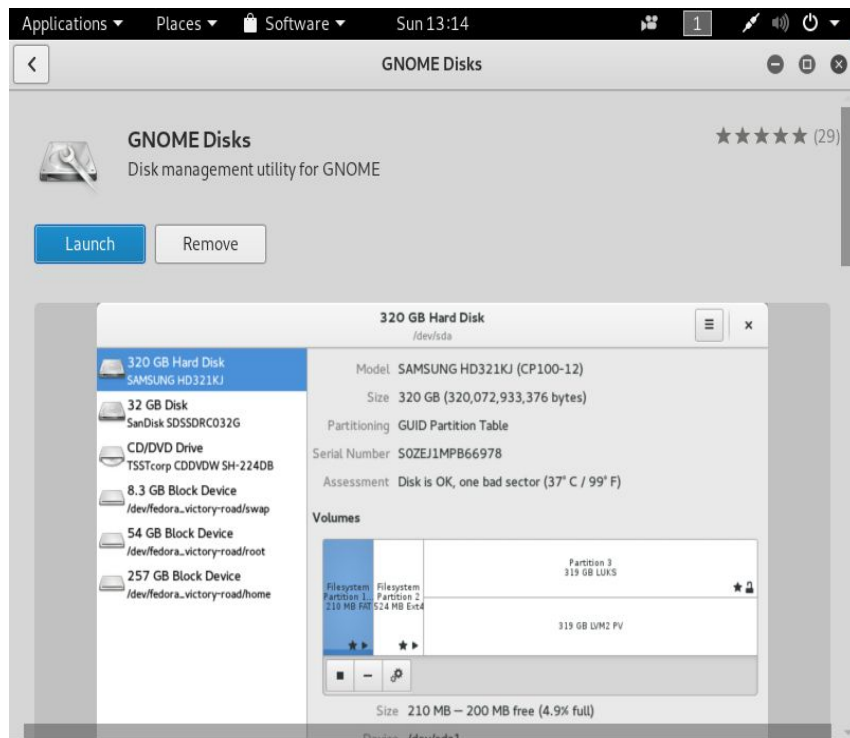
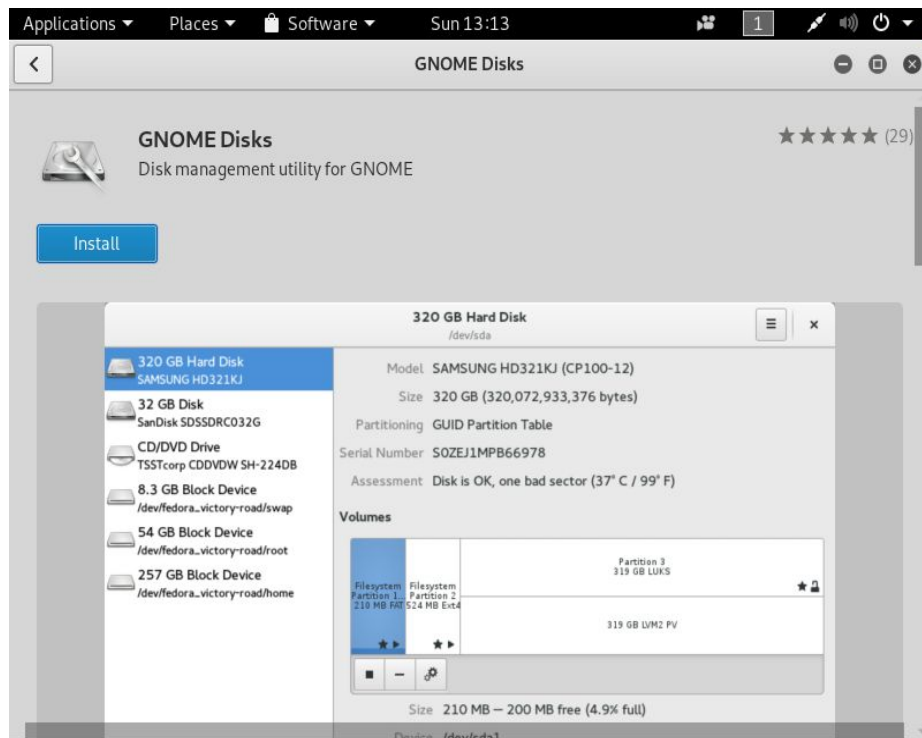
```
root@osboxes:~# apt-get install gimp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  gimp-data libamd2 libbabl-0.1-0 libcamd2 libccolamd2 libcholmod3 libcolamd2
  libgegl-0.4-0 libgegl-common libgimp2.0 libmetis5 libmypaint-1.3-0
  libmypaint-common libraw19 libstdl1.2debian libsuitesparseconfig5 libumfpack5
Suggested packages:
  gimp-help-en | gimp-help gimp-data-extras gimp-python
The following NEW packages will be installed:
  gimp gimp-data libamd2 libbabl-0.1-0 libcamd2 libccolamd2 libcholmod3
  libcolamd2 libgegl-0.4-0 libgegl-common libgimp2.0 libmetis5
  libmypaint-1.3-0 libmypaint-common libraw19 libstdl1.2debian
  libsuitesparseconfig5 libumfpack5
0 upgraded, 18 newly installed, 0 to remove and 1048 not upgraded.
Need to get 30.2 MB of archives.
After this operation, 120 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```



A terminal window titled 'root@osboxes: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'apt-get remove gimp' and its output. The output indicates that gimp and its dependencies will be removed, lists the packages, and shows the disk space to be freed. The prompt 'Do you want to continue? [Y/n]' is visible at the bottom with a cursor.

```
root@osboxes:~# apt-get remove gimp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gimp-data libamd2 libbabl-0.1-0 libcamd2 libccolamd2 libcholmod3 libcolamd2
  libgegl-0.4-0 libgegl-common libgimp2.0 libmetis5 libmypaint-1.3-0
  libmypaint-common libraw19 libstdl1.2debian libsuitesparseconfig5 libumfpack5
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
  gimp
0 upgraded, 0 newly installed, 1 to remove and 1048 not upgraded.
After this operation, 19.5 MB disk space will be freed.
Do you want to continue? [Y/n]
```


Instalação/desinstalação pela interface gráfica



Aplicações essenciais

1. Navegador web -> Chromium, Firefox
2. Bloco de Notas -> Leafpad, Text editor
3. Editor de texto -> Leafpad, Text editor, gVim
4. Apresentação de slides -> não possui
5. Planilha eletrônica -> não possui

Outras informações

1 - Nmap -> Nmap é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker "Fyodor". É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.

site oficial -> https://nmap.org/man/pt_BR/man-examples.html

2 - Metasploit -> é um projeto de segurança de informação com o objetivo de análise de vulnerabilidades de segurança e facilitar testes de penetração (pentests) e no desenvolvimento de assinaturas para sistemas de detecção de intrusos. Está inteiramente integrado ao backtrack e kali linux, distribuições linux atualizadas e modificadas, de acordo com os requisitos de pentest.

698 exploits, 358 módulos auxiliares e 54 módulos de post.

site oficial -> <https://www.metasploit.com>

3 - THC Hydra -> THC Hydra é um cracker de senha muito popular. É uma ferramenta de bypass de login de rede, rápido e estável que usa um dicionário ou ataque de força bruta para tentar várias combinações de senha e login em uma página de login. Ele pode executar ataques rápidos de dicionário contra mais de 50 protocolos, incluindo telnet, FTP, HTTP, https, smb, vários bancos de dados e muito mais.

site de download -> <https://sectools.org/tool/hydra/>

4 - Social Engineer Toolkit -> Esta ferramenta é projetada para executar ataques avançados contra o elemento humano. Os métodos incorporados no kit de ferramentas são projetados para serem ataques direcionados e focados contra uma pessoa ou organização usada durante um teste de penetração. Envolve phishing, coleta de informações, clonagem de dados, etc.

5 - Ettercap -> O Ettercap é uma ferramenta de segurança de rede gratuita e de código aberto para ataques man-in-the-middle na LAN . Ele pode ser usado para análise de protocolos de rede de computadores e auditoria de segurança . Ele é executado em vários sistemas operacionais semelhantes ao Unix , incluindo Linux , Mac OS X , BSD e Solaris , e no Microsoft Windows . Ele é capaz de interceptar tráfego em um segmento de rede, capturar senhas e conduzir escuta ativa contra vários protocolos comuns. Seus desenvolvedores originais posteriormente fundados Equipe de hackers .

Dupla:

Pedro Henrique Da Silva

Luiz Felipe Da Silva