



PODER EXECUTIVO
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE RORAIMA
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

SISTEMAS OPERACIONAIS

RELATÓRIO DO SEMINARIO: KALI LINUX

ALUNOS:

Jasson Marques Fontoura Júnior – 2019014031

Marcos Vinicius Melo da Silva – 2019017919

Junho de 2022
Boa Vista/Roraima

Resumo:

Kali Linux é uma distribuição GNU/Linux baseada no Debian considerada a sucessora do Back Track. O projeto apresenta várias melhorias e mais aplicações. Destinase principalmente à auditoria geral e segurança informática. É desenvolvido e mantido pela Offensive Security Ltd. A partir de 21 de janeiro de 2016, é um lançamento de "lançamento contínuo". O Kali Linux vem pré-instalado com vários softwares, incluindo Nmap (scanner de portas), Wireshark (sniffer), John the Ripper (cracker de senhas) e Aircrack-ng (software para rede de computadores | rede testes de segurança sem fio) O sistema pode ser usado a partir de um live CD ou live-usb e pode ser instalado como o sistema operacional principal. É distribuído em imagens ISO compiladas para arquiteturas x86, x64 e ARM. O sistema aparece até em uma série de TV, neste caso, Mr. Robot

Qual o objetivo da distro Linux? Qual domínio de usuários?

O distro **Kali** tem como objetivo testes de penetração, hackers éticos e avaliações de segurança de rede. No lançamento, estava disponível apenas para profissionais já no setor de segurança. No entanto, com o desenvolvimento da Internet, as pessoas começaram a ter todos os tipos de informações na ponta dos dedos, e as notícias do Kali Linux se espalharam rapidamente.

Qual ambiente gráfico?

Por padrão, o **Kali Linux** usa **XFCE** pois é mais leve e rápido.

Descrever (vantagens e facilidades) do tipo de interface gráfica adotado pela distribuição.

A área de trabalho do **XFCE** é fina, rápida e elegante, tornando fácil descobrir como fazer o trabalho. Sua estrutura leve economiza memória e ciclos de CPU. Isso o torna ideal para hosts mais antigos com poucos recursos para a área de trabalho.

Quais wallpapers, ícones, cores e outros são disponibilizados pela distro?

Chromebook Image

Beaglebone Black ARM image

MK/SS808 ARM image

ODROID image

Raspberry Pi ARM image

Apresentar um tutorial de uso e de instalação do OS, apresentando os requisitos mínimos para instalação e qual deve ser o formato da partição do HD para a instalação.

Requisitos Mínimos:

Um mínimo de 20 GB de espaço em disco para a instalação do Kali Linux. RAM para arquiteturas i386 e amd64, mínimo: 1 GB, recomendado: 2 GB ou mais. Suporte de inicialização de unidade de CD-DVD / USB.

Instalação

Para iniciar sua instalação, inicialize com a mídia de instalação escolhida. Você deve ser saudado com a tela de inicialização do Kali Linux. Escolha instalação gráfica ou instalação (modo de texto). Neste exemplo, escolhemos a instalação gráfica.

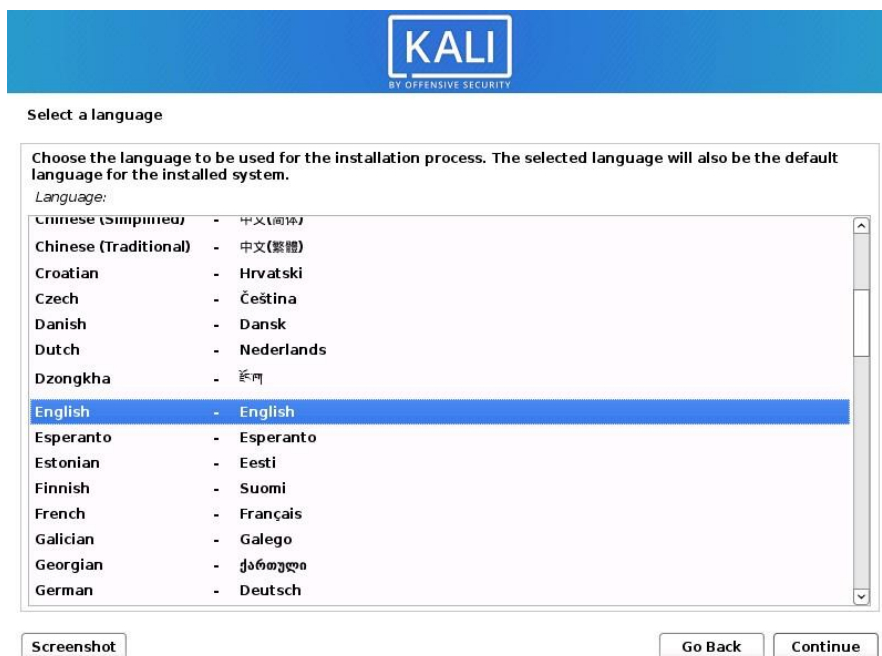


Se você estiver usando a imagem ao vivo, verá outro modo, Live, que também é a opção de inicialização padrão.



Linguagem

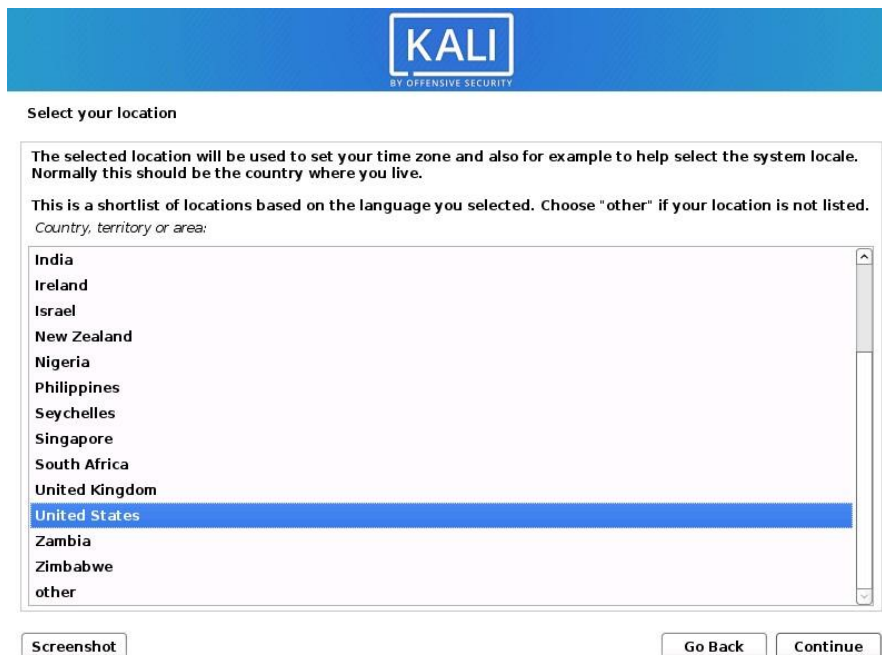
Selecione seu idioma preferido. Isso será usado para o processo de configuração e quando você estiver usando o Kali Linux.



The image shows the Kali Linux language selection screen. At the top is the Kali logo with the text "BY OFFENSIVE SECURITY". Below it, the heading "Select a language" is followed by instructions: "Choose the language to be used for the installation process. The selected language will also be the default language for the installed system." A list of languages is displayed, with "English" selected. At the bottom, there are buttons for "Screenshot", "Go Back", and "Continue".

Language:	
Chinese (Simplified)	- 中文(简体)
Chinese (Traditional)	- 中文(繁體)
Croatian	- Hrvatski
Czech	- Čeština
Danish	- Dansk
Dutch	- Nederlands
Dzongkha	- རྫོང་ཁ།
English	- English
Esperanto	- Esperanto
Estonian	- Eesti
Finnish	- Suomi
French	- Français
Galician	- Galego
Georgian	- ქართული
German	- Deutsch

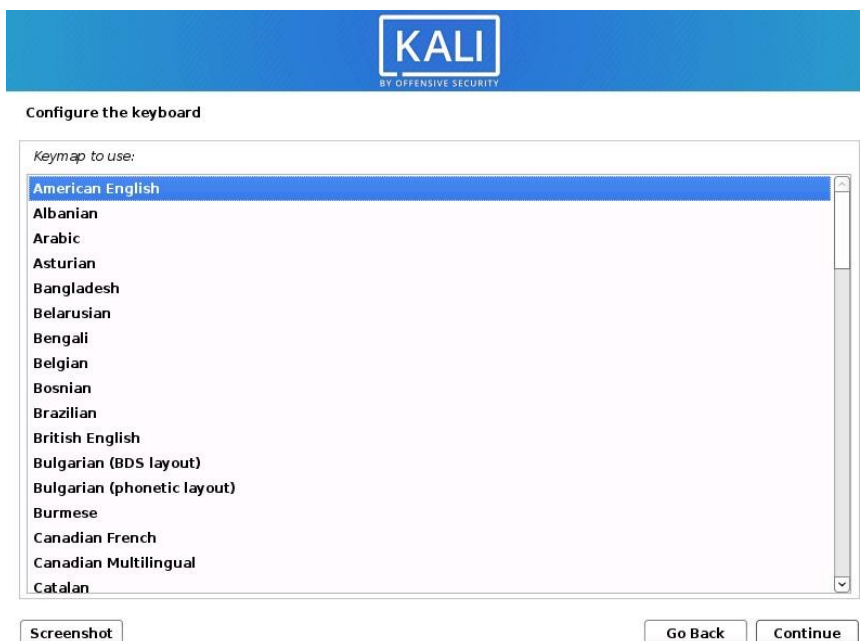
Especifique sua localização geográfica.



The image shows the Kali Linux location selection screen. At the top is the Kali logo with the text "BY OFFENSIVE SECURITY". Below it, the heading "Select your location" is followed by instructions: "The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live." A list of locations is displayed, with "United States" selected. At the bottom, there are buttons for "Screenshot", "Go Back", and "Continue".


Country, territory or area:
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other

Selecione o layout do teclado.



Rede

A configuração agora investigará suas interfaces de rede, procurará um serviço DHCP e solicitará que você insira um nome de host para seu sistema. No exemplo abaixo, inserimos kali como nosso nome de host. Se não houver acesso à rede com o serviço DHCP detectado, pode ser necessário configurar manualmente as informações de rede ou não configurar a rede neste momento. Se não houver um serviço DHCP em execução na rede, ele solicitará que você insira manualmente as informações de rede após pesquisar as interfaces de rede, ou você pode pular. Se o Kali Linux não detectar sua NIC, você precisará incluir os drivers para ela quando solicitado ou gerar uma ISO Kali Linux personalizada com eles pré-incluídos. Se a configuração detectar várias NICs, ela poderá perguntar qual usar para a instalação. Se a NIC escolhida for baseada em 802.11, você será solicitado a fornecer as informações de sua rede sem fio antes de ser solicitado um nome de host.



Configure the network


Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

[Screenshot](#) [Go Back](#) [Continue](#)

Opcionalmente, você pode fornecer um nome de domínio padrão para este sistema usar (os valores podem ser obtidos do DHCP ou se houver um sistema operacional pré-existente).



Configure the network


The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

[Screenshot](#) [Go Back](#) [Continue](#)

Contas de usuário

Em seguida, crie a conta de usuário para o sistema (nome completo, nome de usuário e senha forte).


BY OFFENSIVE SECURITY

Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Screenshot

Go Back

Continue


BY OFFENSIVE SECURITY

Set up users and passwords


Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

Screenshot

Go Back

Continue



BY OFFENSIVE SECURITY

Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

☐ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

☐ Show Password in Clear


Screenshot

Go Back

Continue

Relógio

Em seguida, defina seu fuso horário.


BY OFFENSIVE SECURITY

Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

Eastern

Central

Mountain

Pacific

Alaska

Hawaii

Arizona

East Indiana

Samoa

Screenshot

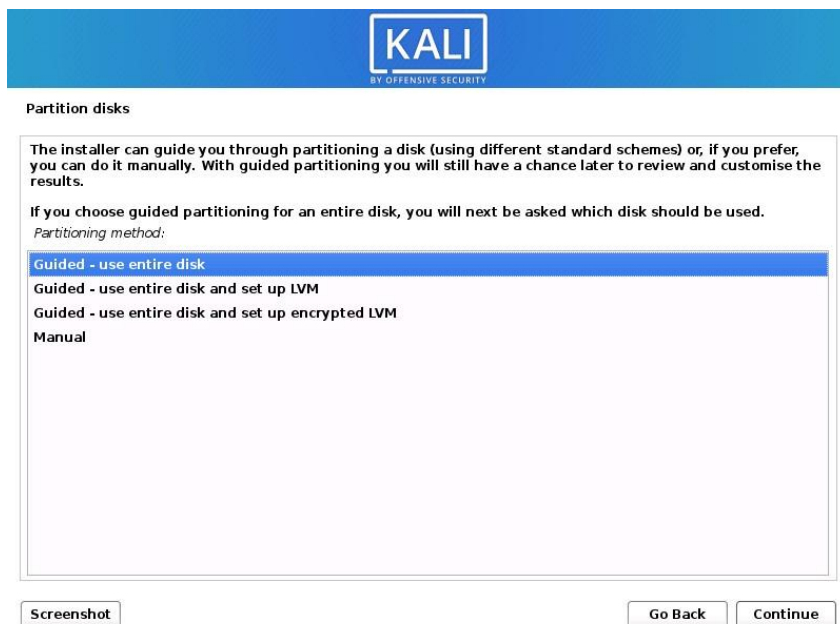
Go Back

Continue

Disco

O instalador agora sondará seus discos e oferecerá várias opções, dependendo da configuração. Em nosso guia, estamos usando um disco limpo, então temos quatro opções para escolher. Vamos selecionar Guided - o disco inteiro, pois esta é a instalação de inicialização única para o Kali Linux, portanto, não queremos nenhum outro sistema operacional instalado, por isso estamos felizes em limpar o disco. Se houver dados pré-existentes no disco, você terá uma opção extra (Guiado - use o maior espaço livre

contínuo) do que o exemplo abaixo. Isso instruiria a configuração a não alterar nenhum dado existente, o que é perfeito para inicialização dupla em outro sistema operacional. Como este não é o caso neste exemplo, não é visível. Usuários experientes podem usar o método de particionamento “Manual” para opções de configuração mais granulares. Se você deseja criptografar o Kali Linux, você pode habilitar Full Disk Encryption (FDE), selecionando Guided - use full disk e setup criptografado LVM. Quando selecionado, mais tarde na configuração (não neste guia) solicitará que você insira uma senha (duas vezes). Você terá que digitar essa senha toda vez que iniciar o Kali Linux.

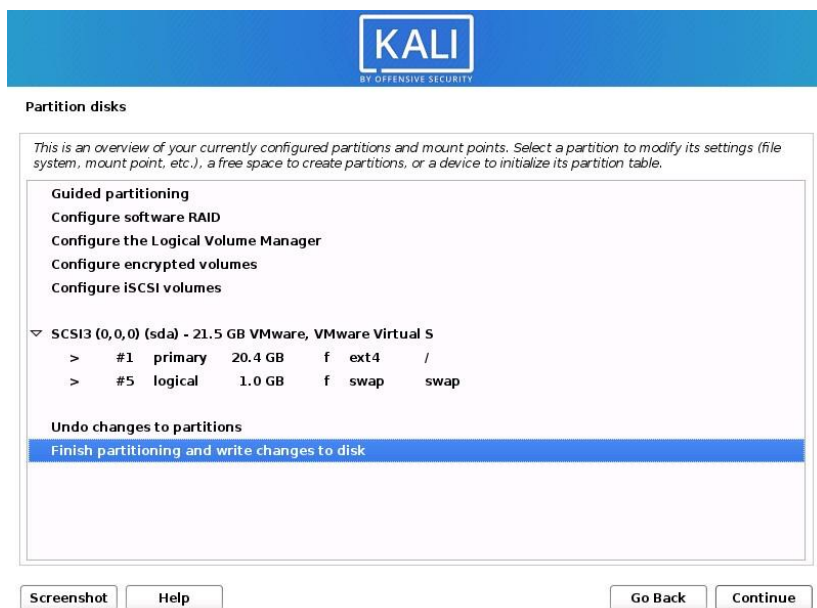
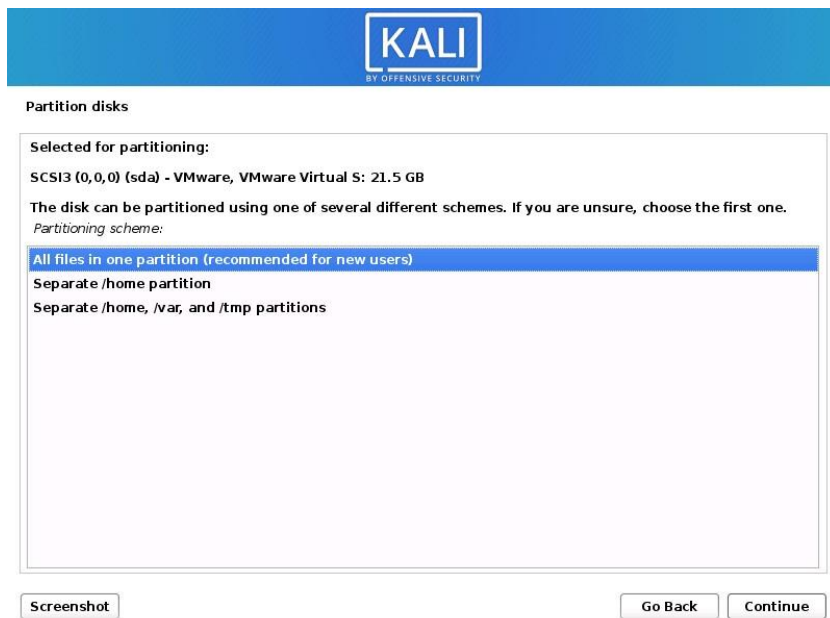


Selecione o disco a ser particionado.




Dependendo de suas necessidades, você pode optar por manter todos os

seus arquivos em uma única partição - o padrão - ou ter partições separadas para um ou mais diretórios de nível superior. Se você não tem certeza de qual deseja, você quer “Todos os arquivos em uma partição”.



Em seguida, você terá uma última chance de revisar a configuração do disco antes que o instalador faça alterações irreversíveis. Depois de clicar em Continuar, o instalador começará a funcionar e você terá uma instalação quase finalizada.



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #2 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

☐ No
☒ Yes


Screenshot Continue

LVM criptografado

Se ativado na etapa anterior, o Kali Linux agora começará a executar uma limpeza segura do disco rígido, antes de solicitar uma senha do LVM. Certifique-se de uma senha forte, caso contrário você terá que concordar com o aviso sobre uma senha fraca. Essa limpeza pode demorar “um pouco” (horas), dependendo do tamanho e da velocidade da unidade. Se você quiser arriscar, pode pular.

Informações de proxy

Kali Linux usa um repositório central para distribuir aplicativos. Você precisará inserir qualquer informação de proxy apropriada conforme necessário.



Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

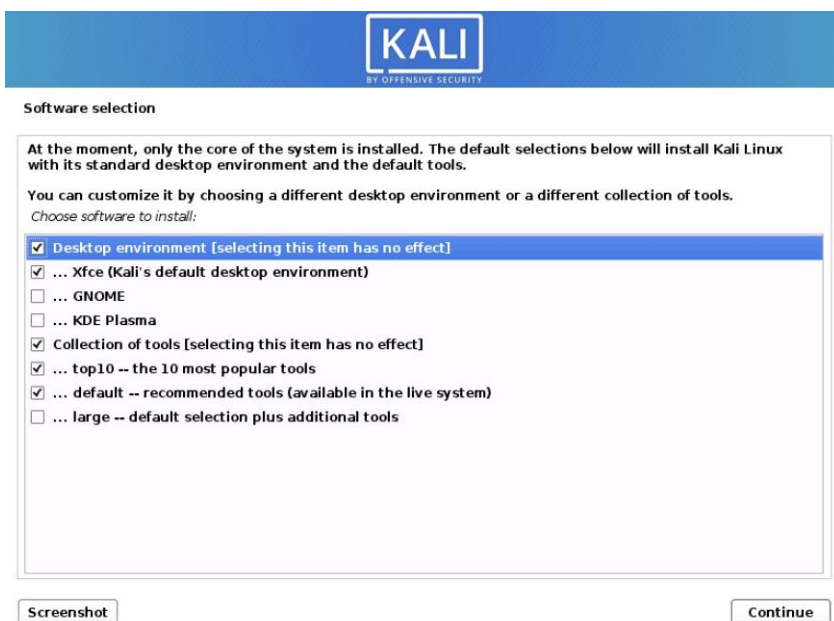
The proxy information should be given in the standard form of “http://[[user]]:[pass]@host[:port]/”.

HTTP proxy information (blank for none):

Screenshot Go Back Continue

Metapackages

Se o acesso à rede não foi configurado, você desejará continuar com a configuração quando solicitado. Se você estiver usando a imagem ao vivo, não terá o seguinte estágio. Em seguida, você pode selecionar quais metapackages você gostaria de instalar. As seleções padrão instalarão um sistema Kali Linux padrão e você realmente não precisa alterar nada aqui.



KALI
BY OFFENSIVE SECURITY

Software selection

At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.

You can customize it by choosing a different desktop environment or a different collection of tools.

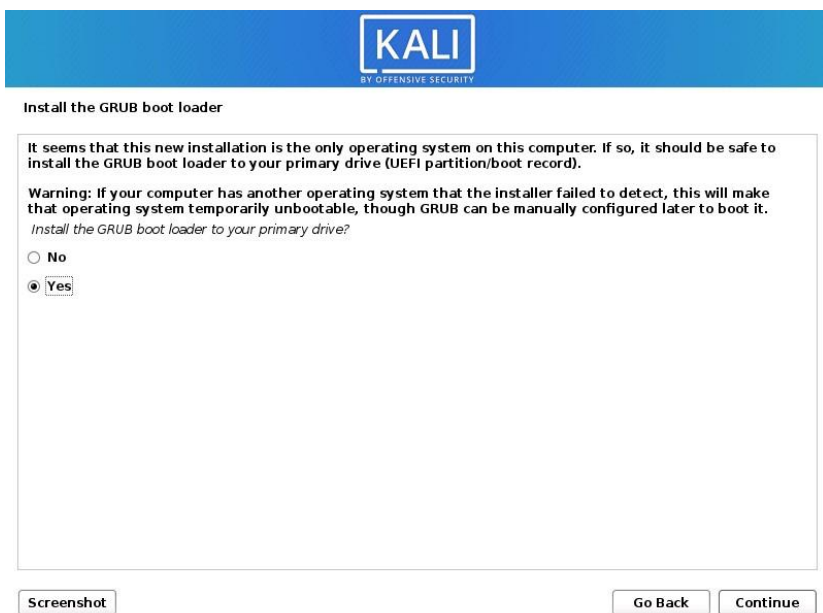
Choose software to install:

- ☒ Desktop environment [selecting this item has no effect]
 - ☒ ... Xfce (Kali's default desktop environment)
 - ☐ ... GNOME
 - ☐ ... KDE Plasma
- ☒ Collection of tools [selecting this item has no effect]
 - ☒ ... top10 -- the 10 most popular tools
 - ☒ ... default -- recommended tools (available in the live system)
 - ☐ ... large -- default selection plus additional tools

Screenshot Continue

Informações de inicialização

Em seguida, confirme para instalar o carregador de inicialização GRUB.



KALI
BY OFFENSIVE SECURITY

Install the GRUB boot loader

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).

Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

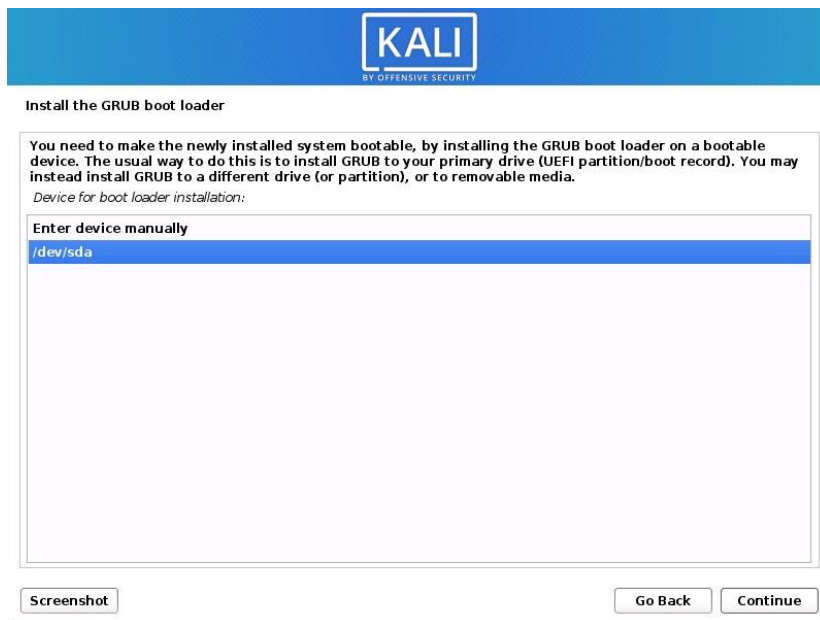
Install the GRUB boot loader to your primary drive?

☐ No

☒ Yes

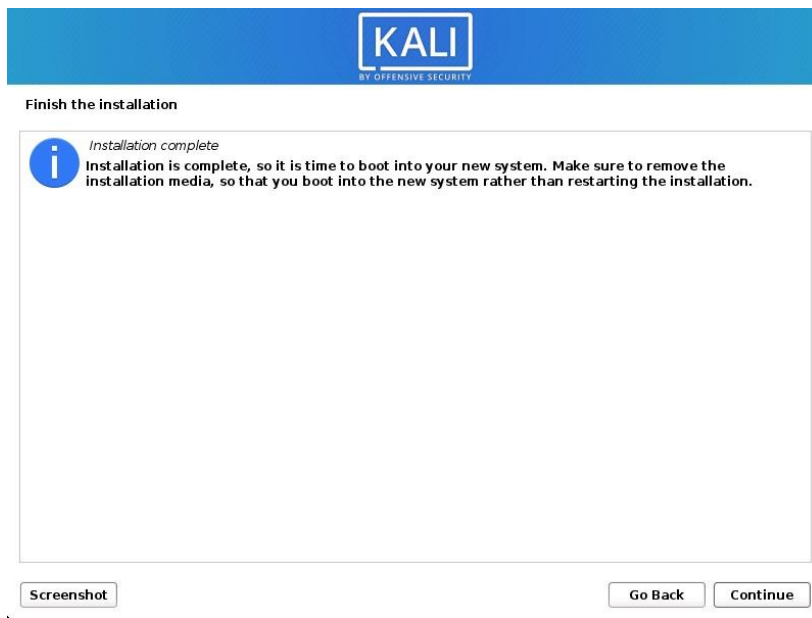
Screenshot Go Back Continue

Selecione o disco rígido para instalar o bootloader GRUB (por padrão, ele não seleciona nenhuma unidade).



Reinício

Por fim, clique em Continuar para reiniciar em sua nova instalação do Kali Linux.



Descrever o uso (vantagens e facilidades) da distribuição linux com exemplos.

Se você estiver interessado em testes de penetração ou segurança de rede,

precisará de algumas ferramentas específicas para executar algumas tarefas pré-instaladas e configuradas no Kali Linux para que você possa usá-las diretamente sem qualquer configuração. Ou, se alguém quiser verificar um site em busca de vulnerabilidades ou aprender sobre bugs relacionados à segurança em qualquer aplicativo, seria ótimo usar o Kali Linux. Muitas pessoas pensam no Kali como uma ferramenta para hackear contas sociais ou servidores da web. Este é um dos maiores mitos sobre o Kali Linux. Kali Linux é apenas mais uma distribuição Debian com uma tonelada de ferramentas de rede e segurança. É uma arma para treinar ou se proteger de atacar alguém. Kali Linux é projetado principalmente para profissionais. É para aqueles que querem entrar em testes de penetração, segurança cibernética ou hacking ético.

Listar os softwares presentes da distribuição, bem como, o objetivo de cada software.

Aircrack-ng: é um conjunto de software de rede que consiste em um detector, sniffer de pacotes, cracker WEP e WPA / WPA2-PSK e ferramenta de análise para LANs sem fio 802.11.

Autopsy: é um software de computador que simplifica a implantação de muitos dos programas e plug-ins de código aberto usados no The Sleuth Kit.

Armitage: é uma ferramenta gráfica de gerenciamento de ataques cibernéticos para o Projeto Metasploit que visualiza alvos e recomenda exploits.

Burp suite: é um software desenvolvido em Java pela PortSwigger, para a realização de testes de segurança em aplicações web

BeEF: é uma ferramenta de teste de penetração de código aberto usada para
testar e explorar aplicações web e vulnerabilidades baseadas em navegador.

Cisco Global Exploiter: um programa educacional gratuito que permite simular uma rede de computadores, através de equipamentos e configurações presente em situações reais.

Ettercap: é uma ferramenta de segurança de rede gratuita e de código aberto para ataques man-in-the-middle em uma LAN.

Hashcat: é uma ferramenta de recuperação de senha. Ele tinha uma base de
código proprietária até 2015, mas foi lançado como software de código aberto.

John the Ripper: é uma ferramenta gratuita de software de quebra de senha.

Kismet: é um detector de rede, sniffer de pacotes e sistema de detecção de intrusão para LANs sem fio 802.11.

Lynis: é uma ferramenta de auditoria de segurança extensível para sistemas de computador que executam Linux, FreeBSD, macOS, OpenBSD, Solaris e outros derivados do Unix.

Maltego: é um software usado para inteligência e forense de código aberto, desenvolvido por Paterva de Pretória, África do Sul.

Metasploit framework: é um projeto de segurança de computadores que fornece informações sobre vulnerabilidades de segurança e auxilia em testes de penetração e desenvolvimento de assinaturas IDS.

Nmap: é um scanner de rede criado por Gordon Lyon (também conhecido por seu pseudônimo *Fyodor Vaskovich*).

Nikto: um scanner de vulnerabilidade de linha de comando de software gratuito que verifica servidores da Web em busca de arquivos/CGIs perigosos, software de servidor desatualizado e outros problemas. Ele executa verificações genéricas e específicas do tipo de servidor.

OWASP ZAP: (abreviação de **Zed Attack Proxy**) é um scanner de segurança de aplicativos da Web de código aberto.

Social engineering tools: é uma ferramenta de código aberto para realizar ataques de engenharia social online.

Sqlmap: é uma ferramenta open source para teste de penetração que automatiza o processo de detecção e exploração de vulnerabilidades de Injeção de SQL, permitindo a invasão de banco de dados de sites.

Wireshark: é um programa que analisa o tráfego de rede, e o organiza por protocolos

WPScan: é um scanner de segurança WordPress de caixa preta gratuito, para uso não comercial, escrito para profissionais de segurança e mantenedores de blogs para testar a segurança de seus sites.

Nessus: é um programa de verificação de falhas/vulnerabilidades de segurança.

Zenmap: É um aplicativo multiplataforma (Linux, Windows, Mac OS X, BSD,

etc.) gratuito e de código aberto que visa tornar o Nmap fácil de usar para iniciantes enquanto fornece recursos avançados para usuários experientes do Nmap.

Hydra: é um cracker de login de rede paralelizado construído em vários sistemas operacionais como Kali Linux, Parrot e outros grandes ambientes de teste de penetração.

Reverse engineering toolkit: Esta é uma coleção de ferramentas que você pode gostar se estiver interessado em engenharia reversa e/ou análise de malware em sistemas Windows x86 e x64.

Foremost: é um programa de recuperação de dados forense para Linux usado para recuperar arquivos usando seus cabeçalhos, rodapés e estruturas de dados por meio de um processo conhecido como esculpimento de dados.

Volatility: é uma estrutura forense de memória de código aberto para resposta a incidentes e análise de malware.

VulnHub: Fornecer materiais que permitam a qualquer pessoa ganhar experiência prática em segurança digital, software de computador e administração de rede.

Descrever o gerenciador de pacotes e a lista de pacotes de softwares presentes na distribuição, exemplo, software de terceiros e proprietários.

O Synaptic Package Manager e o Software Center são dois dos gerenciadores de software mais conhecidos do **Kali**. Com o Ubuntu, por exemplo, o Software Center é instalado automaticamente como o aplicativo padrão. O sistema de orquestração da APT, o Synaptic, são inerentemente mais robustos que o desenvolvimento de software porque funciona dentro de uma arquitetura que depende da GUI.

Alguns dos pacotes de softwares presentes na **Kali Linux**:

Hydra: Debian Security Tools

John: Kali Developers

Nmap: Kali Developers

Samba: Debian Samba maintainers

Gparted: Phillip Susi

Veil: Kali Developers

Testdisk: Jean-Michel Kelbert

Crack: Debian Security Tools

Git: Jonathan Nieder

Apresentar um histórico sobre a distribuição Linux e listar quem usa (empresas, instituições e etc) a distribuição.

Data	Projeto Lançado	Base OS
2004-Agosto-	Whoppix v2 30	Knoppix
2005-Julho-	WHAX v3 17	Slax
2006-Maio-26	BackTrack v1	Slackware Live CD 10.2.0
2007-Março-	BackTrack v2 06	Slackware Live CD 11.0.0
2008-Junho-	BackTrack v3 19	Slackware Live CD 12.0.0
2010-Janeiro-09	BackTrack (Pwnsauce)	v4 Ubuntu 8.10 (Intrepid Ibex)
2011-Maio-10	BackTrack (Revolution)	v5 Ubuntu 10.04 (Lucid Lynx)
2013-Março-13	Kali Linux (Moto)	v1 Debian 7 (Wheezy)
2015-Agosto-11	Kali Linux (Sana)	v2 Debian 8 (Jessie)

2016-Janeiro-

Kali Linux Rolling Debian Testing 16

4 empresas reportaram que estavam usando o **Kali Linux** que são as Labs, studio666.descartes, ventx e Cyber Security.

Qual a versão de kernel Linux adotada? E quais as principais características no kernel Linux adotado pela distribuição?

O kernel é o centro essencial de um sistema operacional de computador (SO). É o núcleo que fornece serviços básicos para todas as outras partes do sistema operacional. Atualmente o Kali Linux acompanha a versão 5.16.0 do Kernel. O Linux 5.16 apresenta um novo sistema de kernel chamado FUTEX2. Contribuído pela Collabora, esse recurso pode ajudar a melhorar a experiência de jogo no Linux, mais especificamente, para jogos Windows executados via Wine. Além disso, o relatório de integridade do sistema de arquivos recebe um impulso graças a uma nova API baseada em fanotify, embora os novatos do Kernel observem que isso suporta apenas o sistema de arquivos EXT4 no momento. Esse ajuste melhora as daemons de monitoramento da integridade do sistema, informando a eles apenas o primeiro erro ocorrido desde a última notificação de erro, em seguida, mantendo uma contagem de erros adicionais.

O quão seguro é a distro Linux analisada?

O sistema de distribuição Linux de código aberto baseado no Debian Kali Linux é uma ferramenta poderosa usada principalmente para segurança ofensiva. Anteriormente conhecido como Backtrack Linux, o sistema é um símbolo de segurança em si. Usado por alunos com o objetivo de aprender computação em profundidade e veteranos experientes praticando testes de penetração e outras coisas. Mas rodar o Kali Linux com as configurações padrões pode não ser uma boa ideia. O Kali Linux inclui mais de 600 ferramentas de teste de penetração incluídas em sua compilação. No entanto, existem algumas configurações e ajustes importantes que precisam ser revertidos pelo usuário:

Alterar a senha padrão:

Uma senha padrão é uma senha muito insegura, o Kali Linux vem com um nome de usuário e senha padrão. É "Kali" ou "toor" por padrão, dependendo de como a distribuição é usada. Alterá-lo é um processo simples.

Atualizando o Kali com frequência:

Existem inúmeras versões do Kali Linux. O sistema de distribuição Linux atualiza seu perfil mensalmente. Ele contém atualizações de segurança, correções de bugs, proteção de extensões e suplementos e muito mais.

Identidade segura:

Ao navegar na internet com uma máquina Kali Linux, podemos usar o script “kalitorify” para navegar de forma segura e anônima. Mesmo que “macchanger” seja recomendado para alterar o nome do host de antemão. Podemos alterar nosso nome de host de Kali para um servidor de nomes.

Filtragem de pacotes ou firewall:

Um firewall atua como uma parede entre as conexões de entrada e saída. Embora o firewall padrão venha com um conjunto de regras, os usuários podem alterar e modificar conforme a necessidade. O firewall analisa todos os pacotes e evita conexões e arquivos não autorizados. Um firewall atua como uma parede entre as conexões de entrada e saída. Embora o firewall padrão venha com um conjunto de regras, os usuários podem alterar e modificar conforme a necessidade. O firewall analisa todos os pacotes e evita conexões e arquivos não autorizados.

Qual a documentação da distro Linux? A documentação é ampla?

A documentação é ampla, composta pela:

Introdução: Como o nome já diz, traz um belo resumo sobre a distro

Instalação: Possui um tutorial de instalação para diferentes tipos de sistemas operacionais

Virtualização: Tutorial para softwares de virtualização

USB: Tutoriais para desenvolver um pen drive bootável com o Kali dentro.

Existem diversas outras documentações presentes no site oficial do Kali Linux, com muitas outras informações tornando – se uma distro bem completa em relação a documentação.

Qual a configuração de hardware mínima para instalação e uso do OS?

Os requisitos de instalação do Kali Linux variam dependendo do que você deseja instalar e da sua configuração. Para requisitos do sistema:

No limite inferior, você pode configurar o Kali Linux como um servidor Secure Shell (SSH) básico sem desktop, usando apenas 128 MB de RAM (512 MB recomendados) e 2 GB de espaço em disco. Na extremidade superior, se você optar por instalar o desktop Xfce4 padrão e o metapacote kali-linux-default, você deve realmente procurar pelo menos 2 GB de RAM e 20 GB de espaço em disco. Ao usar aplicativos de uso intensivo de recursos, como o Burp Suite, eles recomendam pelo menos 8 GB de RAM (e ainda mais se for um aplicativo da Web grande!) ou usar programas simultâneos ao mesmo tempo.

Quais as placas de GPU suportadas pela distro?

Ele suporta as placas da NVIDIA, o driver NVIDIA deve ser instalado via `run sudo apt install NVidia-detect` usando `sudo apt install NVidia-detect`.

Suporte para TPM2, SecureBoot ecriptografia de armazenamento automatizado.

Um TPM (Trusted Platform Module) é um componente de processador de criptografia seguro que nos permite melhorar a segurança do hardware por meio de chaves criptográficas integradas. Sistemas operacionais modernos como Linux ou Windows podem fazer isso e, portanto, geralmente, o requisito mínimo é habilitar seu módulo TPM nas opções do BIOS e configurar o sistema operacional para usá-lo, no Windows o processo deve ser mais fácil para o usuário, enquanto no Linux ainda requer uma pequena dificuldade; O Kali Linux não suporta ser inicializado via secureboot, então o processo de ir na bios do dispositivo e desativar o secureboot; A configuração da criptografia completa do disco com o Kali é um processo simples. O instalador do Kali inclui um processo direto para configurar partições criptografadas com LVM e LUKS. Uma vez criptografado, o sistema operacional Kali requer uma senha no momento da inicialização para permitir que o sistema operacional inicialize e decriptografe sua unidade, protegendo assim esses dados caso seu laptop seja roubado. O gerenciamento de chaves e partições de decriptografia é feito usando o utilitário cryptsetup.

Quais as deamons padrões do OS?

Os padrões no distro são os mesmos do Linux, logo para identificar um daemon é só procurar um processo que termine com a letra d. É uma regra geral do Linux que os nomes dos daemons terminem dessa maneira. Há muitas maneiras de identificar um daemon em execução. Eles podem ser vistos nas listagens de processos por meio de `ps`, `top` ou `htop`. Esses são programas úteis por si só – eles têm um propósito específico, mas para ver todos os daemons em execução em sua máquina, o comando `ps tree` se adequará melhor.

Interpretador de comandos padrão do OS.

O shell é o interpretador de linha de comando do Linux. Ele fornece uma interface entre o usuário e o kernel e executa programas chamados comandos. Por exemplo, se um usuário inserir `ls`, o shell executará o comando `ls`. O shell também pode executar outros programas, como aplicativos, scripts e programas de usuário. Zsh é um outro interpretador de comandos UNIX (shell) presente no Kali utilizável como um shell de login interativo e como um processador de comandos de script de shell. Dos shells padrão,

o zsh se assemelha mais ao ksh, mas inclui muitos aprimoramentos. O Zsh possui edição de linha de comando, correção ortográfica integrada, conclusão de comando programável, funções de shell (com carregamento automático), um mecanismo de histórico e uma série de outros recursos.

Edições ou spin-offs

Kali Linux 1.1.0

A primeira versão lançada após a criação acompanhou os seguintes features:

- A nova versão executou um kernel 3.18, corrigido para ataques de injeção sem fio.
- Ossistemas de compilação ISO foram executados no live-build 4.x.
- Suporte aprimorado ao driver sem fio, devido a atualizações de kernel e firmware.
- Suporte a hardware NVIDIA Optimus.

Kali Linux 2020.1

Lançada no começo do século ela trouxe:

- Non-Root. Ao longo da história do Kali (e seus predecessores BackTrack, WHAX e Whoppix), as credenciais padrão foram root/toor. Não usaram mais a conta de superusuário, root, como padrão no Kali 2020.1. A conta de usuário padrão se tornou um usuário padrão, sem privilégios.
- Novos Pacotes. O Kali Linux é uma distribuição contínua, por isso recebe atualizações assim que estão disponíveis, em vez de esperar pelo “próximo lançamento”. Portanto, desde a última versão, tem as atualizações normais de ferramentas, bem como algumas novas ferramentas foram adicionadas, como: cloud-enum, emailharvester, phpggc, sherlock, splinter.

Referências Bibliográficas:

<https://www.kali.org/>

https://en.wikipedia.org/wiki/Kali_Linux