

Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Introdução ao Kali Linux

Introdução

O Kali Linux é uma distribuição Linux **gratuita e código fonte aberto** baseada no Debian destinada a *testes de penetração e auditoria de segurança*. Kali contém centenas de ferramentas que são voltadas para várias tarefas de segurança da informação, como Teste de Penetração, Pesquisa de Segurança, Computação Forense e Engenharia Reversa.

O Kali Linux é desenvolvido, financiado e mantido pela *Offensive Security*, uma empresa líder em treinamento de segurança da informação. Eles oferecem cursos e certificados.

Introdução

Características

Desenvolvido para ser usado num cenário que envolve um único usuário logado como *root*.

Download

site: <https://www.kali.org/downloads/>. É possível baixar a ISO (32 e 64 bits), máquinas virtuais (VMWare e VBox) ou na arquitetura ARM (Raspberry Pi).

Instalação

Pré-requisitos para instalação

- No mínimo 8 GB de espaço em disco para a instalação.
- No mínimo 512MB de RAM para as arquiteturas i386 e amd64.
- Suporte a boot pelo drive de CD-DVD / USB

Criando a Máquina Virtual - Definição de SO

Nome e Sistema Operacional

Escolha um nome descritivo para a nova máquina virtual e selecione o tipo de sistema operacional que você pretende instalar nela. O nome que você escolher será utilizado pelo VirtualBox para identificar esta máquina.

Nome:

Tipo: 

Versão:

Criando a Máquina Virtual - Tamanho da Memória



Criando a Máquina Virtual - Disco



Criando a Máquina Virtual - Tipo de Disco



Criando a Máquina Virtual - Tipo de Disco

Criar Disco Rígido Virtual



Armazenamento em disco rígido físico

Escolha se o arquivo contendo o disco rígido virtual deve crescer à medida em que é utilizado (dinamicamente alocado) ou se ele deve ser criado já com o tamanho máximo (tamanho fixo).

Um arquivo de disco rígido virtual **dinamicamente alocado** irá utilizar espaço em seu disco rígido físico à medida em que for sendo utilizado (até um **tamanho máximo pré-definido**), mas não irá encolher caso seja liberado espaço nele.

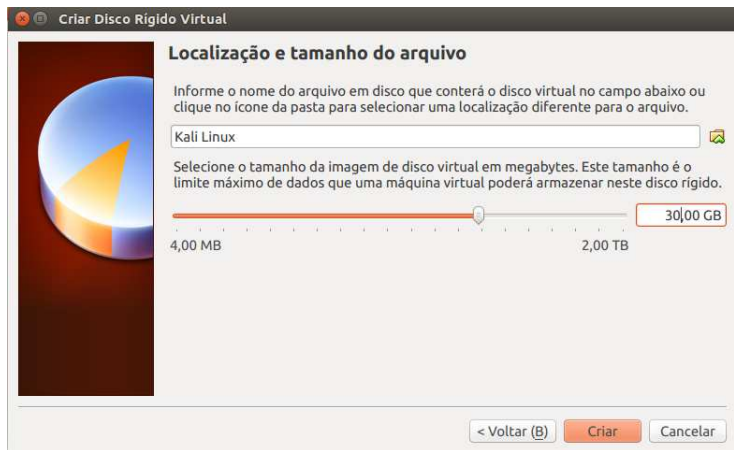
Um arquivo de disco rígido virtual de **tamanho fixo** pode levar mais tempo para ser criado em alguns sistemas, mas geralmente possui acesso mais rápido.

Dinamicamente alocado

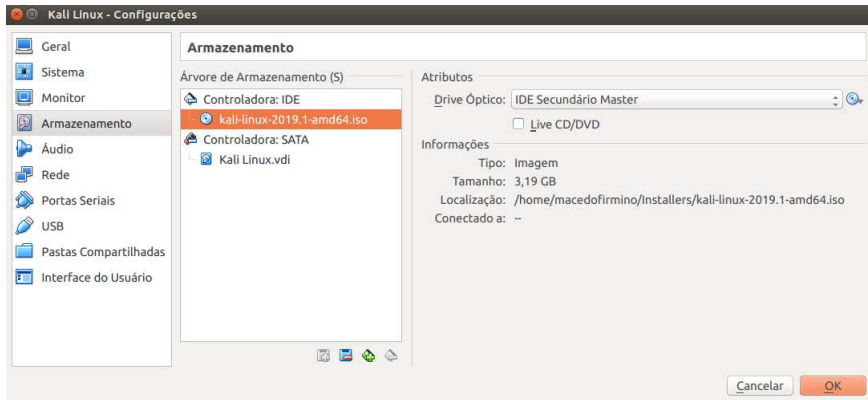
Tamanho Fixo

< Voltar (B) Próximo (N) > Cancelar

Criando a Máquina Virtual - Tamanho do Disco



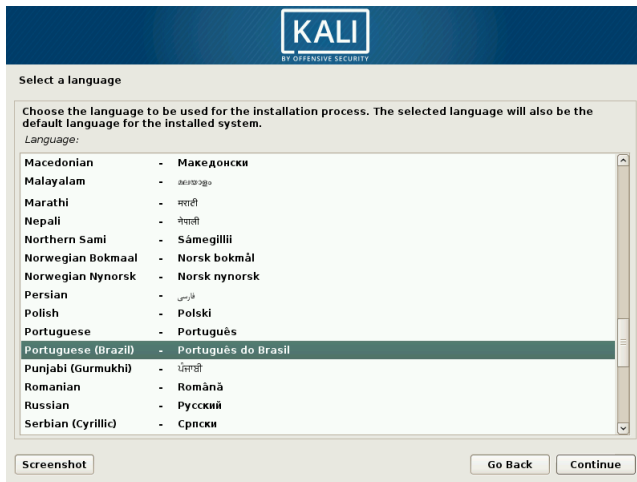
Inserindo a Imagem de Instalação



Instalação do SO com a Interface Gráfica



Selecionando o Idioma



Selecionando a Localização



Selecionar sua localidade

A localidade selecionada será usada para configurar seu fuso horário e também para, por exemplo, selecionar o "locale" do sistema. Normalmente este deveria ser o país onde você vive.

Esta é uma pequena lista de localidades baseada no idioma selecionado. Escolha "outro" se sua localidade não está listada.


Pais, território ou área:

- Brasil
- Portugal
- outro

Selecionando o Teclado



Nome da Máquina



Configurar a rede

Por favor, informe o nome de máquina ("hostname") para este sistema.

O nome de máquina ("hostname") é uma palavra única que identifica seu sistema na rede. Se você não sabe qual deve ser o nome de sua máquina, consulte o seu administrador de redes. Se você está configurando sua própria rede doméstica, você pode usar qualquer nome aqui.

Nome de máquina:

Nome do Domínio (Deixar em branco)



Configurar a rede

O nome do domínio é a parte de seu endereço Internet à direita do nome de sua máquina. Geralmente algo que finaliza com .com.br, .net.br, .edu.br, .org.br, .com, .net, .edu ou .org. Se você está configurando uma rede doméstica, você pode usar qualquer nome, mas certifique-se de usar o mesmo nome de domínio em todos os seus computadores.

Nome de domínio:

Inserindo a Senha



Configurar usuários e senhas

Você precisa definir uma senha para o 'root', a conta administrativa do sistema. Um usuário malicioso ou não qualificado com acesso root pode levar a resultados desastrosos, portanto você deve tomar o cuidado de escolher uma senha que não seja fácil de ser adivinhada. Essa senha não deve ser uma palavra encontrada em dicionários ou uma palavra que possa ser facilmente associada a você.

Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.

O usuário root não deverá ter uma senha em branco. Se você deixar este campo vazio, a conta do root será desabilitada e a conta do usuário inicial do sistema receberá o poder de tornar-se root usando o comando "sudo".

Note que você não poderá ver a senha enquanto a digita.

Senha do root:

 Mostrar a senha

Por favor, informe novamente a mesma senha de root para verificar se você digitou-a corretamente.

Informe novamente a senha para verificação:

 Mostrar a senha

Selecionando o Fuso Horário



KALI
BY OFFENSIVE SECURITY

Configurar o relógio

Se o fuso horário desejado não estiver listado, por favor, volte ao passo "Escolher idioma" e selecione o país que usa o fuso horário desejado (o país onde você vive ou está localizado).

Selecione um estado ou província para definir seu fuso horário:

- Mato Grosso
- Pará
- Paraíba
- Pernambuco
- Piauí
- Paraná
- Rio de Janeiro
- Rio Grande do Norte**
- Rondônia
- Roraima
- Rio Grande do Sul
- Santa Catarina
- Sergipe
- São Paulo
- Tocantins

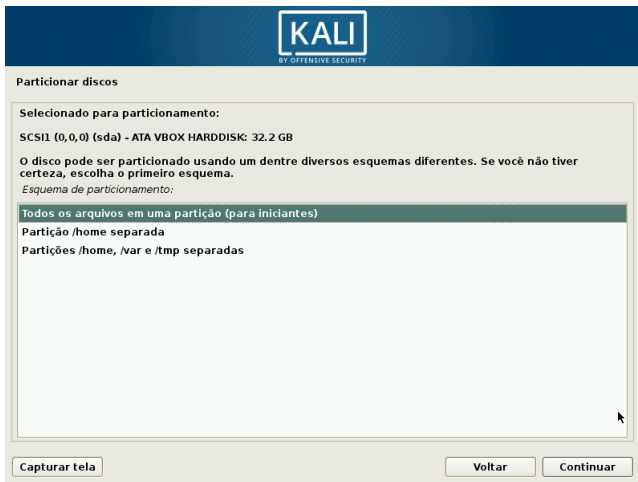
Gerenciando o Disco



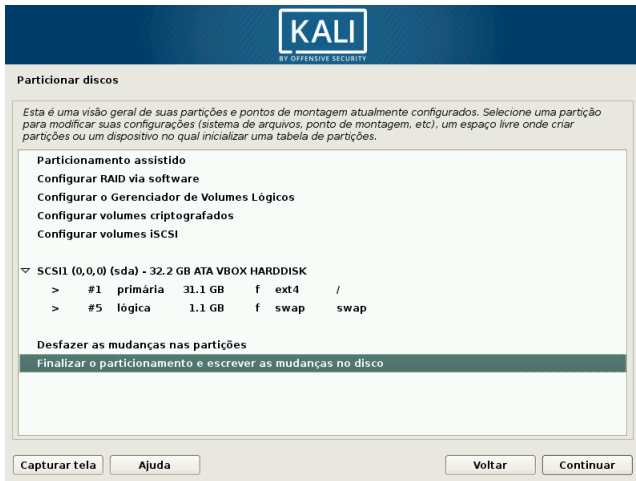
Selecionando o Disco



Gerenciando o Disco



Gerenciando o Disco



KALI
BY OFFENSIVE SECURITY

Particionar discos

Esta é uma visão geral de suas partições e pontos de montagem atualmente configurados. Selecione uma partição para modificar suas configurações (sistema de arquivos, ponto de montagem, etc), um espaço livre onde criar partições ou um dispositivo no qual inicializar uma tabela de partições.

- Particionamento assistido
 - Configurar RAID via software
 - Configurar o Gerenciador de Volumes Lógicos
 - Configurar volumes criptografados
 - Configurar volumes iSCSI
- ▼ SCSII (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
 - > #1 primária 31.1 GB f ext4 /
 - > #5 lógica 1.1 GB f swap swap

Desfazer as mudanças nas partições

Finalizar o particionamento e escrever as mudanças no disco

Capturar tela Ajuda Voltar Continuar


Gerenciando o Disco



Início da Instalação



Configuração de Pacotes



Configurar o gerenciador de pacotes

Um espelho de rede pode ser usado para suplementar o software que está incluído no CD-ROM. Isto também pode disponibilizar novas versões de softwares.

Usar um espelho de rede?

Não

Sim

Capturar tela

Voltar Continuar

Configuração de Pacotes com Proxy



Configurar o gerenciador de pacotes

Se você precisa usar um proxy HTTP para acessar locais fora de sua rede local, insira a informação de proxy aqui. Caso contrário, deixe em branco.

A informação sobre o proxy deverá ser fornecida no formato padrão "http://[[usuário]:[senha]@[máquina]:porta]".
Informação sobre proxy HTTP (deixe em branco para nenhum):

Instalação do Grub



Instalar o carregador de inicialização GRUB em um disco rígido

Parece que esta nova instalação será o único sistema operacional neste computador. Se isso for verdade, será seguro instalar o carregador de inicialização GRUB no registro mestre de inicialização de seu primeiro disco rígido.


Aviso: Se o instalador falhou ao detectar outro sistema operacional que esteja presente em seu computador, modificar o registro mestre de inicialização fará com que os sistemas operacionais não detectados não possam ser inicializados temporariamente, porém o GRUB poderá ser configurado posteriormente para permitir a inicialização dos outros sistemas operacionais.

Instalar o carregador de inicialização GRUB no registro mestre de inicialização?

Não

Sim

Instalação do Grub



Instalar o carregador de inicialização GRUB em um disco rígido

Você precisa fazer com que seu novo sistema recém-instalado seja inicializável, instalando o carregador de inicialização GRUB em um dispositivo inicializável. A maneira usual de fazer isso é instalar o GRUB no registro mestre de inicialização de seu primeiro disco rígido. Se preferir, você pode instalar o GRUB em outro local de seu disco rígido, em outro disco ou até mesmo em um disquete.

Dispositivo no qual instalar o carregador de inicialização:

Informar manualmente o dispositivo

```
/dev/sda (ata-VBOX_HARDDISK__VBD92246e-a-88b0c7a9)
```

Capturar tela

Voltar

Continuar

Instalação Finalizada



Interface Gráfica do Kali 2019.1



Ferramentas de Coleta de Informações

- Nmap;
- p0f;
- Wireshark;
- Arp-scan;
- dnswalk;
- DotDotPwn;
- enum4linux;
- enumIAX;
- EyeWitness;
- Faraday;
- Fierce;
- Firewalk.
- etc.

Análise de Vulnerabilidade

- sfuzz;
- SidGuesser;
- SIPArmyKnife;
- sqlmap;
- SqlNinja;
- sqlsus;
- THC-IPV6;
- tnscommand10g;
- unix-privesc-check;
- etc.

Ataques sem Fio

- Airbase-ng
- Aircrack-ng
- Airdecap-ng and Airdecloak-ng
- Aireplay-ng
- airgraph-ng
- Airmon-ng
- Airodump-ng
- Airolib-ng
- etc.

Aplicativos Web

- Uniscan;
- w3af;
- WebScarab;
- Webshag;
- WebSlayer;
- WebSploit;
- WhatWeb;
- WPScan;
- etc.

Ferramentas de Exploração de Vulnerabilidade

- Armitage;
- Backdoor Factory;
- BeEF;
- Commix;
- crackle;
- exploitdb;
- jboss-autopwn;
- Linux Exploit Suggester;
- Maltego Teeth;
- Metasploit Framework;
- etc.

Ferramentas Forenses

- Foremost;
- Galleta;
- Guymager;
- iPhone Backup Analyzer;
- p0f;
- pdfid;
- pdgmail;
- peepdf;
- RegRipper;
- etc.

Sniffing e Spoofing

- WebScarab;
- Wifi Honey;
- Wireshark;
- xspy;
- Yersinia;
- zaproxy;
- protos-sip;
- rebind;
- responder;
- etc.

Ataques por Senha

- THC-Hydra;
- John the Ripper;
- keimpx;
- Maltego Teeth;
- Maskprocessor;
- multiforcer;
- Ncrack;
- RainbowCrack;
- rcracki-mt;
- RSMangler;
- SecLists;
- etc.