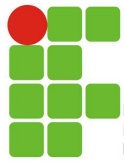
Segurança de Redes

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

Introdução ao Kali Linux



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

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.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

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).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Criando a Máquina Virtual - Definição de SO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criando a Máquina Virtual - Tamanho da Memória

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criando a Máquina Virtual - Disco

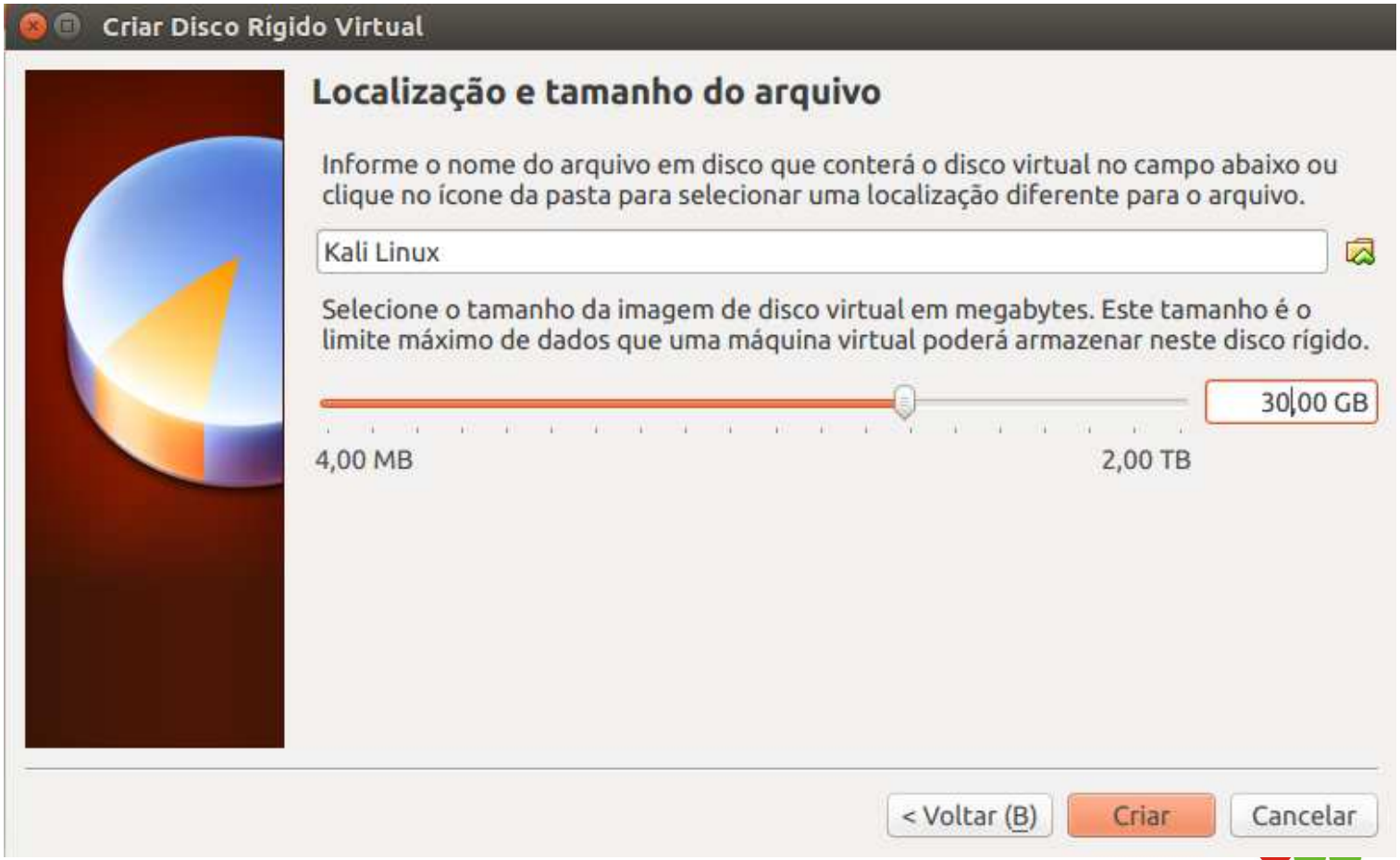
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criando a Máquina Virtual - Tipo de Disco

Criando a Máquina Virtual - Tipo de Disco

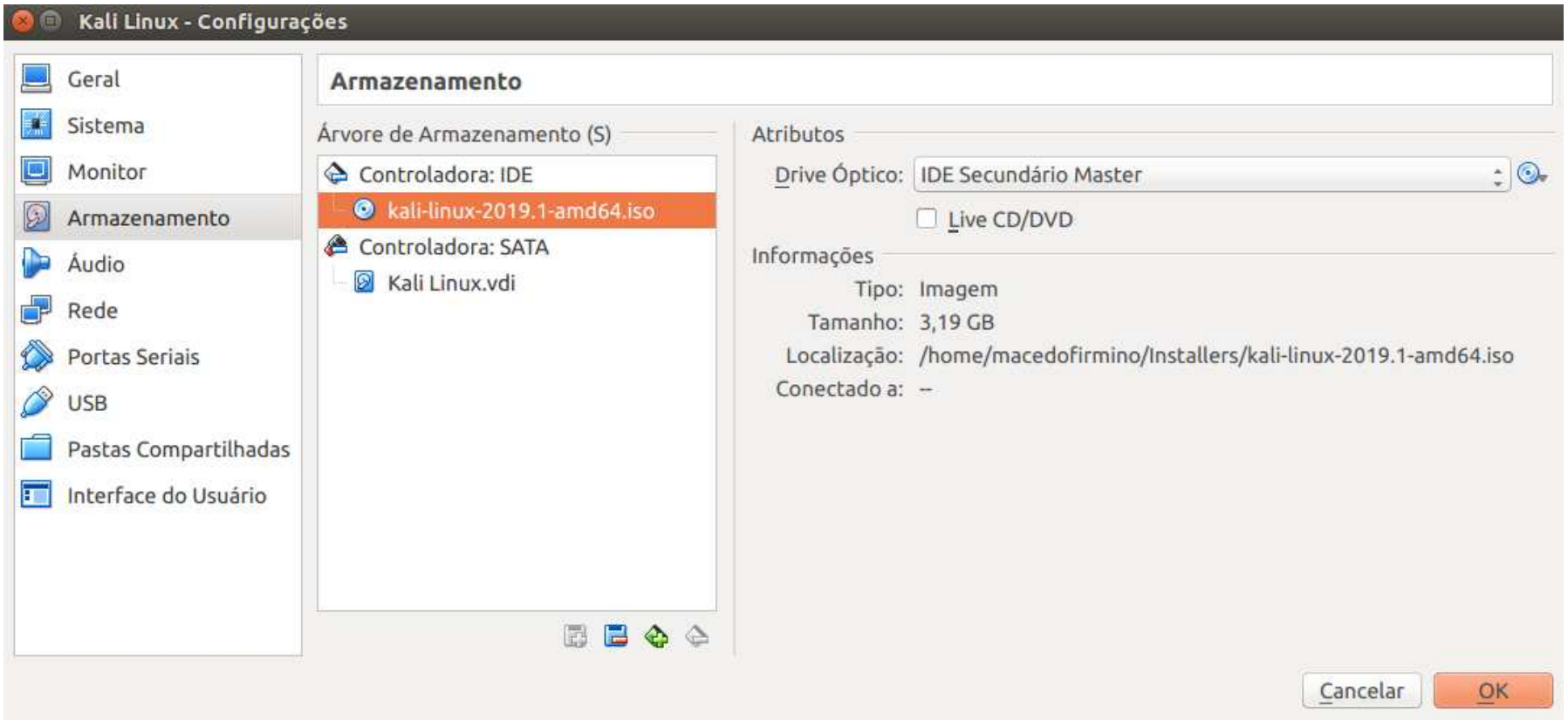
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criando a Máquina Virtual - Tamanho do Disco



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Inserindo a Imagem de Instalação

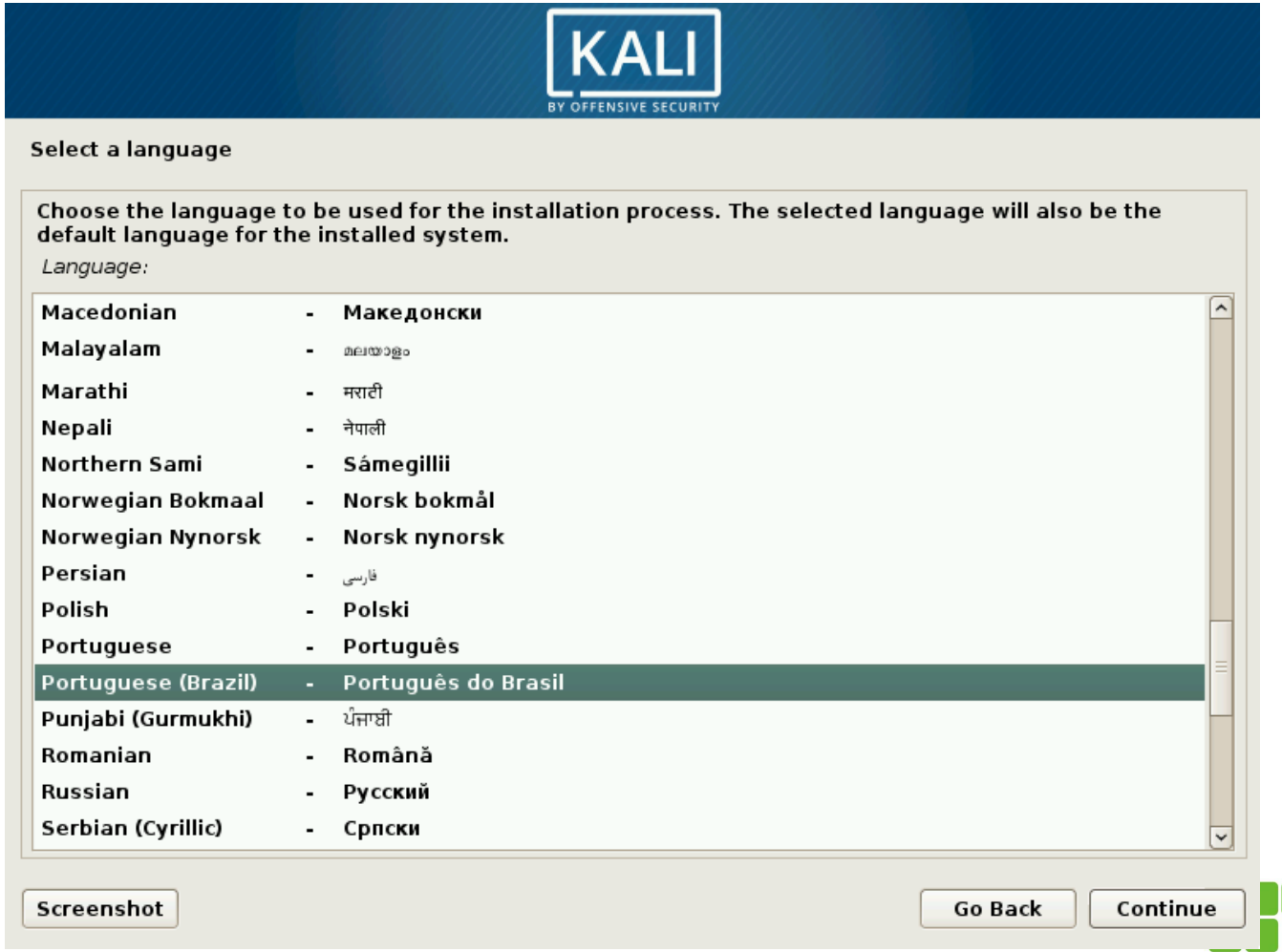


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Instalação do SO com a Interface Gráfica

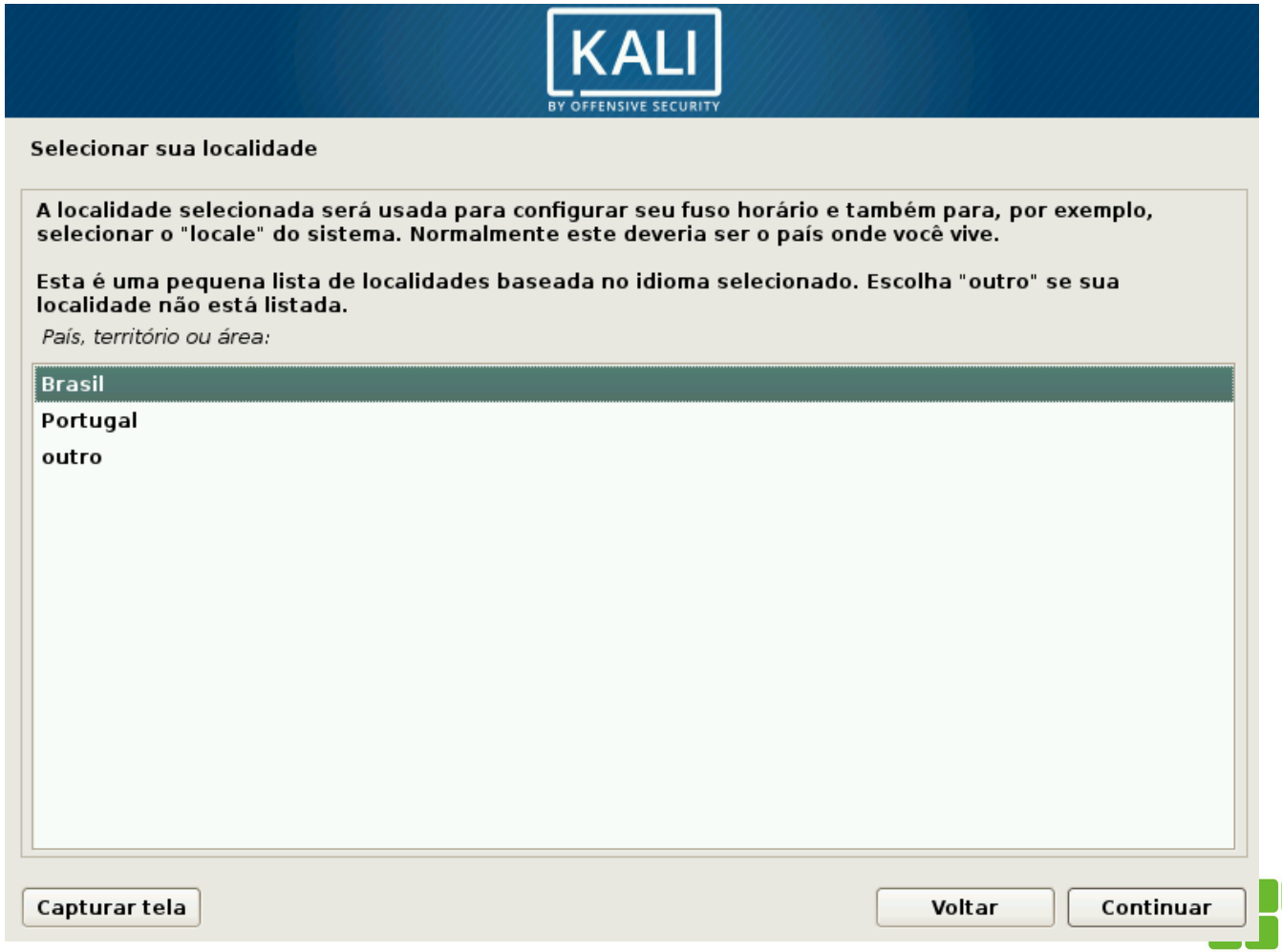
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Selecionando o Idioma



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Selecionando a Localização

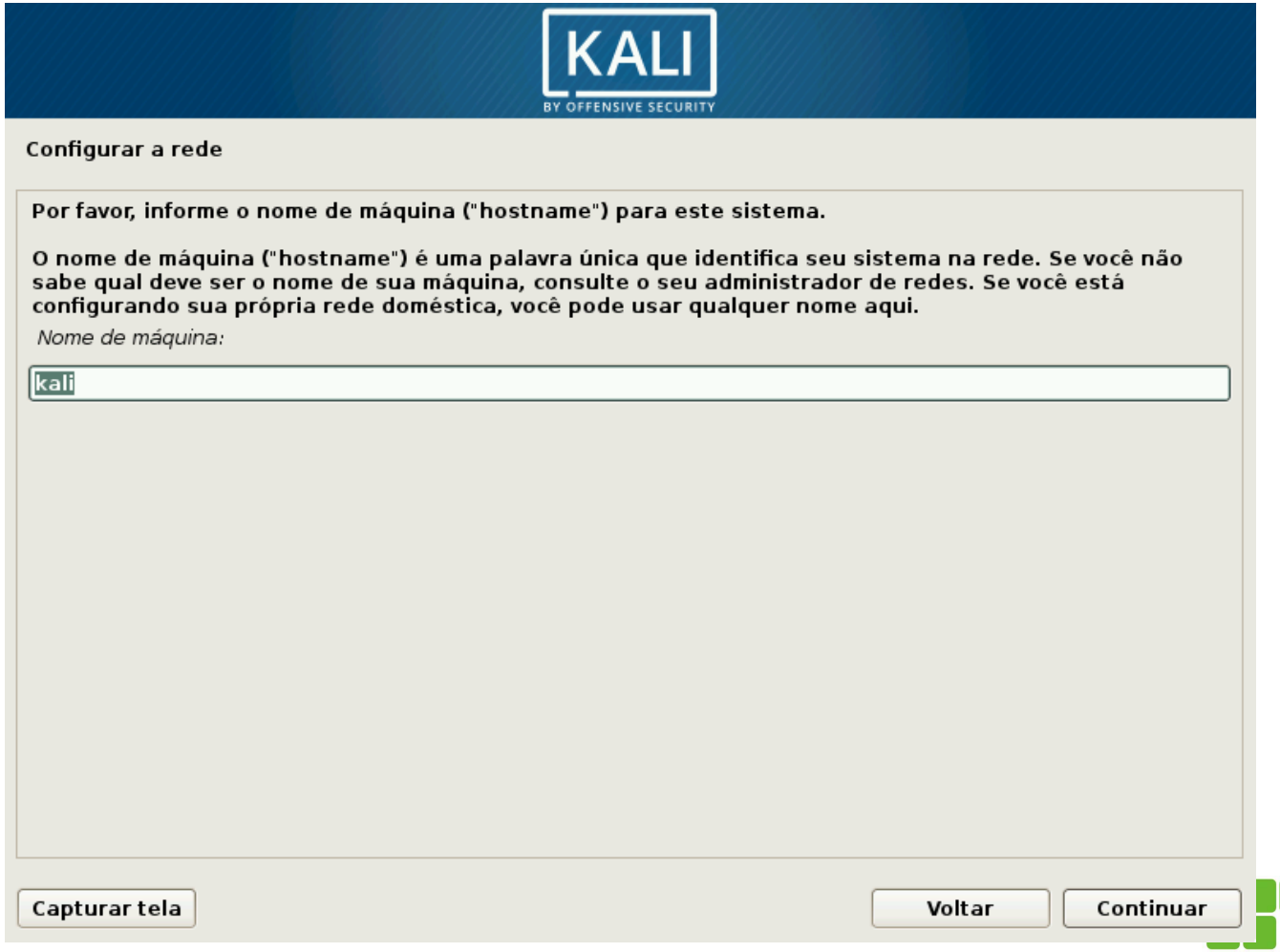


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Selecionando o Teclado

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Nome da Máquina

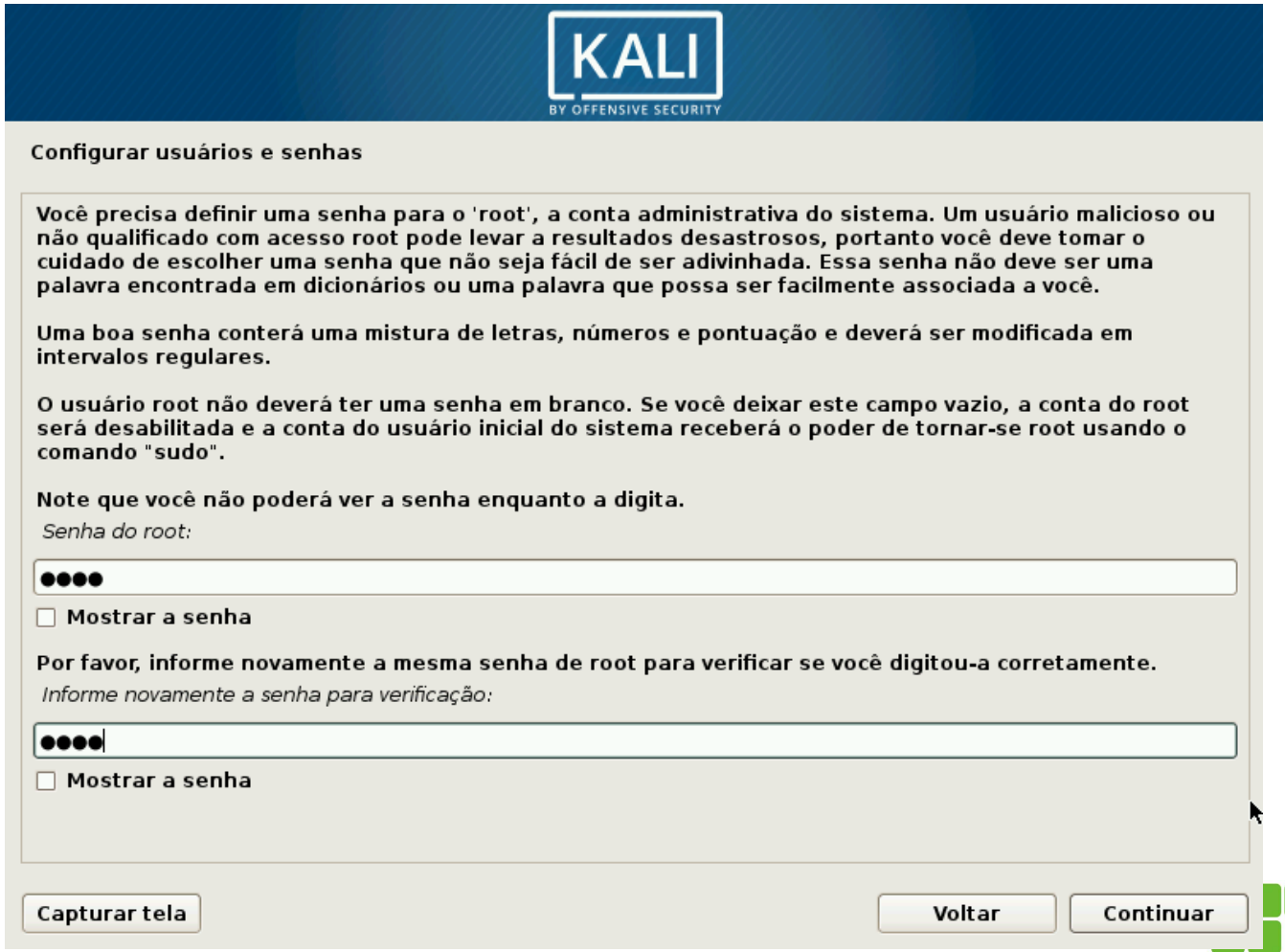


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Nome do Domínio (Deixar em branco)

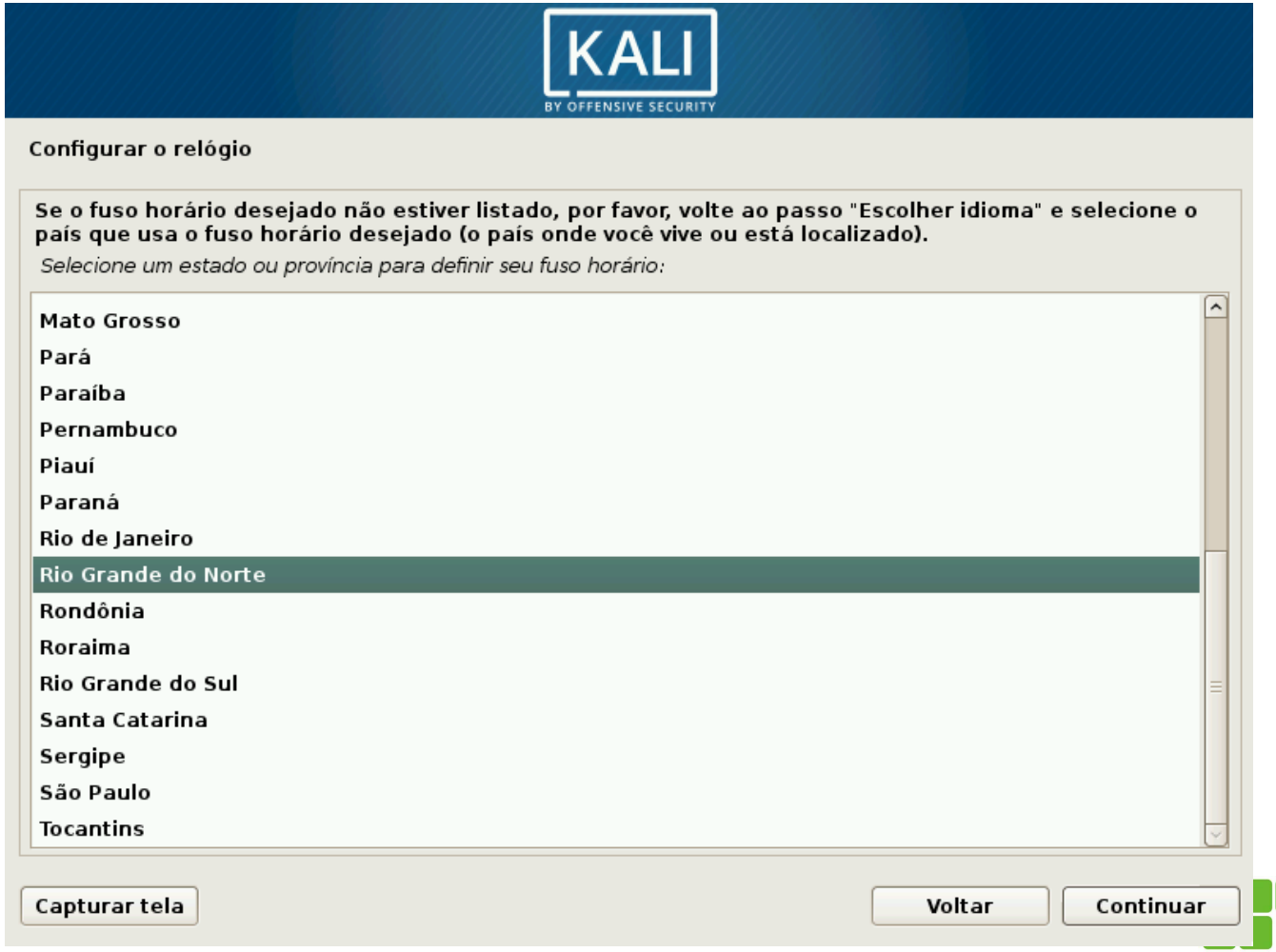
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Inserindo a Senha



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Selecionando o Fuso Horário



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

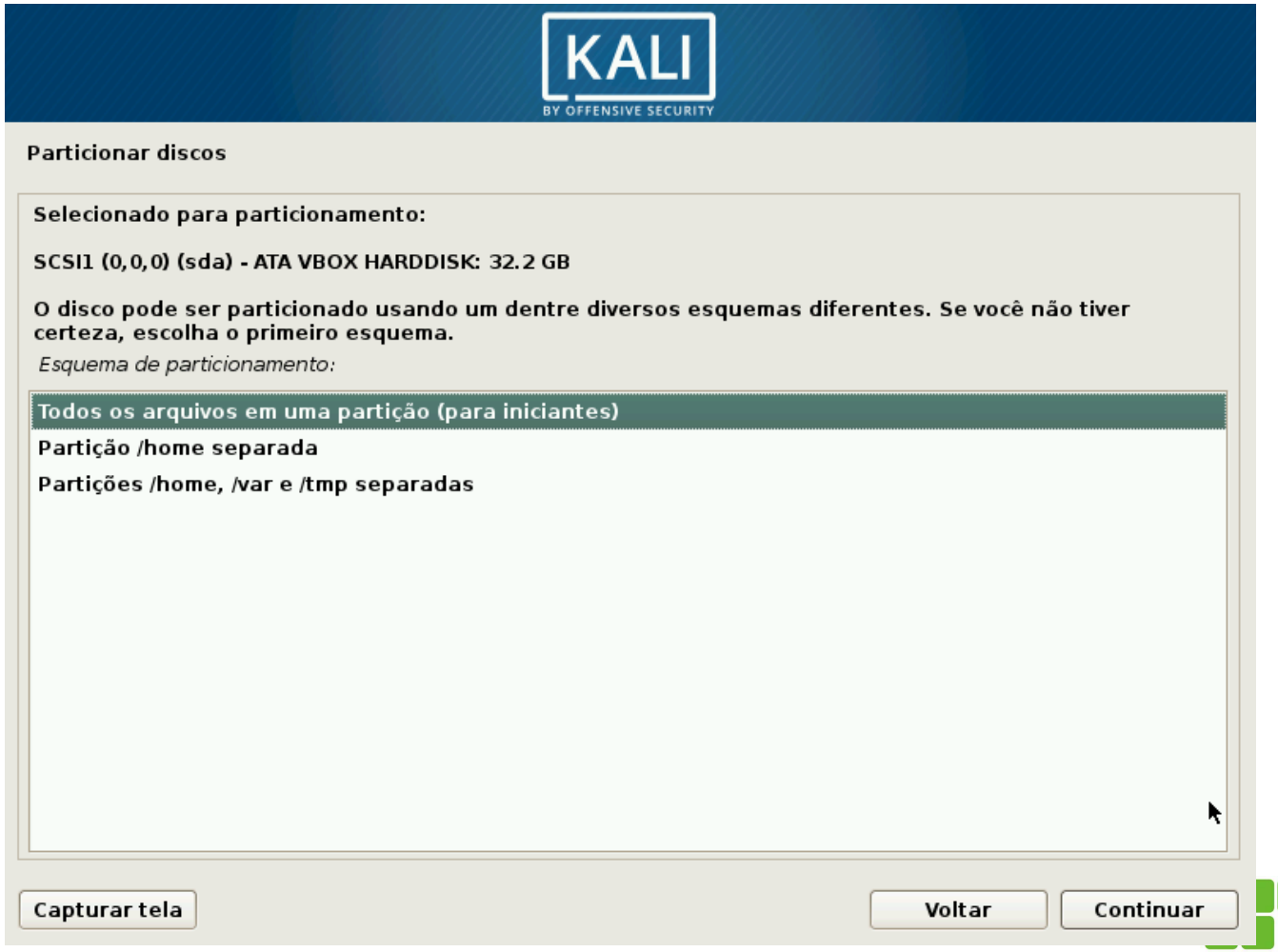
Gerenciando o Disco

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Selecionando o Disco

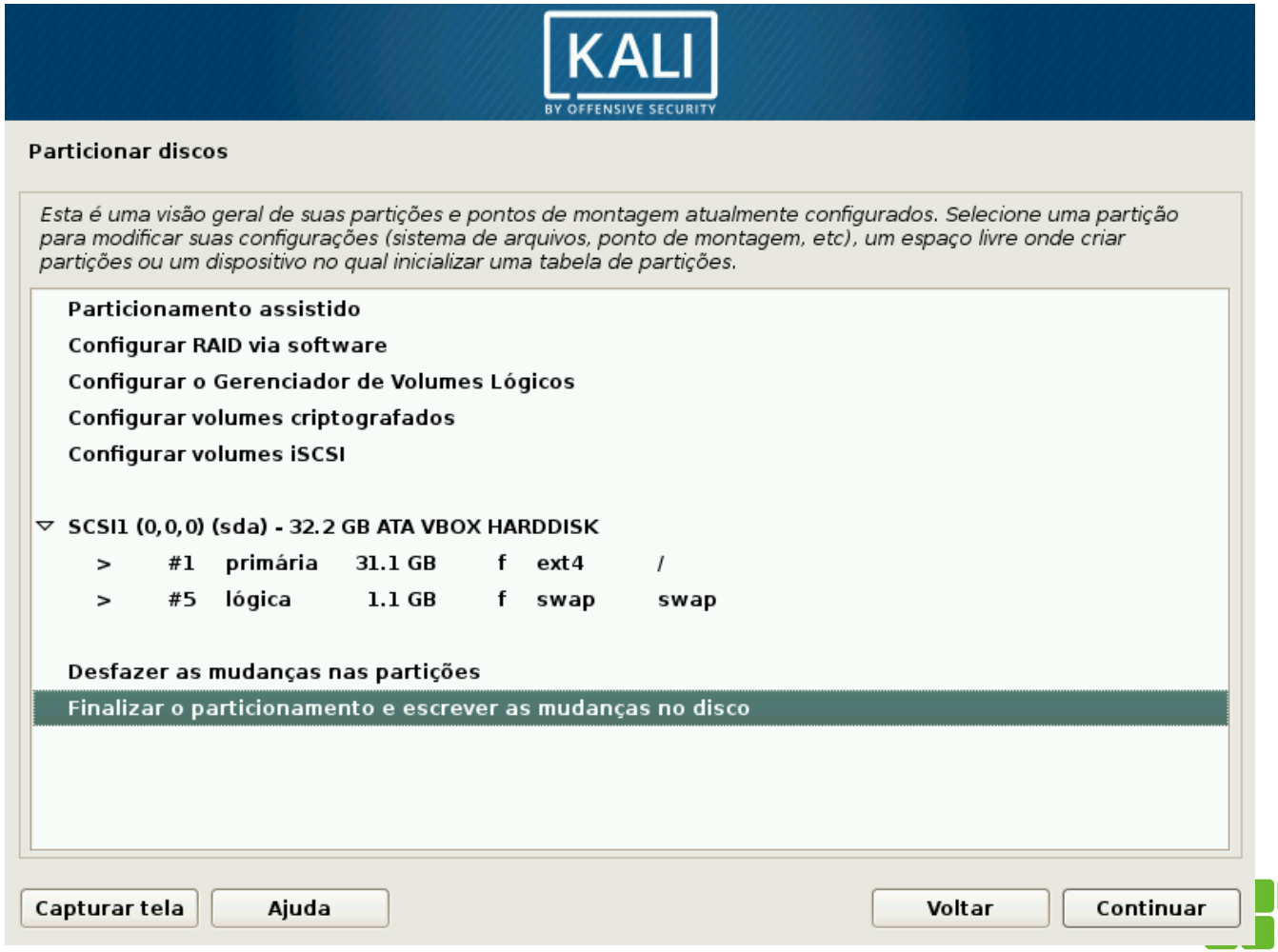
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gerenciando o Disco



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gerenciando o Disco



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Gerenciando o Disco

Início da Instalação

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Configuração de Pacotes

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

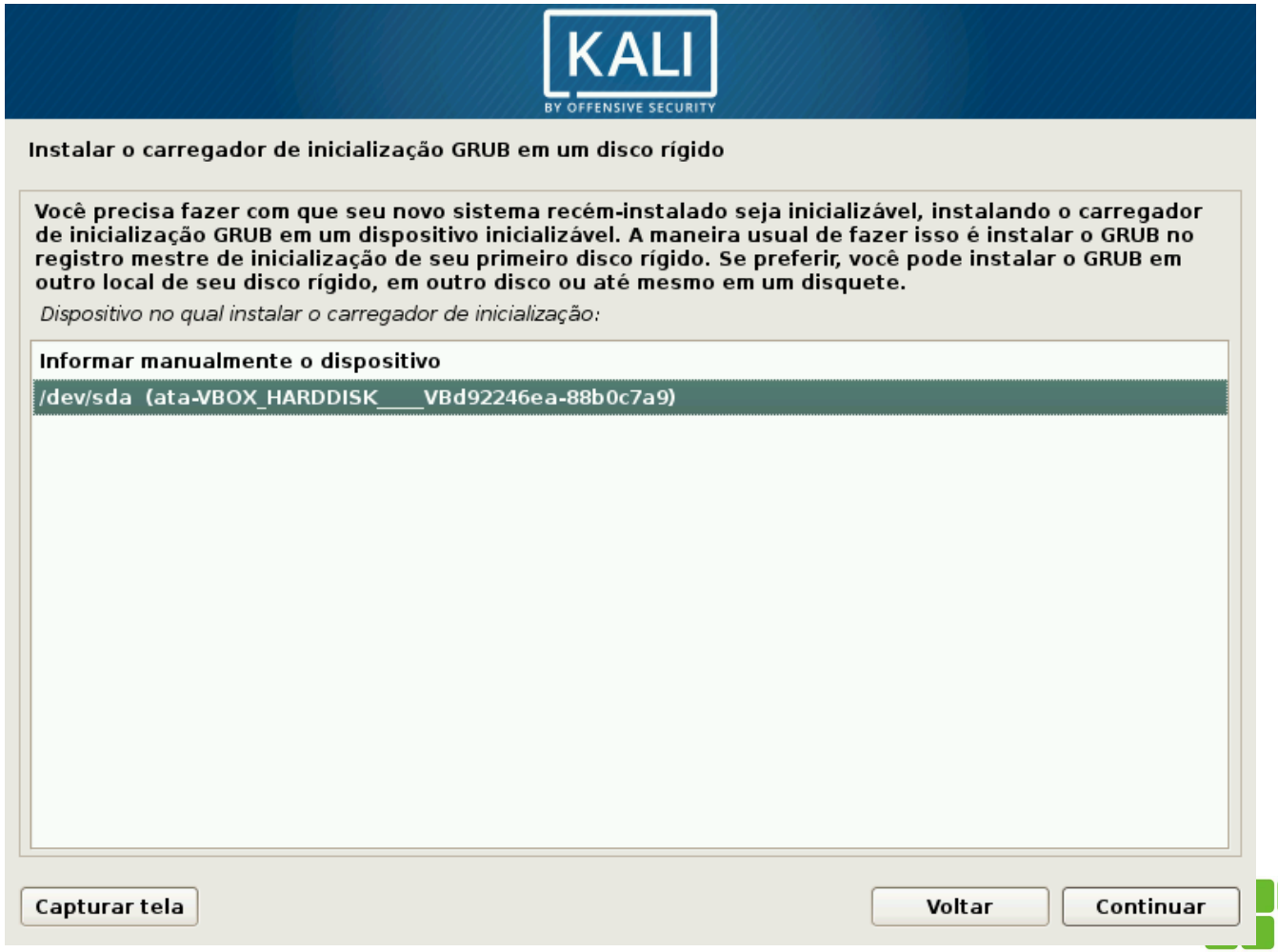
Configuração de Pacotes com Proxy

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Instalação do Grub

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Instalação do Grub



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Instalação Finalizada

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Interface Gráfica do Kali 2019.1

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ferramentas de Coleta de Informações

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Análise de Vulnerabilidade

- sfuzz;
- SidGuesser;
- SIPArmyKnife;
- sqlmap;
- Sqlninja;
- sqlsus;
- THC-IPV6;
- tnscmd10g;
- unix-privesc-check;
- etc.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ataques sem Fio

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Aplicativos Web

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ferramentas de Exploração de Vulnerabilidade

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ferramentas Forenses

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Sniffing e Spoofing

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ataques por Senha

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

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE