

Treinamento em Teste de Invasão com Backtrack/Kali

Módulo 1 – Introdução ao Processo de Teste de Invasão e Kali Linux

Instrutor: Daniel Araújo Melo – dnl.amelo@gmail.com

Roteiro de Instalação do Kali

1. Introdução

Este roteiro apresenta como instalar o Kali Linux 1.0 (<http://www.kali.org>), em uma Máquina Virtual (VM – *Virtual Machine*) do hipervisor Virtualbox (<https://www.virtualbox.org/>).

A instalação do Virtualbox está fora do escopo deste roteiro.

A VM do Kali faz parte de um conjunto de VMs que serão utilizadas no decorrer do treinamento, simulando uma rede vulnerável sendo analisada pelo Kali, como pode ser observado na Figura 1.

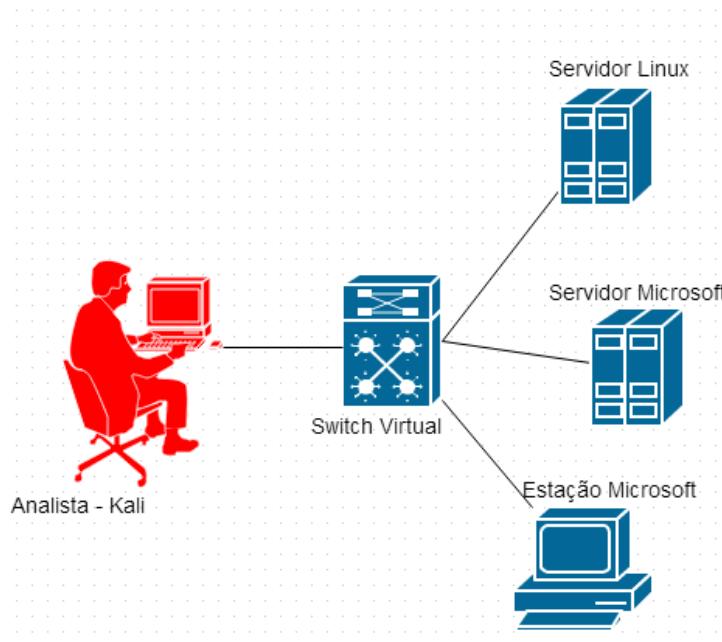


Figura 1: Topologia do Laboratório

2. Instalação do Kali

2.1 Execute o Gerenciador do Virtualbox (Figura 2).

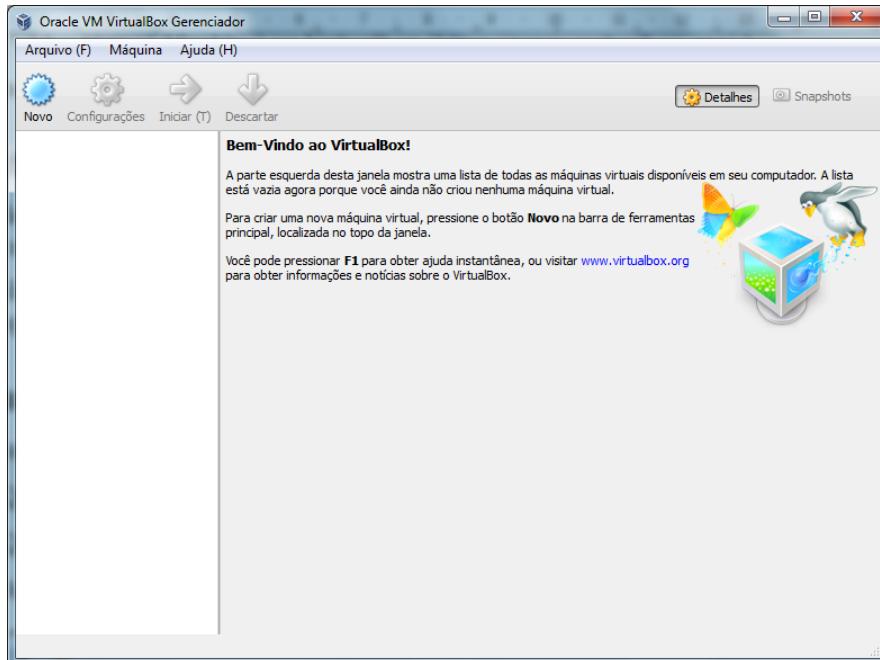


Figura 2: Gerenciador do Virtualbox

2.2 Clique em “*Novo*” para instalar uma nova VM e preencha a janela “*Criar Máquina Virtual*” com as informações a seguir, e selecione “*Próximo (N)*” - Figura 3:

- Nome: *Kali Linux 1.0.3*
- Tipo: *Linux*
- Versão: *Debian*

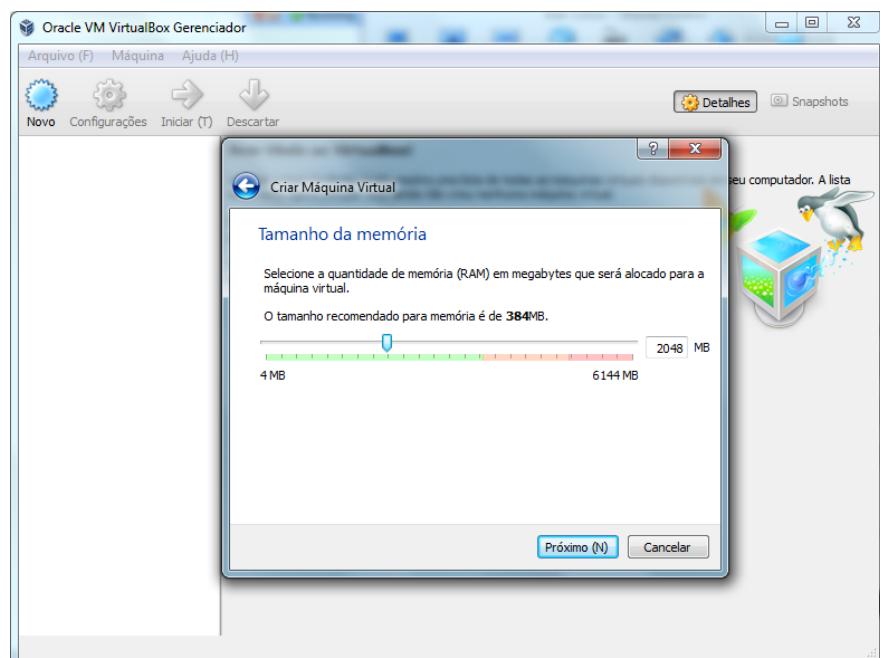


Figura 3: Quantidade de Memória RAM

2.3 Configure a quantidade de memória RAM da VM com 2048 MB. Em seguida selecione “Próximo (N)” - (Figura 4).

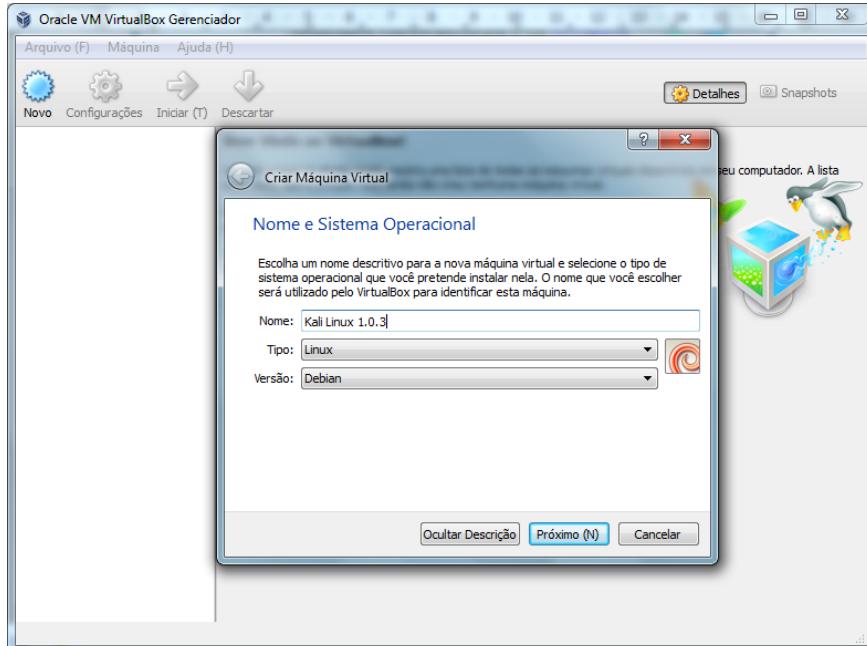


Figura 4: Criar nova Máquina Virtual - Passo 1

2.4 Selecione a opção “Criar um disco rígido virtual agora” e clique em “Criar” - (Figura 5)

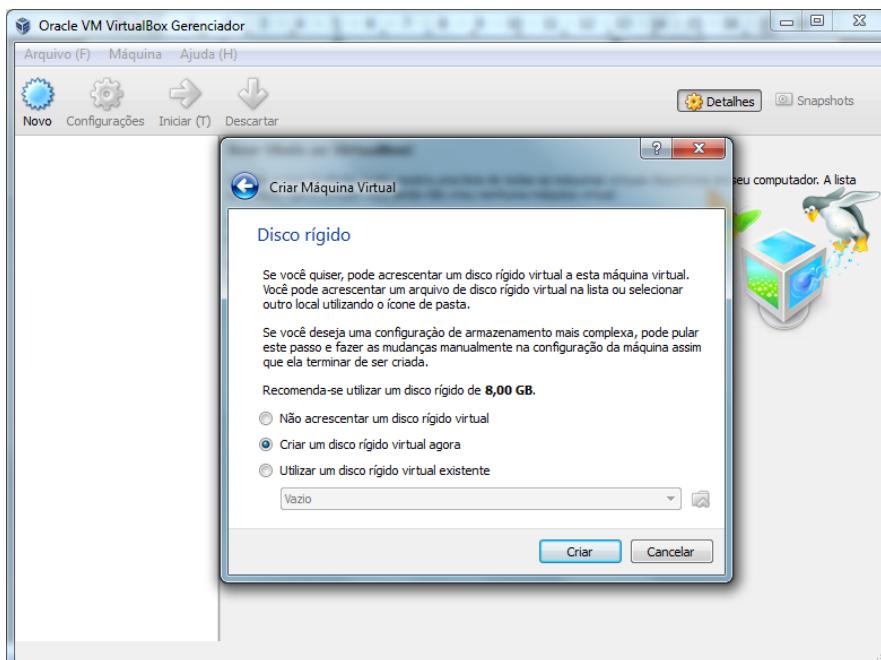


Figura 5 - Disco Rígido

2.5 Selecione a opção “VDI” e clique em “Próximo (N)” - (Figura 6).

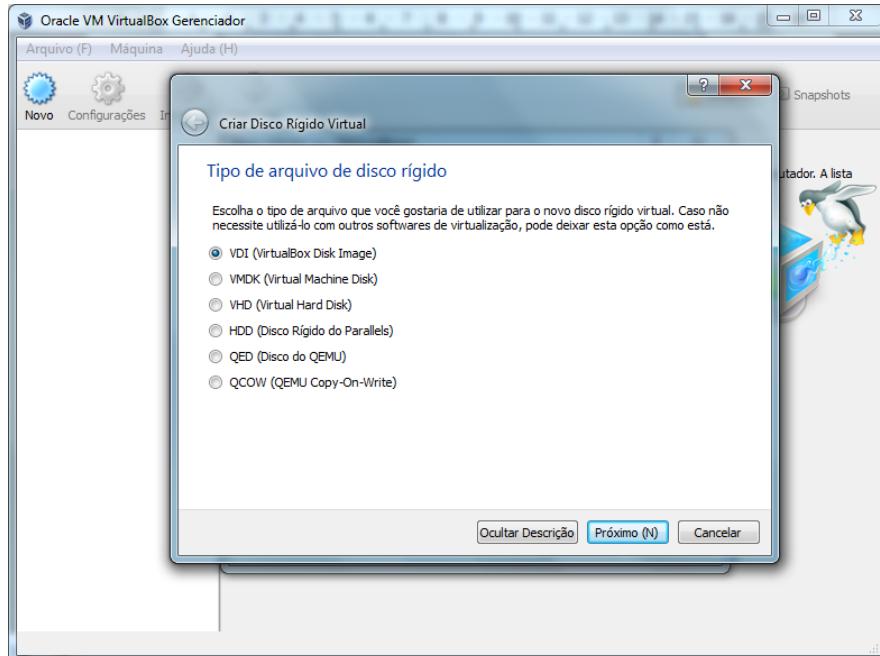


Figura 6 - Tipo de arquivo do disco rígido

2.6 Selecione a opção “*Dinamicamente Alocado*” e clique em “*Próximo (N)*” - (Figura 7). Com esta opção, o arquivo do disco rígido virtual crescerá dinamicamente de acordo com sua ocupação.



Figura 7 - Tipo de Armazenamento.

2.7 Mantenha o nome do arquivo (“*Kali Linux 1.0.3*”), configure o tamanho do arquivo para “*20,00 GB*” e clique em “*Criar*”. O arquivo será criado na pasta padrão do Virtualbox. - (Figura 8). Vale lembrar que o arquivo iniciará com um tamanho mínimo necessário para a instalação e crescerá de acordo com sua ocupação.

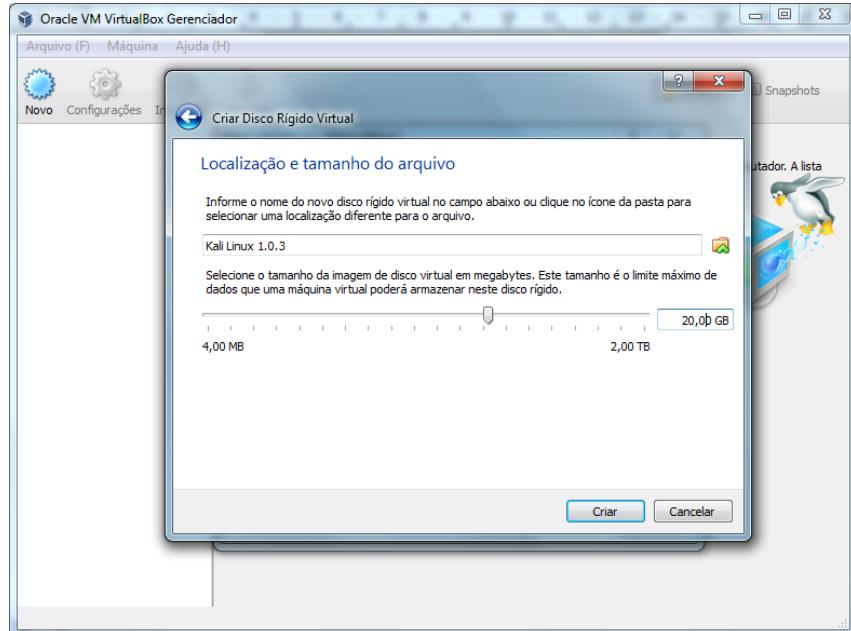


Figura 8 - Localização e tamanho do arquivo

2.8 Em seguida o Gerenciador apresentará a VM do Kali Linux criada. (Figura 9). A instalação ainda não finalizou e ainda é necessário configurar a VM, a partir do item **2.9**.

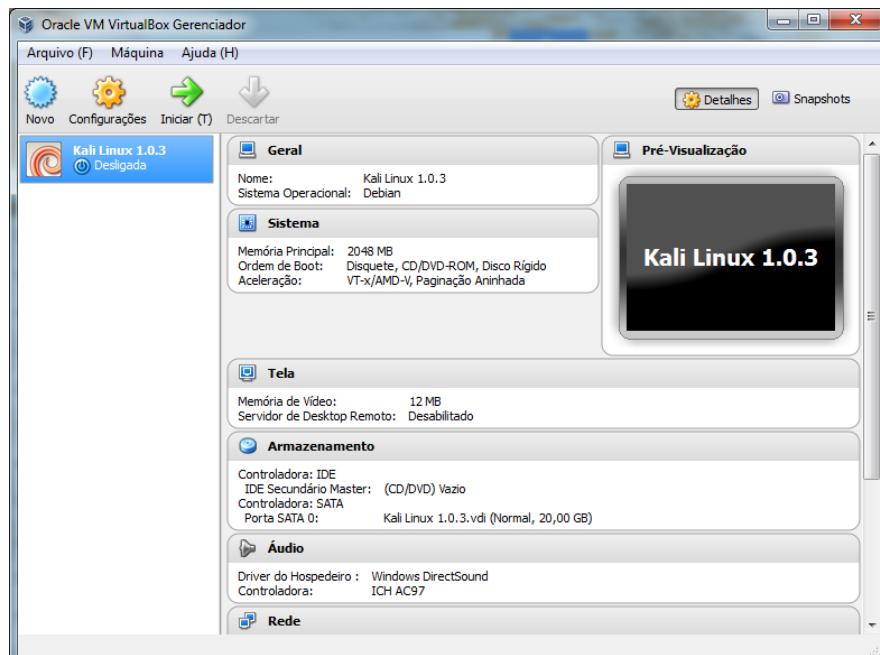


Figura 9 - Gerenciador do Virtualbox apresentando a VM do Kali.

2.9 Selecione a VM do Kali e clique em “*Configurações*”. Na barra lateral esquerda da janela de

configuração, selecione a opção “*Geral*”. Em seguida, na aba “*Avançado*” parametrize da seguinte forma (Figura 10) – **Atenção! Não clique em OK**.

- Área de transferência compartilhada: *Bi-direcional*;
- Arrastar e soltar (D): *Bi-direcional*;

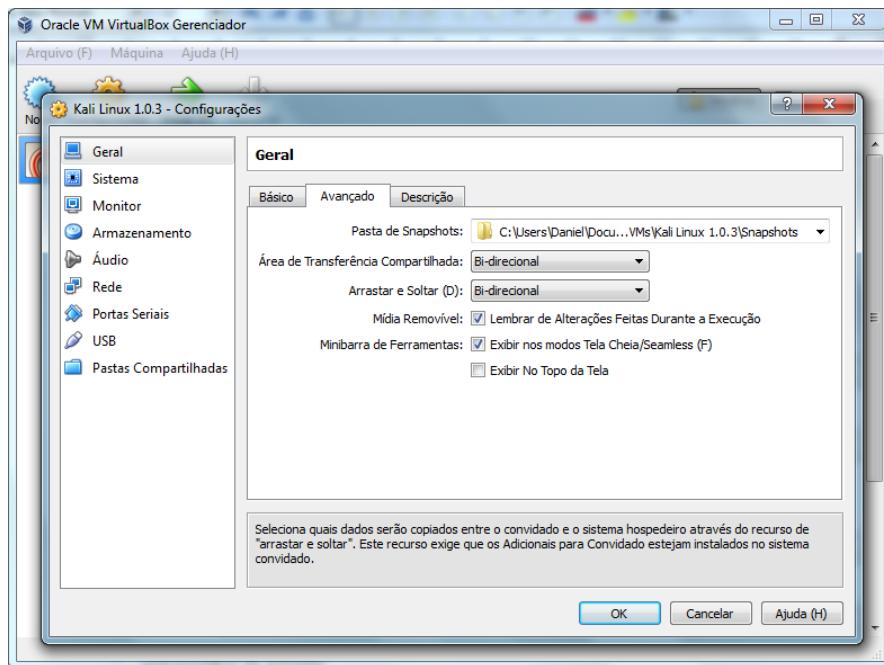


Figura 10 - Configurações - Geral

2.10 Selecione a opção “Sistema”. Na aba “*Placa-Mãe*” selecione o check-box “*Habilitar o I/O Apic*” (Figura 11).

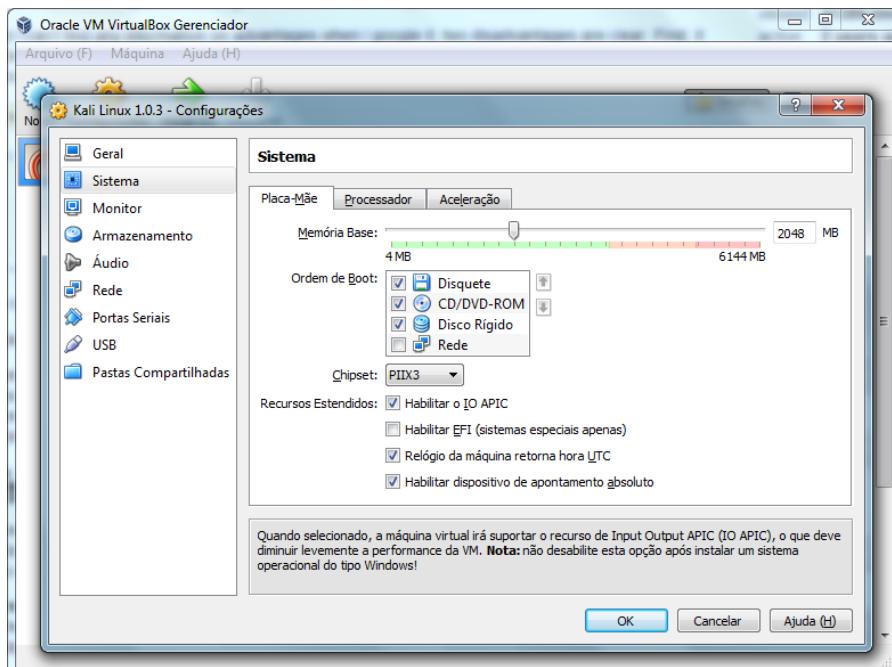


Figura 11 - Configurações - Sistema

Esta opção (I/O APIC) deve ser usada em sistemas de 64 bits e quando mais de um processador virtual for utilizado.

2.11 Na opção “*Sistema*”, selecione a aba “*Processador*” e habilite 2 processadores (Figura 12).

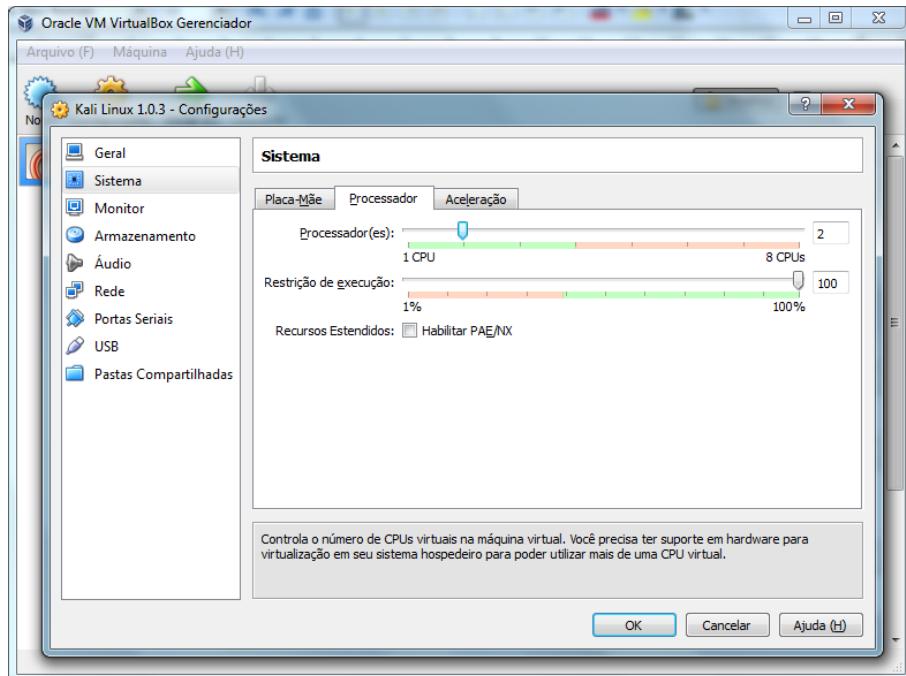


Figura 12 - Configurações - Sistema - Processador

2.12 Selecione a opção “*Armazenamento*” na barra lateral esquerda. Observe que no painel com a “Árvore de Armazenamento” existe uma “*Controladora: IDE*” com um CD/DVD vazio. (Figura 13).

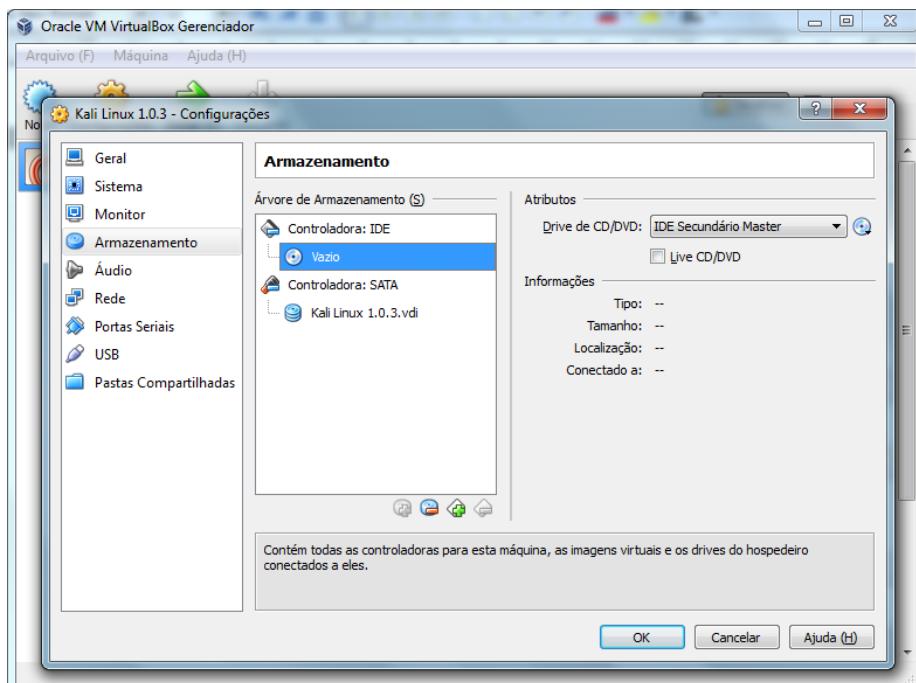


Figura 13 - Configurações - Armazenamento

2.13 Ainda na opção “Armazenamento”, selecione o CD/DVD vazio, no painel direito clique na imagem do CD/DVD e selecione a opção “Selecionar um arquivo de CD/DVD virtual”. (Figura 14). Ao abrir a janela de navegação nas pastas, selecione o seguinte arquivo, disponível no diretório material_modulo_1.

- *kali-linux-1.0.3-i386.iso*

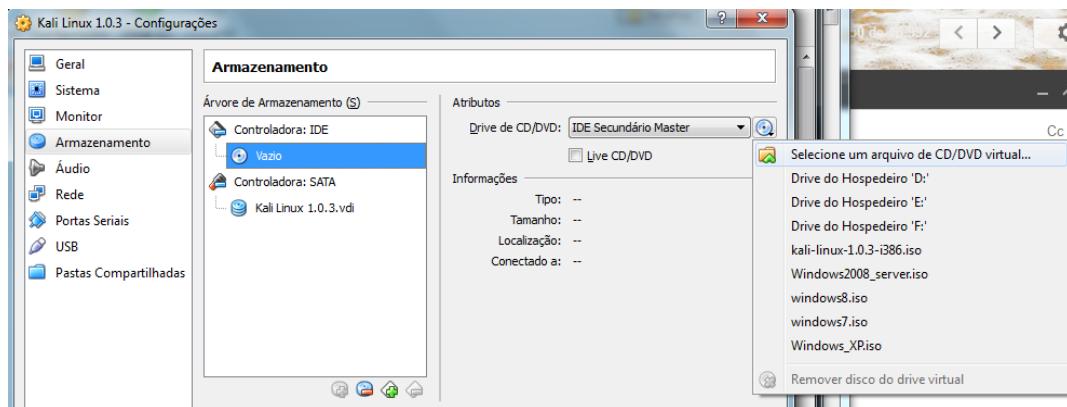


Figura 14 - Configurações – Armazenamento – Selecionando DVD Virtual

2.14 Após selecionar o arquivo “.iso”, a “Árvore de Armazenamento” apresentará o referido arquivo, como um CD/DVD Virtual. (Figura 15).

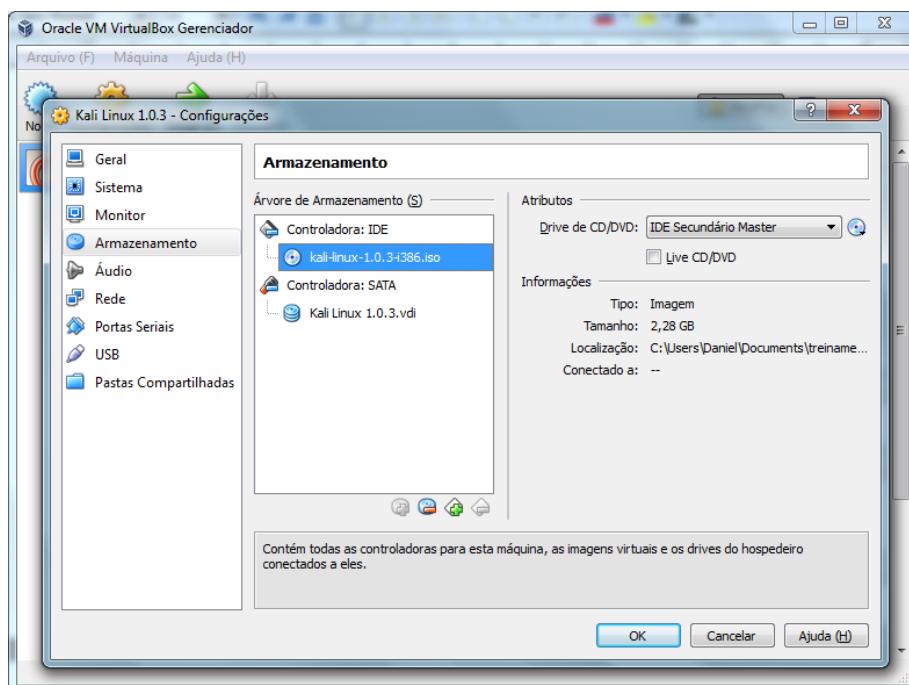


Figura 15 - DVD Virtual com instalador do Kali Linux 1.0.3

2.15 Selecione a opção “Rede”, no painel lateral esquerdo. Mantenha o adaptador 1 habilitado com a opção “Conectado a:” com o valor “NAT”. Selecione a aba “Adaptador 2”, habilite o adaptador através do checkbox “Habilitar Placa de Rede” e a opção “Conectado a” com o valor “Placa de rede exclusiva do Hospedeiro (host-only)” (Figura 16).

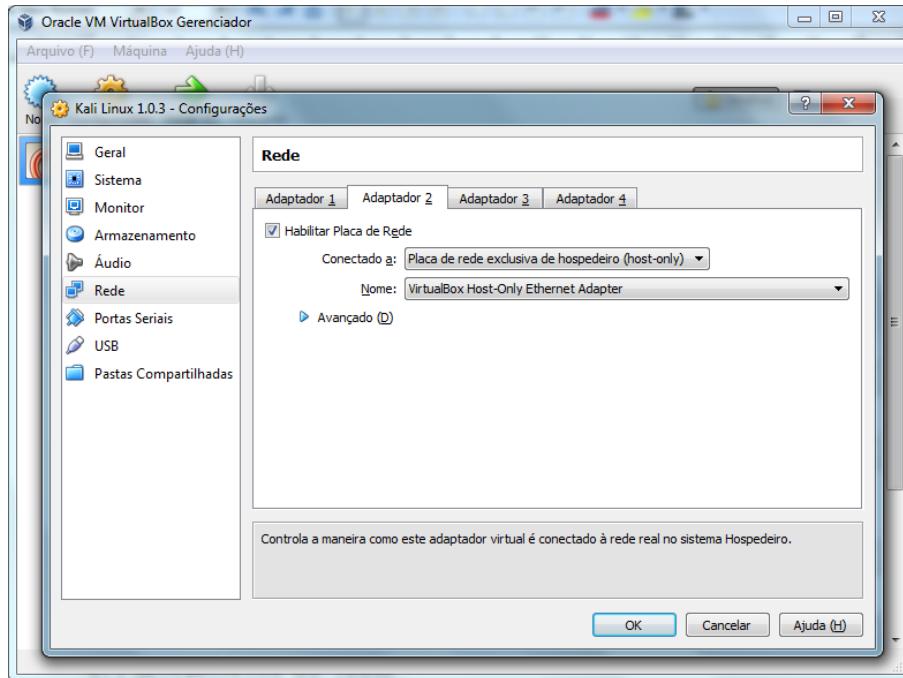


Figura 16 - Configurações – Rede - Adaptadores

Resumindo, teremos 2 adaptadores de rede:

- Adaptador 1 – será utilizado para acessar a Internet e realizar consultas em serviços públicos – configurado como “*NAT*”;
- Adaptador 2 – utilizado para disparar varreduras e ataques para as outras VMs do laboratório – configurado como “*Host-only*”

2.16 O recurso de Pasta Compartilhada permite que o sistema hospedeiro compartilhe uma pasta com a VM, recurso necessário para evitar a duplicação de arquivos, ao copiar entre hospedeiro e VM. Selecione a opção “Pastas Compartilhadas” e acrescente um compartilhamento clicando no botão de adição de pastas, localizado no lado direito da janela. Será necessário informar o caminho para a pasta que será compartilhada e o nome do compartilhamento (Figura 17). Utilize:

- “*Caminho da Pasta*”: Caminho para diretório com o material do treinamento;
- “*Nome da Pasta*”: Nome do Compartilhamento

Em seguida, clique em OK na janela “*Acrescentar Compartilhamento*” e OK na janela “*Configurações*”.

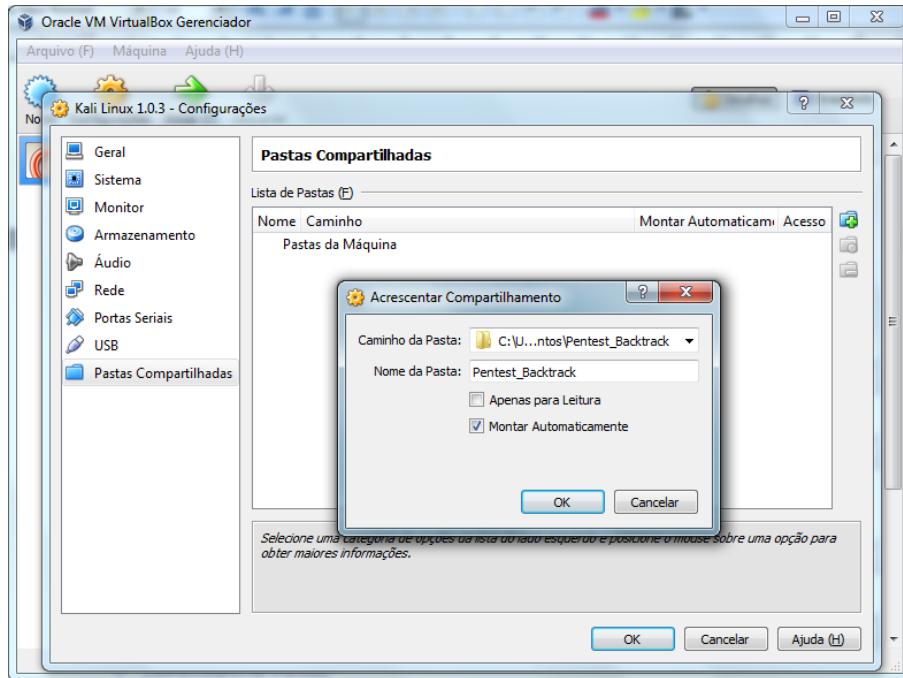


Figura 17 - Configurações – Pastas Compartilhadas

2.17 Após a finalização da configuração da VM, verifique se as configurações estão de acordo com o apresentado na Figura 18. Caso alguma configuração esteja incorreta, você ainda pode alterá-la utilizando o botão “Configurações” no painel superior.

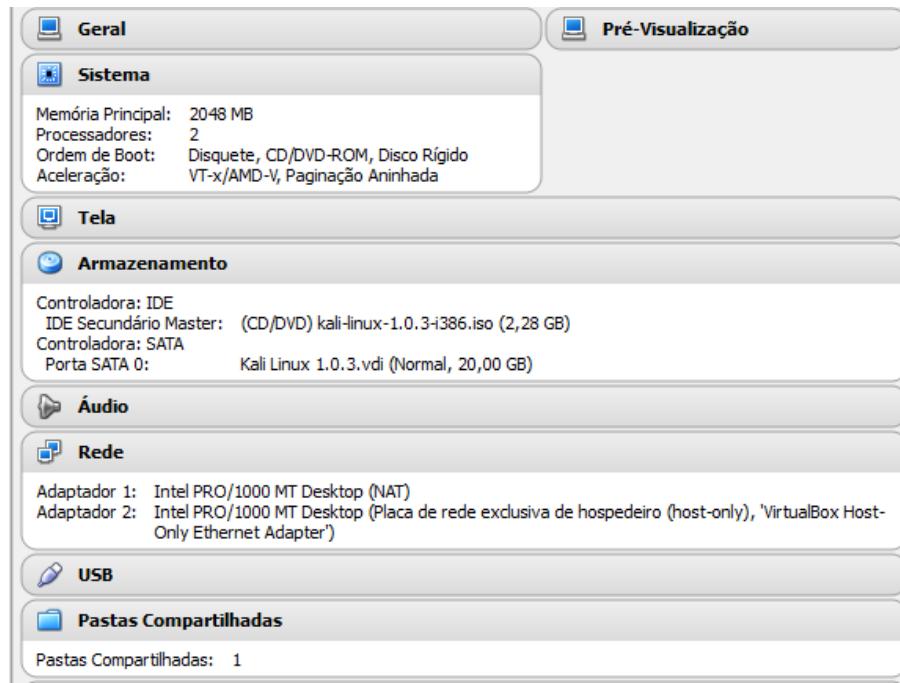


Figura 18 - Configuração da VM

2.18 Ao inicializar a VM pela primeira vez, a inicialização (boot) carregará o SO a partir do DVD virtual. A tela inicial apresentará o menu de Boot do Kali. Utilize o teclado para selecionar a opção “Graphical Install” e pressione Enter – (Figura 19).

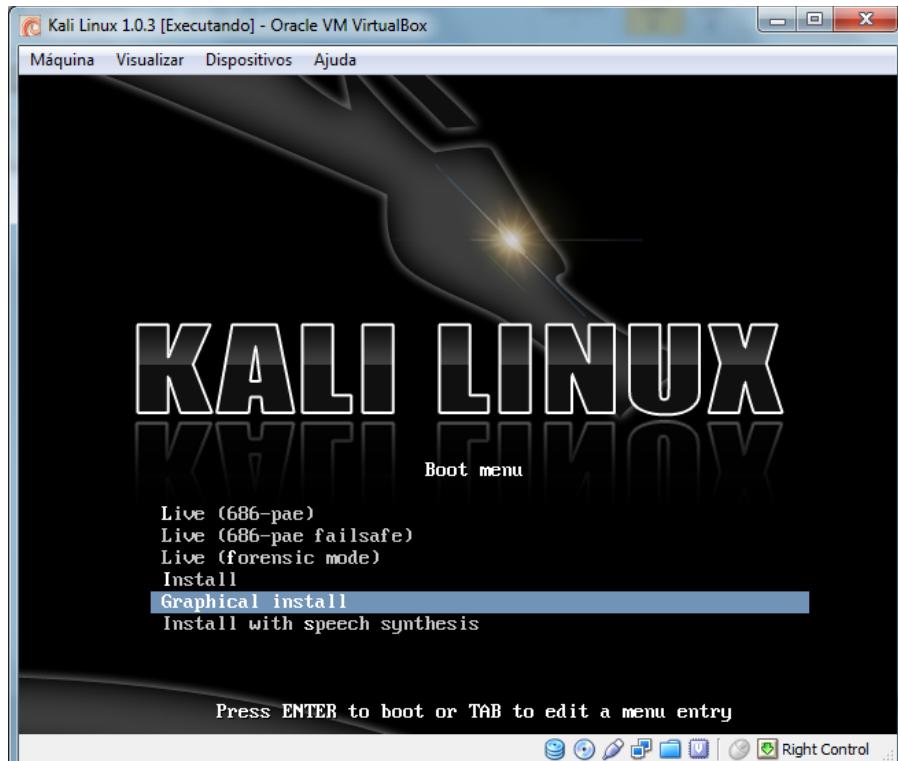


Figura 19 - Menu de Boot do Kali Linux

2.19 Selecione a opção de idioma “Portuguese (Brazil) – Português do Brasil” e clique em “Continue” - (Figura 20).

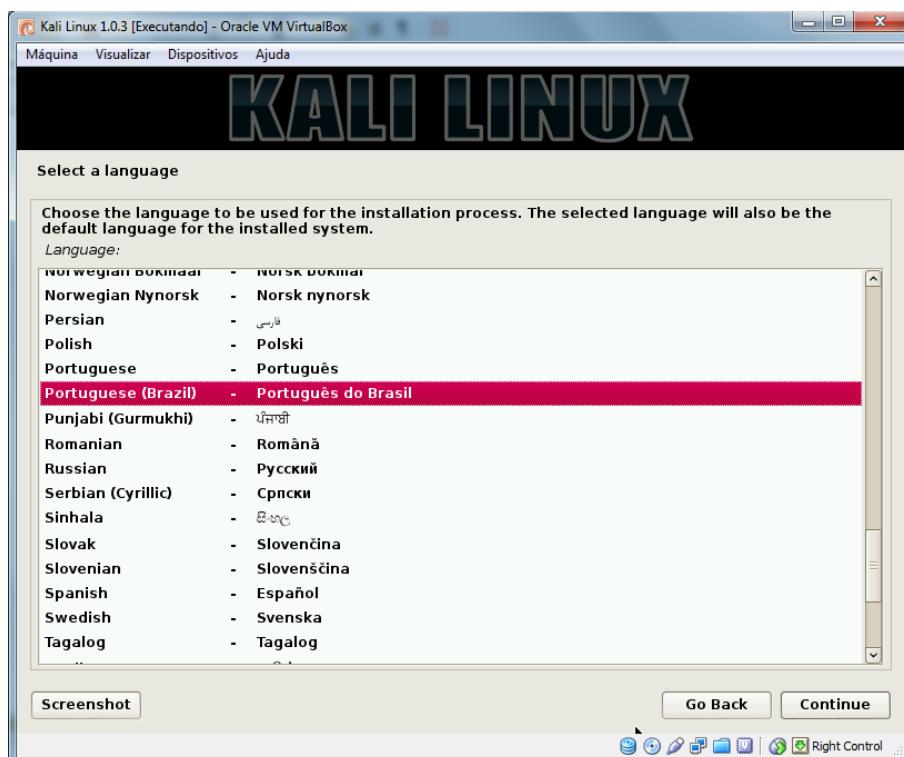


Figura 20 - Seleção de Idioma

2.20 Selecione sua localidade, provavelmente “*Brasil*” (Figura 21), e clique em “*Continuar*”.

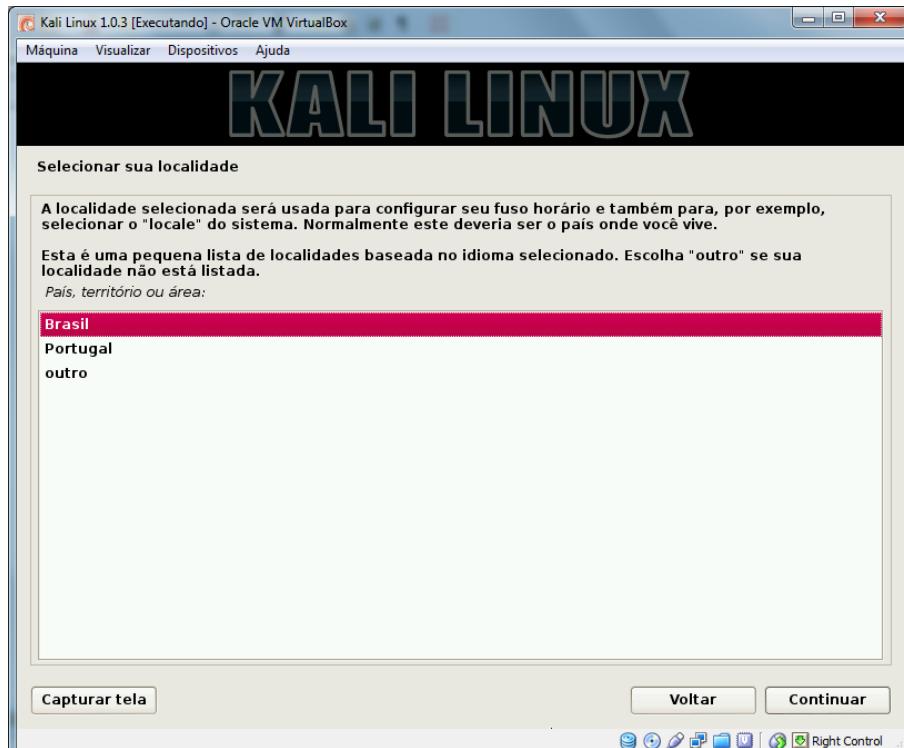


Figura 21 - Seleção de Localidade

2.21 Selecione o teclado de acordo com o que você está utilizando, provavelmente “*Português Brasileiro*”, e clique em “*Continuar*” - (Figura 22).

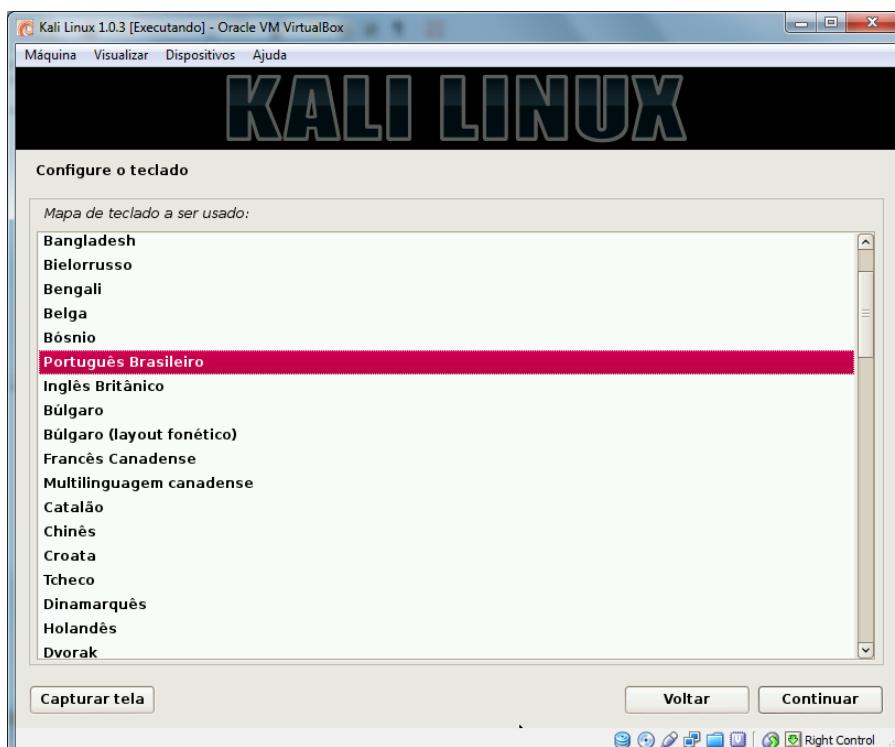


Figura 22 - Seleção do teclado

2.22 – Em seguida você poderá acompanhar a instalação do sistema através de uma barra de carregamento – (Figura 23) - Aguarde até o final.

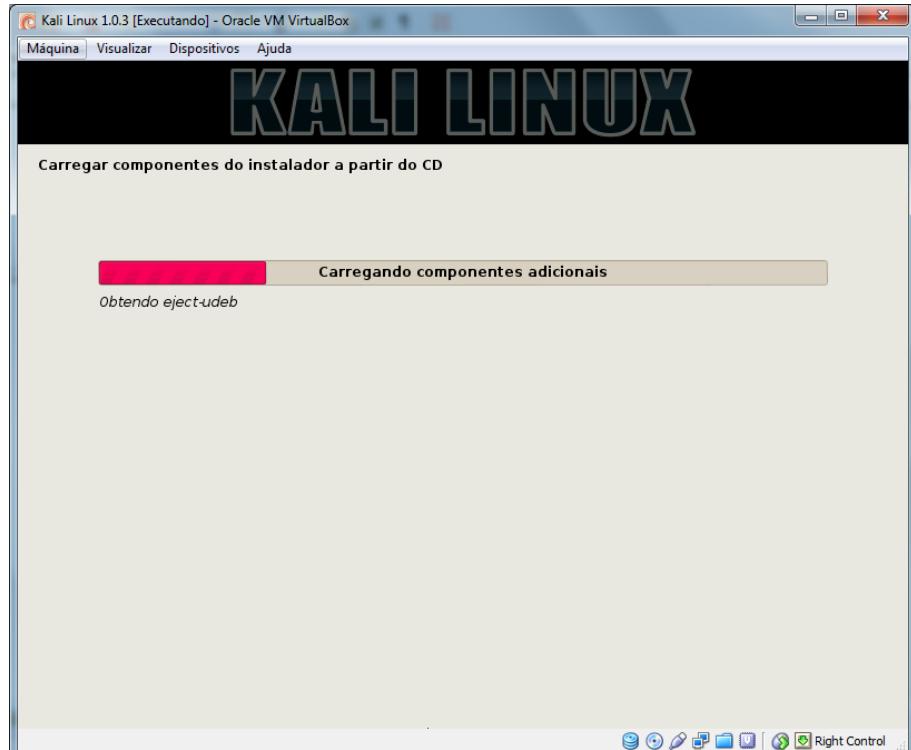


Figura 23 - Instalando Componentes

2.23 Após a instalação de todos os componentes, é necessário configurar as interfaces de rede. Se você configurou o Adaptador 1 para acessar a Internet (opção “NAT”), então selecione a interface “Eth0” e clique em “Continuar”. - (Figura 24).

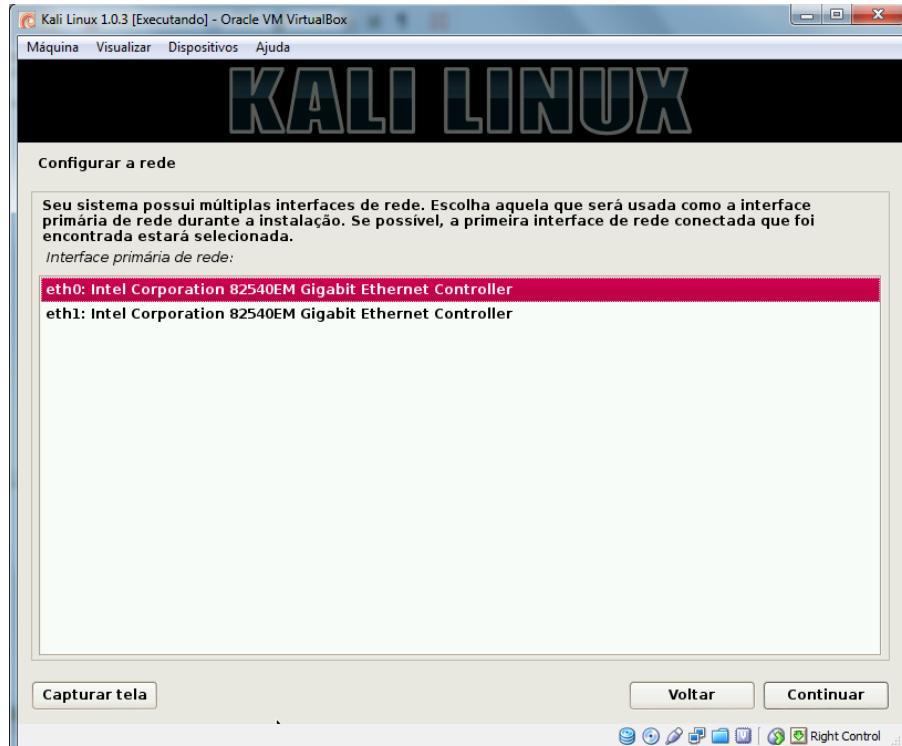


Figura 24 - Seleção da Interface de Rede Primária.

2.24 Digite o nome da máquina (*hostname*) e clique em “Continuar”. (Figura 25).

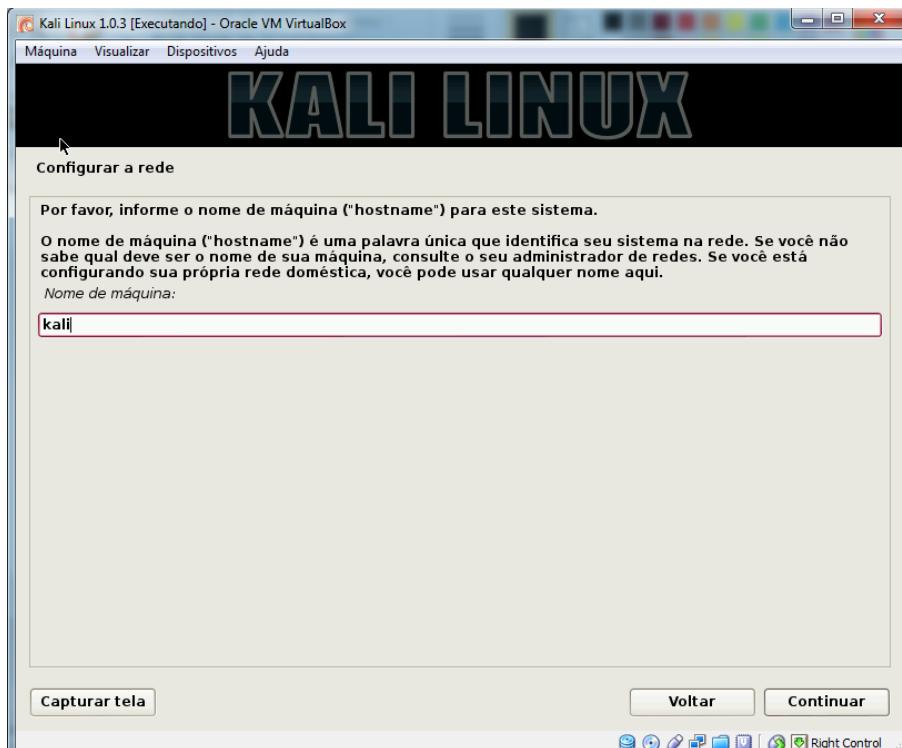


Figura 25 - Nome da Máquina - Hostname

2.25 Digite o nome do domínio e clique em “Continuar”. Ex.: “treinamento.local”. (Figura 26)

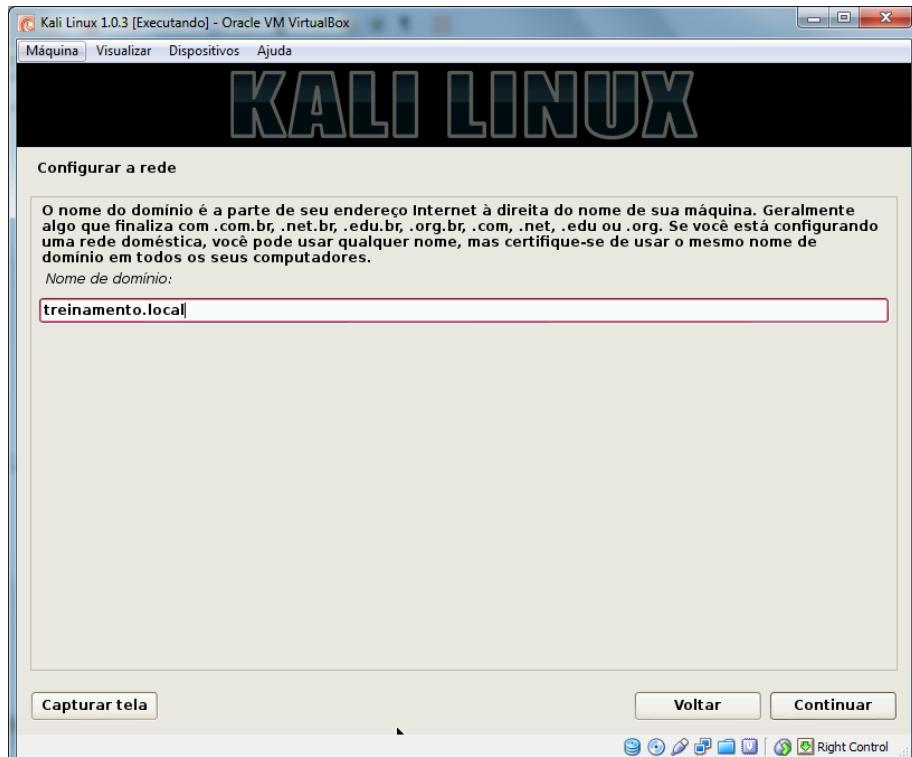


Figura 26 - Nome do Domínio

2.26 Digite a senha de root e clique em “Continuar” - (Figura 27)

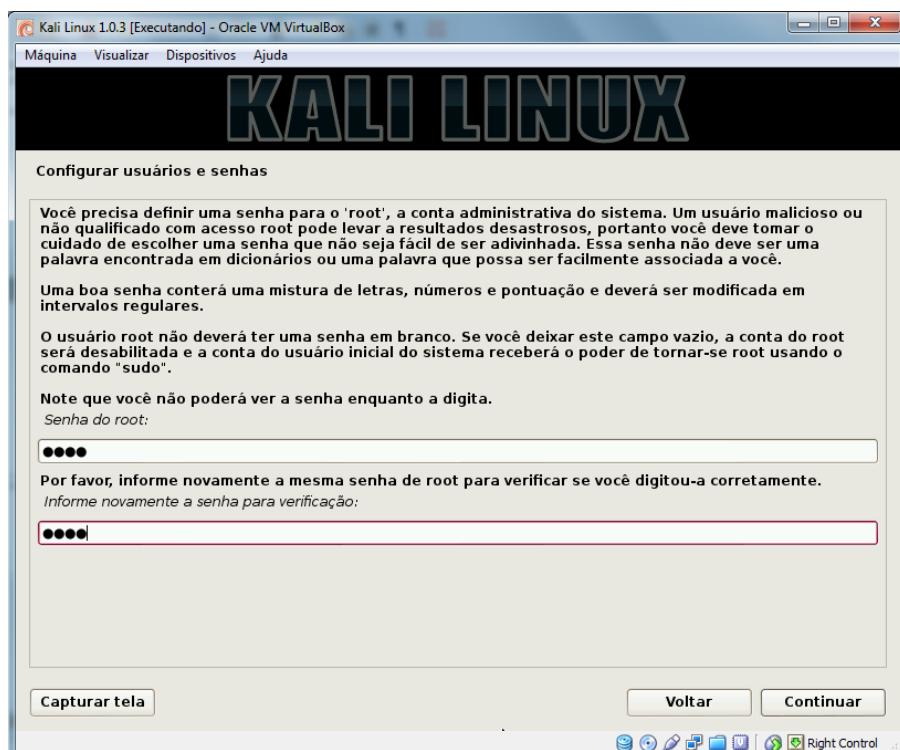


Figura 27 - Senha de root

2.27 Para configurar o seu fuso horário, selecione um estado ou província (Figura 28)

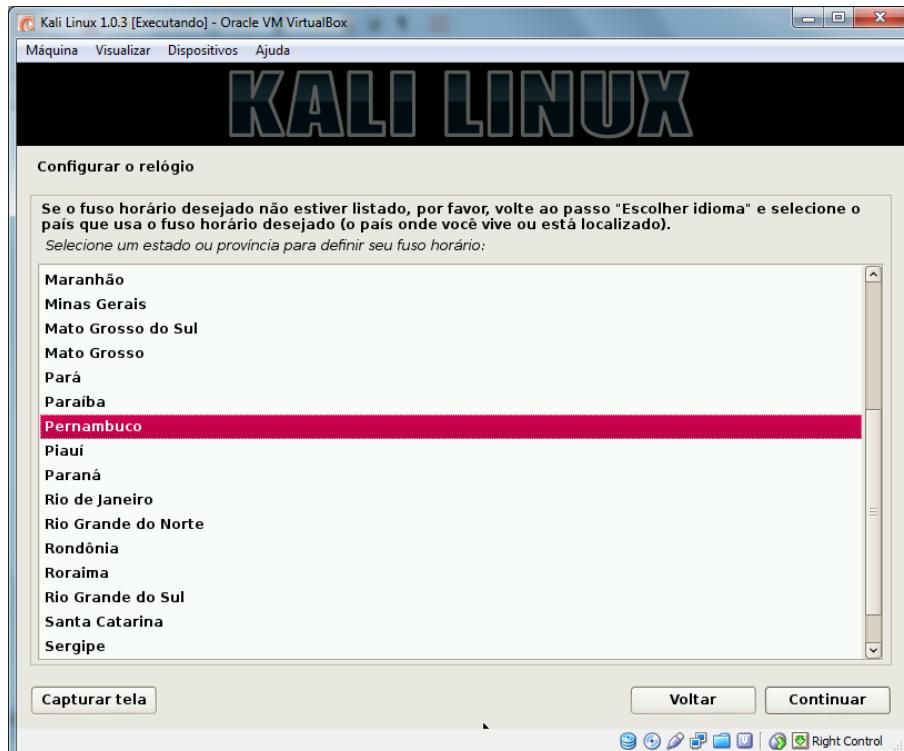


Figura 28 - Seleção de Estado ou Província

2.28 Para particionar o disco, selecione “*Assistido – usar o disco inteiro*” e clique em “*Continuar*” - Figura 29)

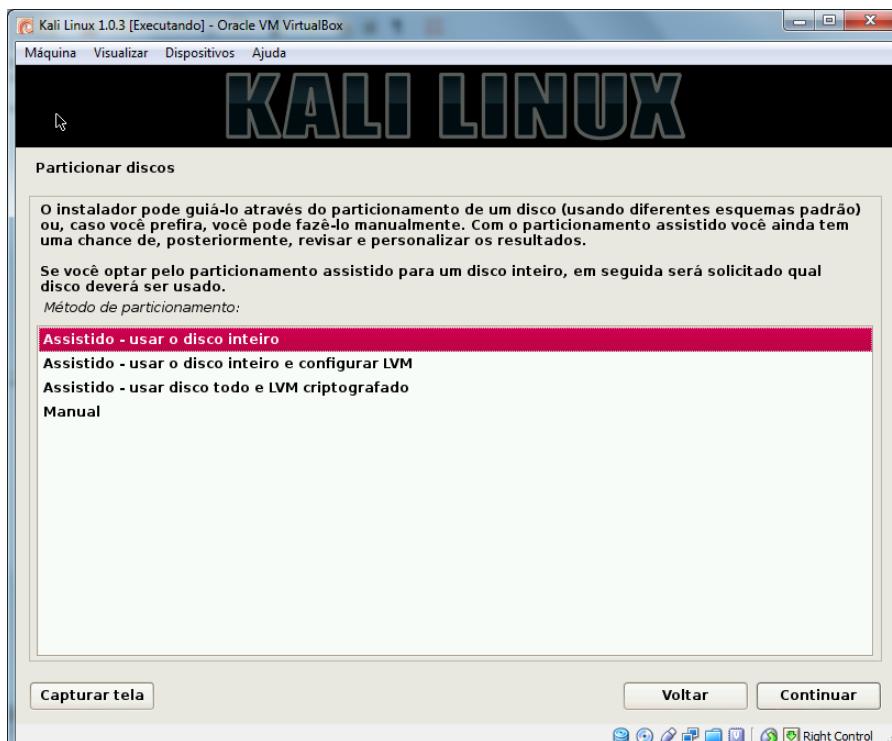


Figura 29 - Método de Particionamento

2.29 Selecione o disco que será particionado e clique em “Continuar” - (Figura 30).

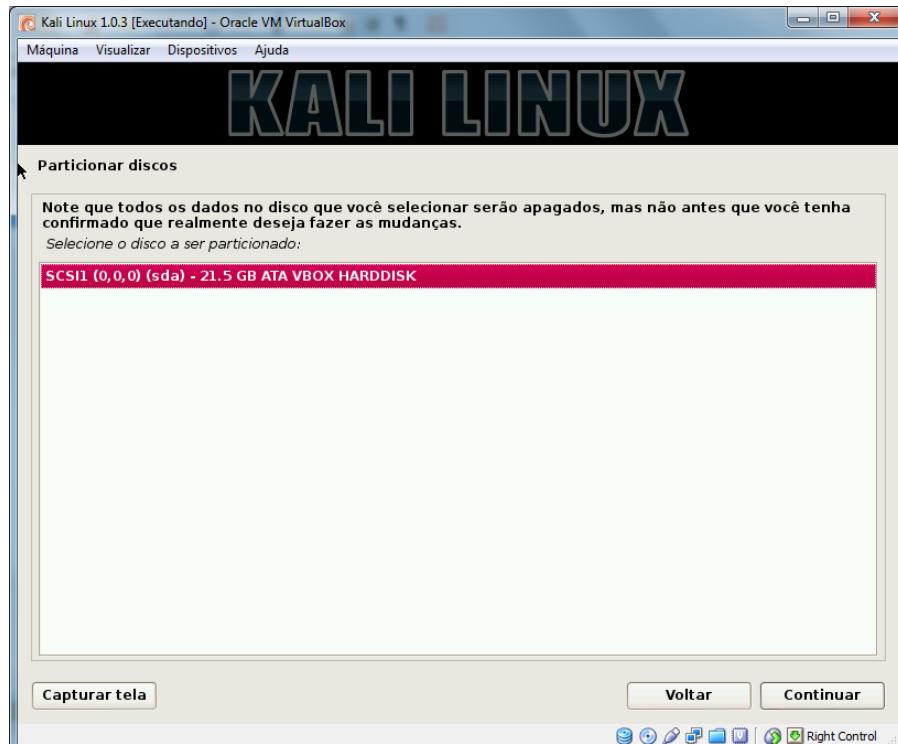


Figura 30 - Seleção do disco para particionamento

2.30 Selecione o esquema de particionamento e clique em “Continuar”. Recomendo a opção “Todos os arquivos em uma partição (para iniciantes)” (Figura 31).

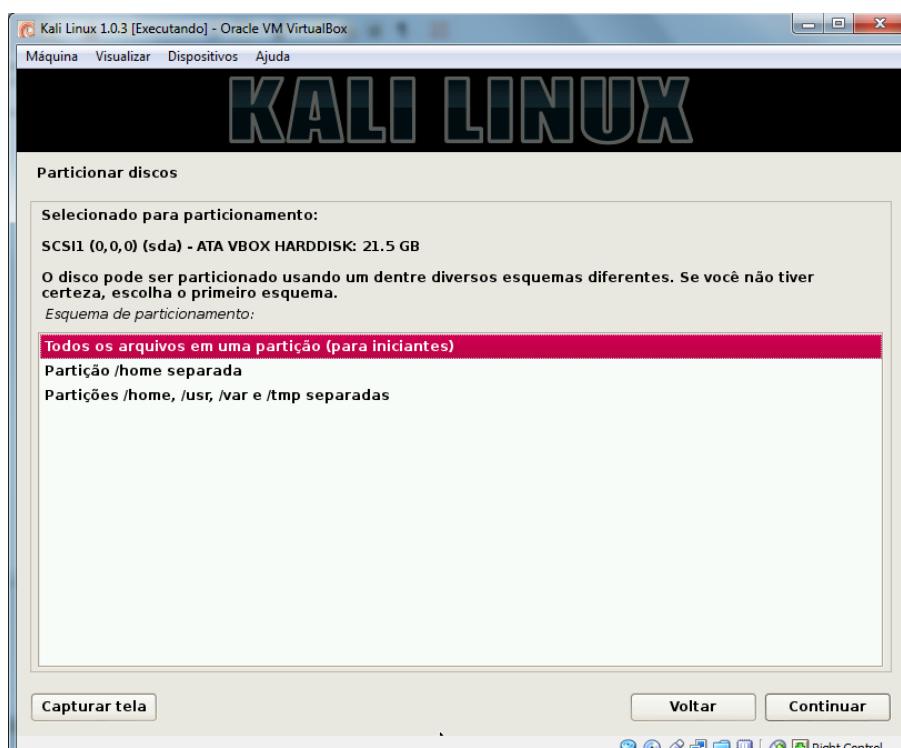


Figura 31 - Esquema de Particionamento.

2.31 Em seguida finalize o particionamento (Figura 32).

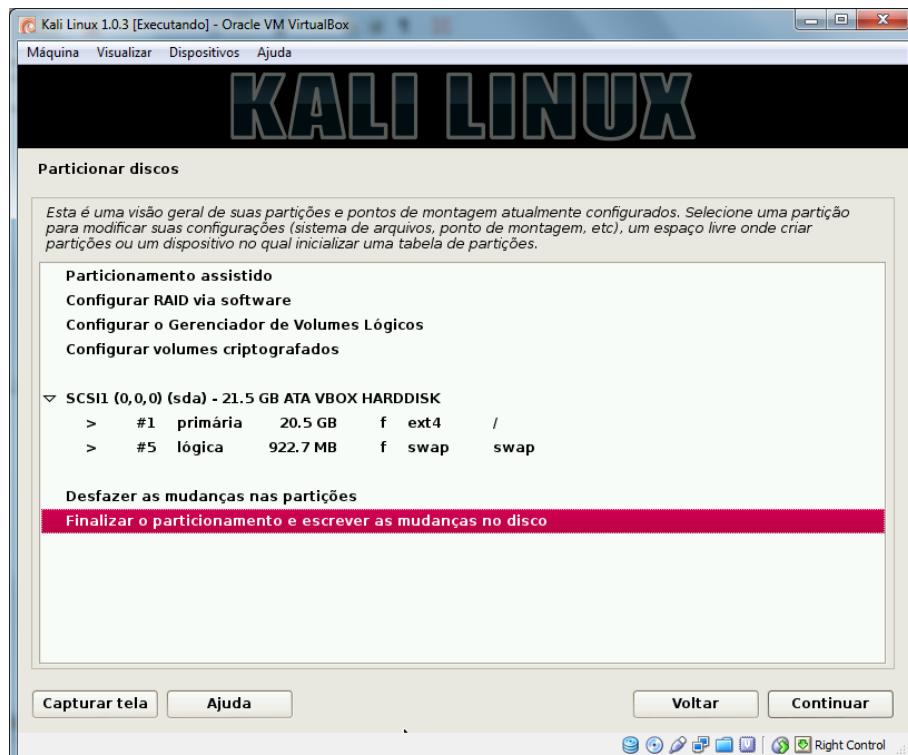


Figura 32 - Finalização de Particionamento.

2.32 Confirme o particionamento do disco (Figura 33) e clique em “Continuar”.

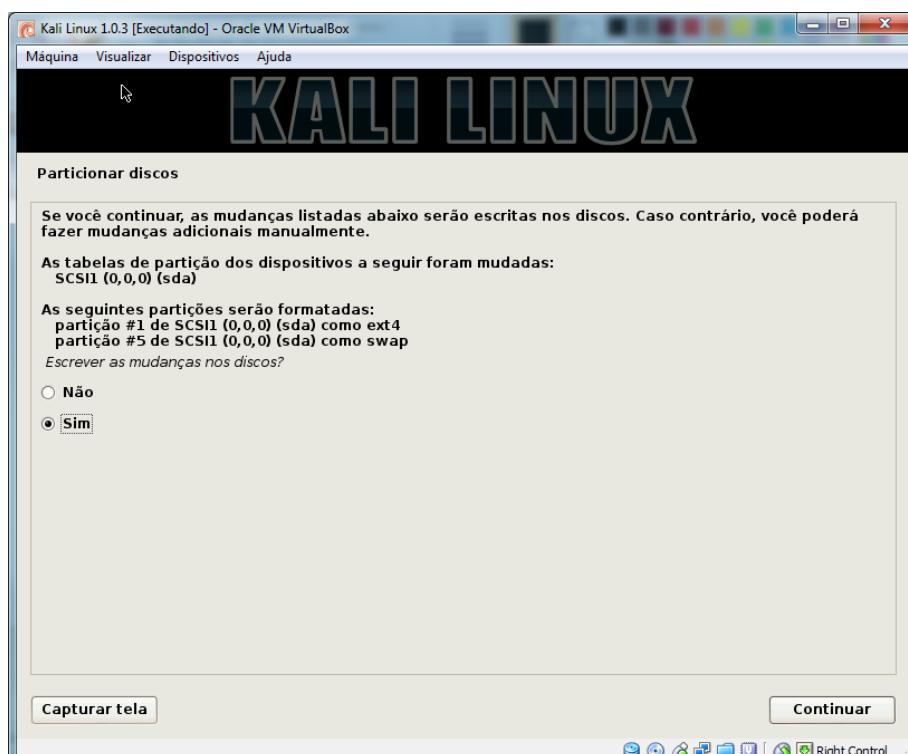


Figura 33 - Confirmação de Particionamento

2.33 Acompanhe a formatação na próxima janela - (Figura 34).

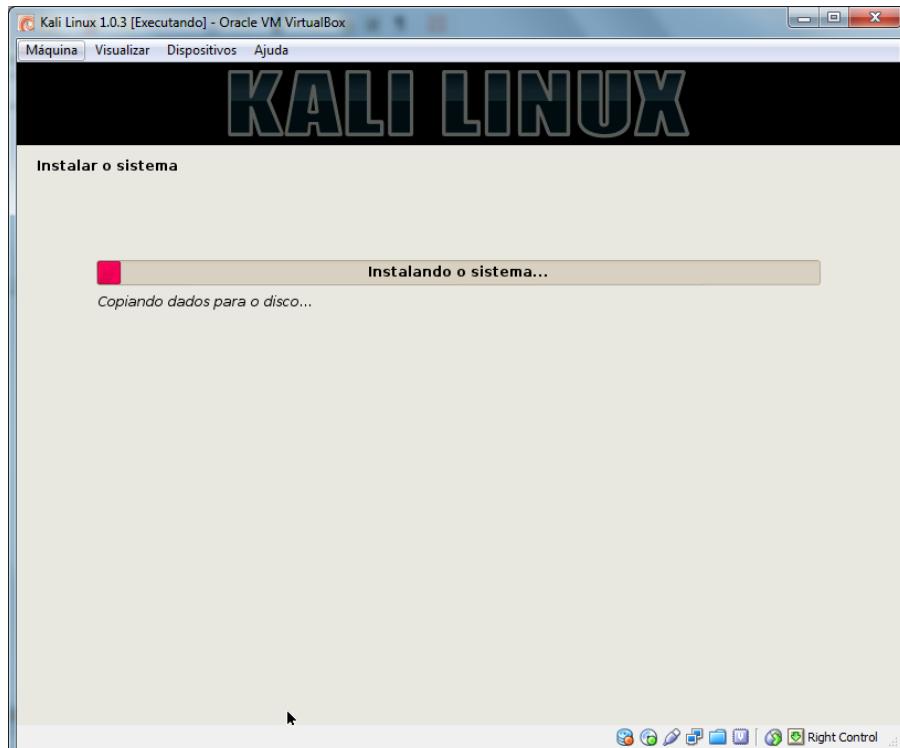


Figura 34 - Andamento da formatação.

2.34 Selecione a opção para utilizar um espelho de rede e clique em “Continuar” -(Figura 35).

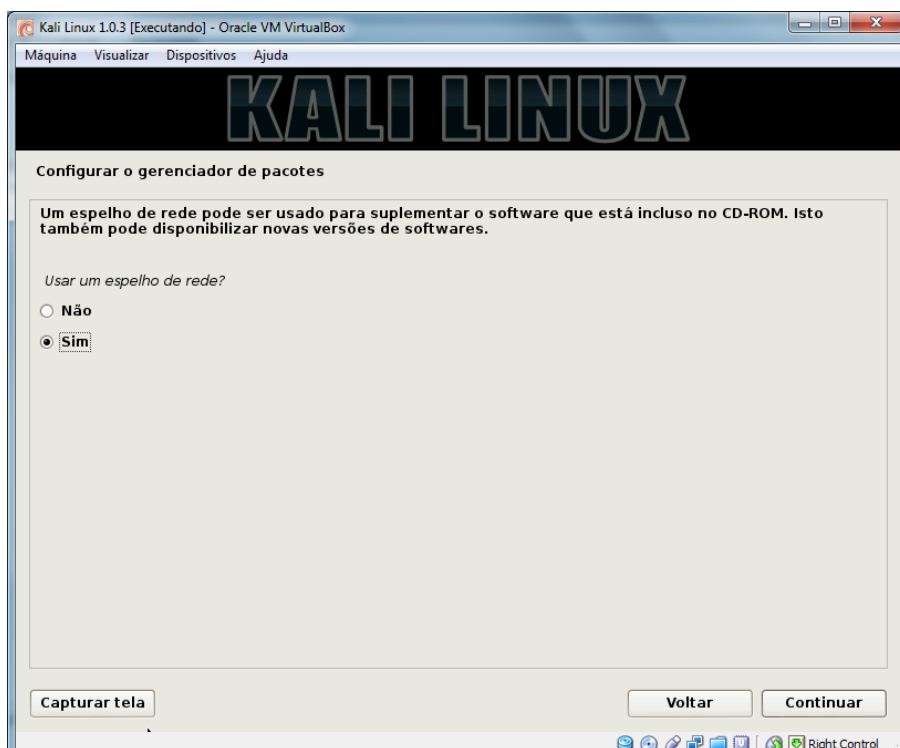


Figura 35 - Seleção de espelho de rede.

2.35 Se você utilizar um *Proxy*, digite a informação solicitada. Caso contrário, deixe em branco e clique em “Continuar” - (Figura 36).

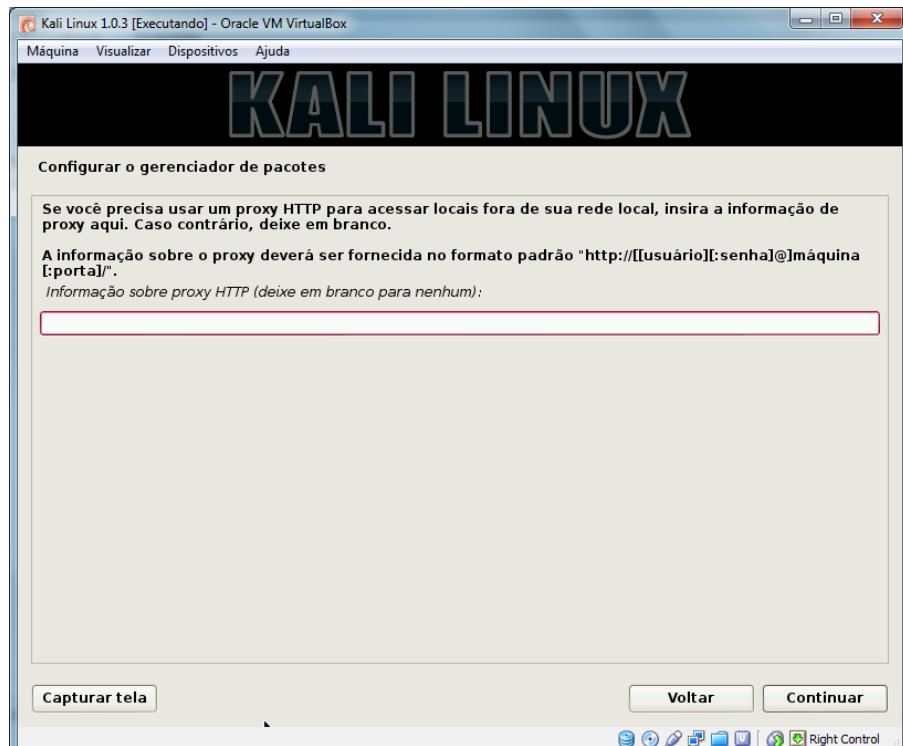


Figura 36 - Configuração do Proxy

2.36 Selecione a opção para instalar o Grub no MBR e clique em “Continuar”. - Figura 37).

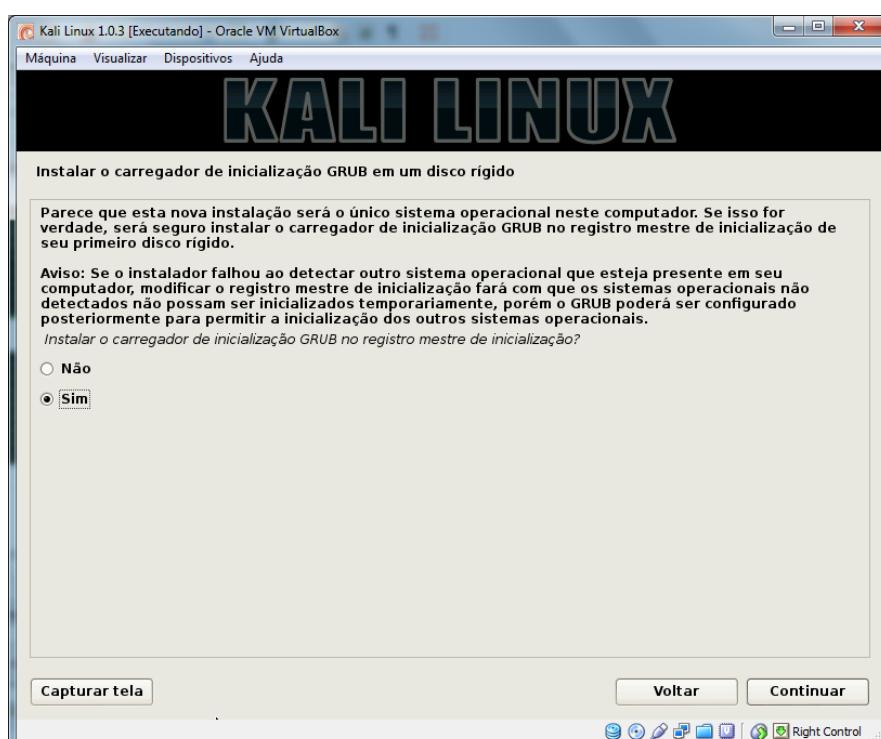


Figura 37 - Instalação do Grub

2.37 Neste momento a instalação do Kali foi concluída. Clique em “Continuar”. (Figura 38)

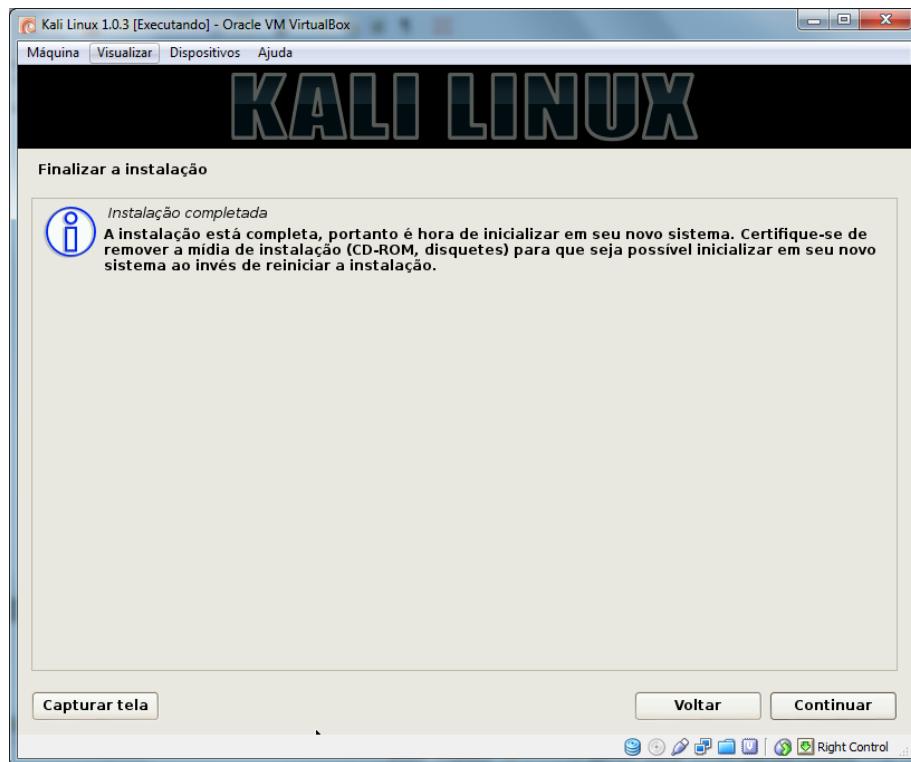


Figura 38 - Instalação do Kali concluída.

2.38 Certifique-se de remover o disco virtual, antes de executar a VM do Kali novamente. (Figura 39).

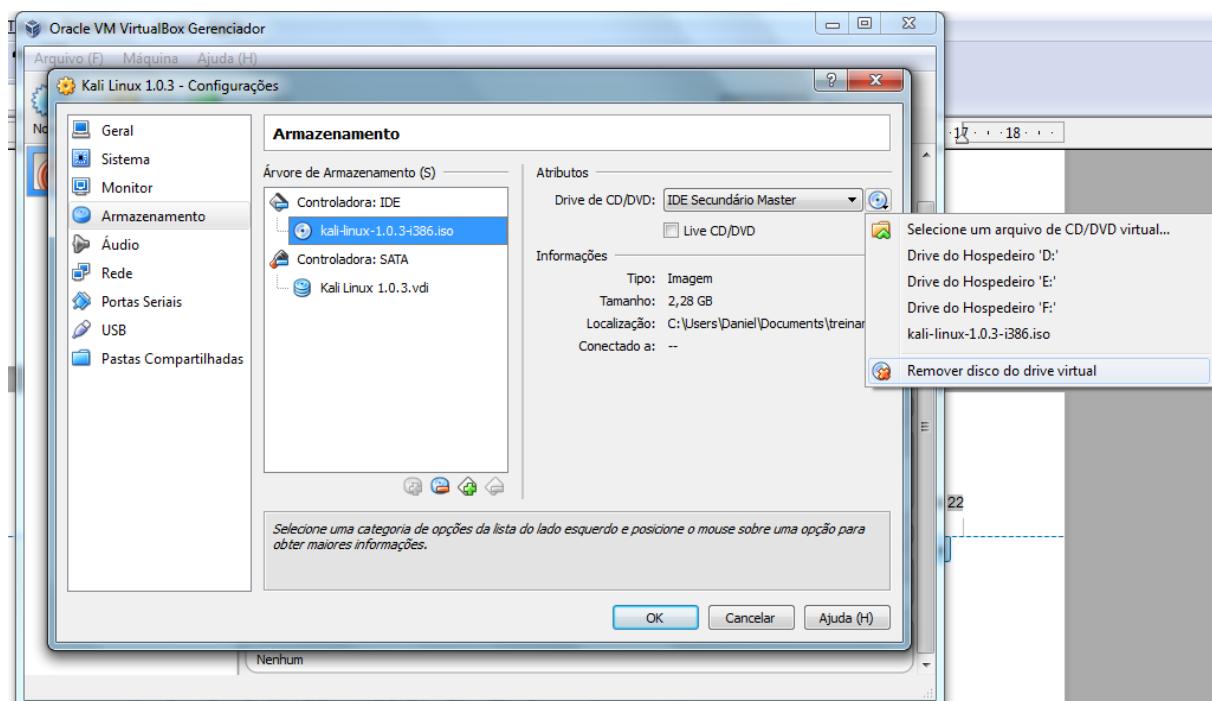


Figura 39: Remover DVD virtual.

3. Instalação de Adicionais para Convidado (Guest Additions)

Como o Virtualbox é um Hipervisor que implementa Paravirtualização, é necessário instalar módulos no Kernel da Vm, para permitir recursos como compartilhamento de pastas, recursos gráficos avançados e melhor desempenho de operações de I/O.

3.1 Após execução da VM e inicialização do Kali, será necessário realizar o login. Selecione a opção “Outro” e sem seguida forneça o usuário “root” e a senha “toor”. (Figura 40).

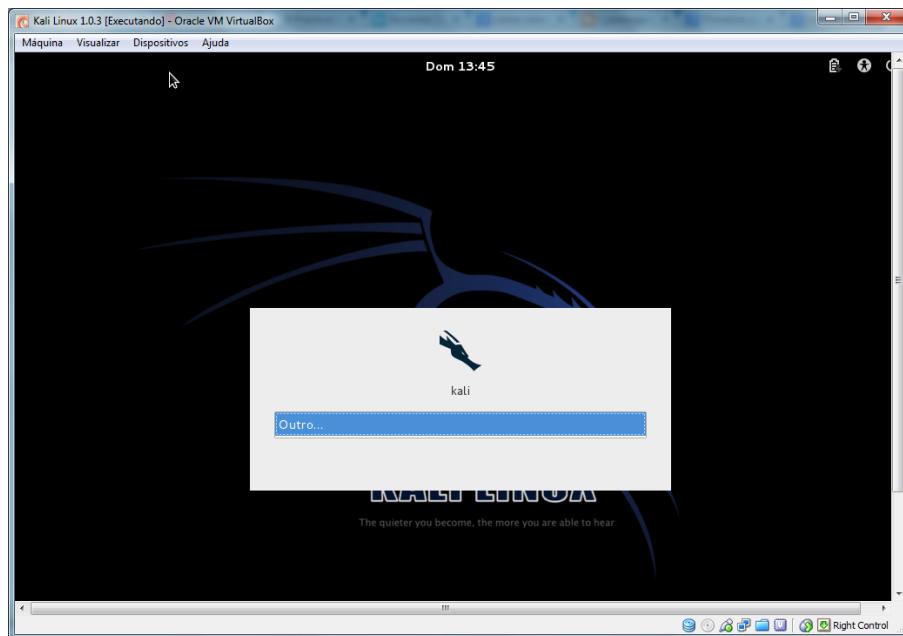


Figura 40: Tela inicial do Kali

3.2 Abra uma janela de terminal e verifique se a configuração de rede está funcionando corretamente. Para isso, execute o comando “ping www.google.com”. Se não houver resposta, adicione o servidor de nomes 8.8.8.8 (Figura 41), através do comando:

- `echo "nameserver 8.8.8.8" >> /etc/resolv.conf`

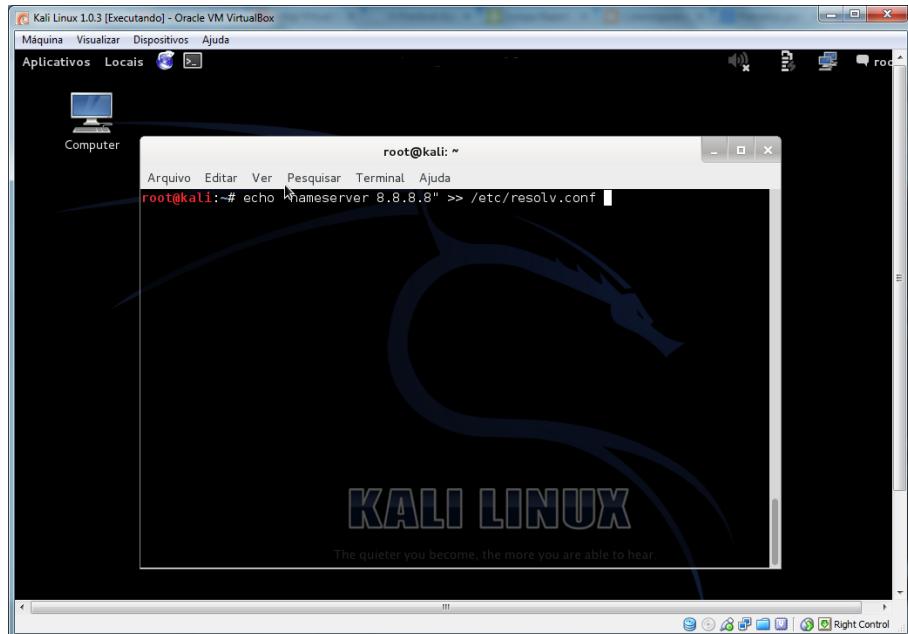


Figura 41: Adicionando servidor de nomes

Em seguida teste novamente a resolução de nomes para garantir que está funcionando.

3.3 Na janela de terminal execute o seguinte comando (Figura 42):

- *apt-get update && apt-get install -y linux-headers-\$(uname -r)*

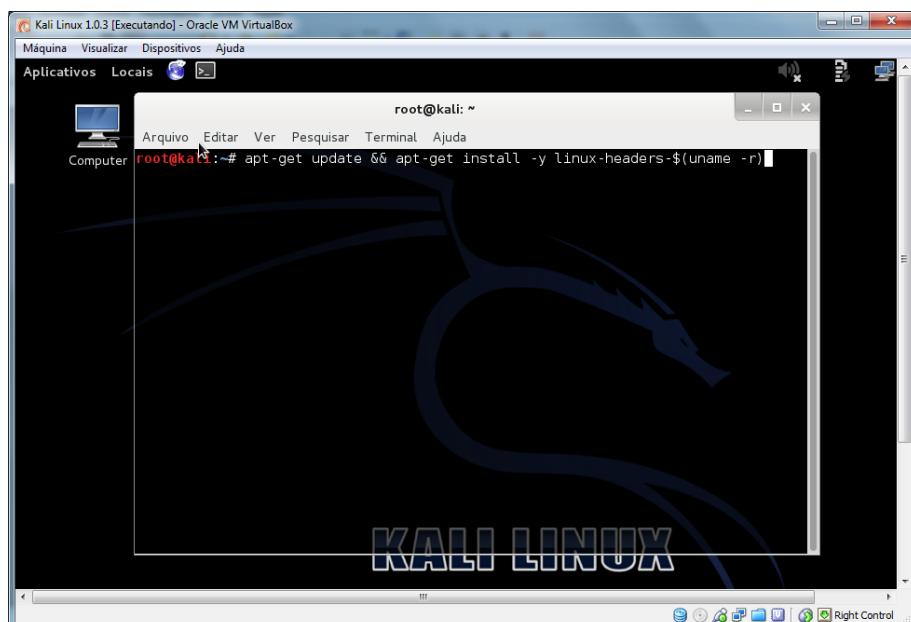


Figura 42: Instalação dos headers do Kernel via terminal

3.4 A partir do Menu “Dispositivos” do Virtualbox, selecione a opção “Instalar Adicionais para Convidado” - (Figura 43).

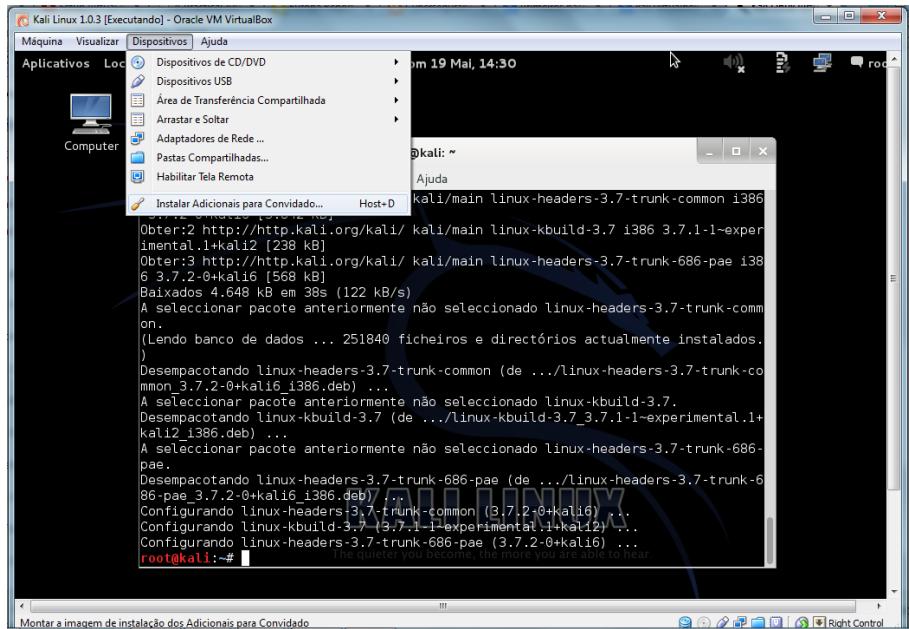


Figura 43 - Instalação de Adicionais Para Convidados

3.4 Ao surgir a janela solicitando a execução automática se um software, clique em “**CANCELAR**” - (Figura 44)

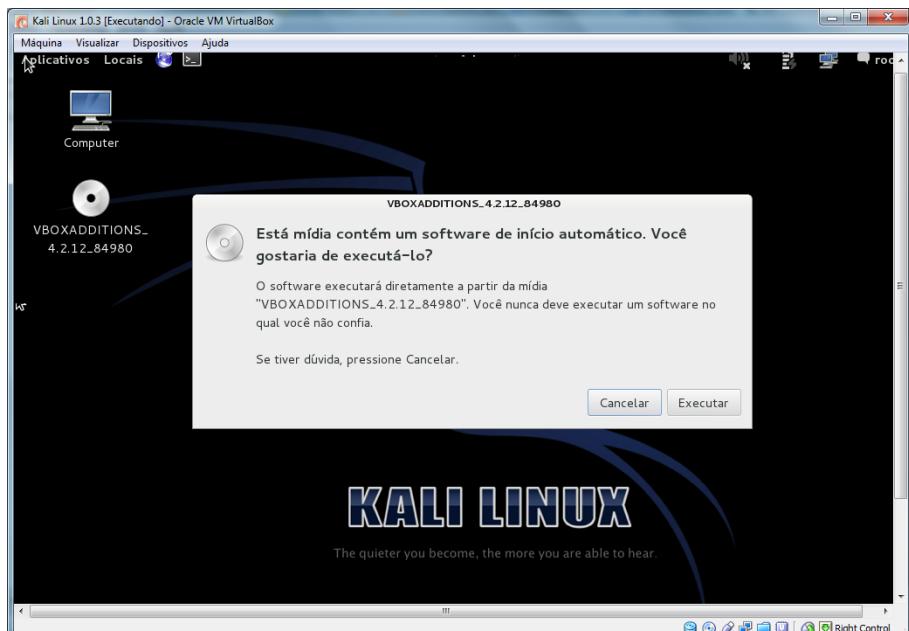


Figura 44 - Janela de execução automática – Clique em Cancelar

3.5 A partir da janela de terminal, execute os seguintes comandos:

```
cp /media/cd-rom/VBoxLinuxAdditions.run /root/
chmod 755 /root/VBoxLinuxAdditions.run
cd /root
./VBoxLinuxAdditions.run
```

Como pode ser visualizado na Figura 45.

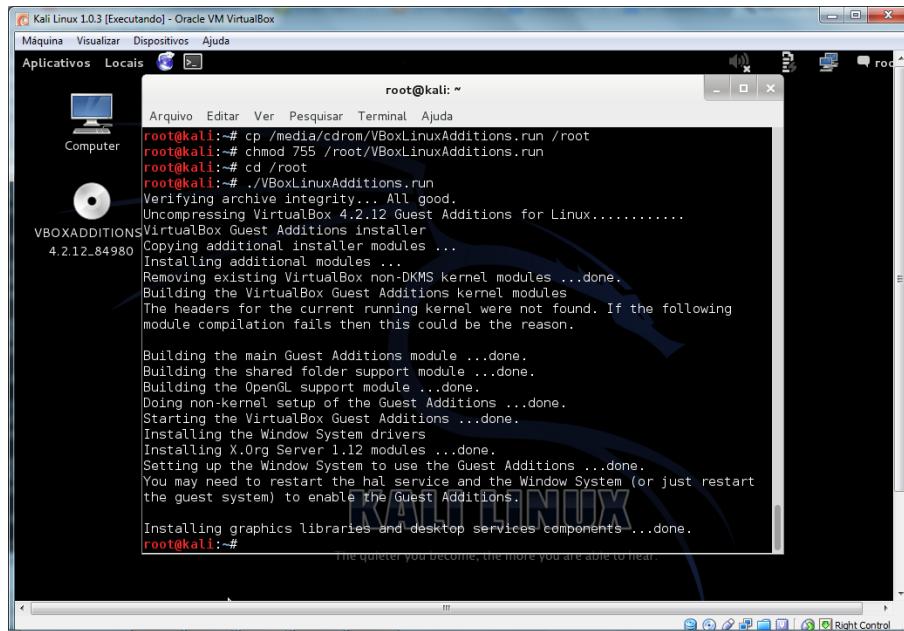


Figura 45 - Execução do Script de instalação dos Adicionais

Em seguida, reinicie o Kali para que a instalação surta efeito.

Se você estiver usando um sistema Hospedeiro da família Windows, pode ser necessário reiniciar o Hospedeiro antes de usar o Kali.