

Kali Linux

Instalação e Configuração de
um Ambiente para

Hacking Ético

e Teste de Vulnerabilidade



SOBRE OS DIREITOS AUTORAIS

Todos os direitos são reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida livremente de alguma forma, sem o consentimento prévio dos seus autores. Se por ventura tiver interessado na publicação de uma análise livro por favor entre em contato com atendimento@e-tinet.com.

Atualizações do livro visite sempre em <http://e-tinet.com/materiais/ebook-kali-linux/>

UTILIZAÇÃO DO LIVRO

O autor deste livro não se responsabiliza direta ou indiretamente pela utilização de qualquer um dos exercícios ou dicas nele contidos. Estes exercícios e dicas são baseados em experiências pessoais e profissionais de Pedro Delfino, bem como da experiência adquirida através de testemunhos de outros usuário. O objetivo deste livro é ensinar como você pode montar seu ambiente de trabalho utilizando Kali Linux, focado em Hacking Ético e Teste de Vulnerabilidade

SOBRE PEDRO DELFINO

Pedro Delfino é o fundador do PROFISSIONAIS LINUX (<http://profissionaislinux.com.br>) que tem como principal objetivo formar novos profissionais para atuar na área de administração de servidores LINUX assim como soluções opensource, é autor do E-tinet, (<http://e-tinet.com>) um blog sobre soluções LINUX que já ajudou milhares de leitores com seus Ebooks e treinamentos On-line.

Utiliza Linux como ferramenta de trabalho a mais de 14 anos, e a mais de 3 anos vem ajudando milhares de pessoas a aprender Linux de forma fácil e rápida, através de artigos em seu Blog.





SUMÁRIO

SOBRE O KALI LINUX

REQUISITOS DE SISTEMA PARA MONTAR SEU AMBIENTE COM KALI LINUX

8

2.1 VAMOS AOS REQUISITOS PARA A INSTALAÇÃO DO KALI LINUX

10

COMO CRIAR UM PENDRIVE BOOTÁVEL PARA INSTALAÇÃO DO KALI LINUX

11

3.1 PARA QUEM NÃO UTILIZA LINUX

13

3.2) PARA QUEM JÁ UTILIZA LINUX

15

INSTALAÇÃO DO KALI LINUX

18

CONCLUSÃO

31



SOBRE O KALI LINUX



1. SOBRE O KALI LINUX

Kali Linux é indiscutivelmente uma das melhores distribuições Linux disponíveis para testes de segurança e hackers em geral.

Muitas das ferramentas do Kali Linux podem ser instaladas na maioria das distribuições, a equipe de desenvolvimento do Kali investiu horas e mais horas para aperfeiçoar sua distribuição 100% focada em segurança, e pronta para inicializar em qualquer computador.

O Kali Linux é uma distribuição focada em segurança da informação e baseada em Debian. A distribuição vem com centenas de ferramentas de segurança bem conhecidas, e hoje já tem uma ótima fama.

Na imagem ao lado, cena da série Mr. Robot onde o Kali Linux é amplamente utilizado.



O Kali ainda é ligado a uma indústria respeitada de certificação, chamada "Pentesting with Kali (Pentesting com Kali).

A certificação é um desafio rigoroso de 24 horas em que os candidatos devem comprometer com êxito um número de computadores, escrever um relatório de teste de penetração profissional que será enviado para o pessoal da Offensive Security ([veja mais aqui](#)).

A aprovação deste exame permitirá obter a credencial do OSCP. (Offensive Security Certified Professional – OSCP Certification)

O foco deste guia é ajudar você a se familiarizar mais com o Kali Linux e várias das ferramentas disponíveis na distribuição.

Certifique-se de usar extrema cautela com as ferramentas incluídas com Kali como muitos deles podem acidentalmente ser usado de uma maneira que quebrará sistemas de computador.

As informações contidas dentro deste ebook de Kali Linux são pretendidas para usos legais.



REQUISITOS DE SISTEMA PARA MONTAR SEU AMBIENTE COM KALI LINUX



2. REQUISITOS DE SISTEMA PARA MONTAR SEU AMBIENTE COM KALI LINUX

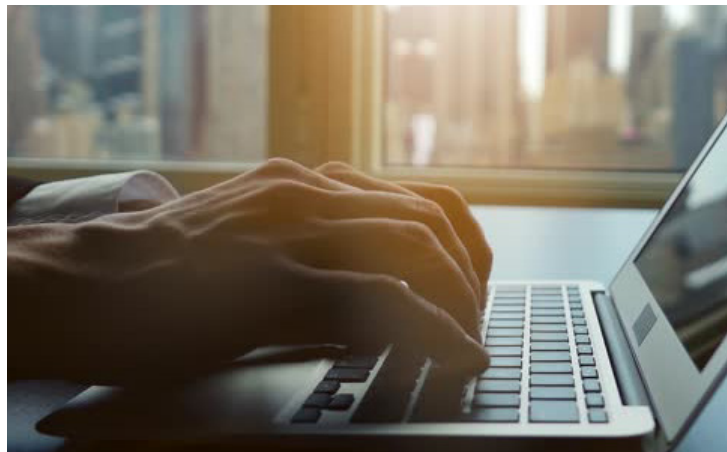
Kali tem algumas especificações mínimas sugeridas para o hardware. Dependendo do uso pretendido. Este guia iremos assumir que o leitor vai instalar Kali como o único sistema operacional no computador.

*"É claro que você também poderá montar uma máquina virtual com o virtualbox para instalar o Kali Linux e rodar ele dentro do seu Windows, Mac ou qualquer outra distribuição Linux, para isso você pode pegar uma cópia do nosso ebook sobre [Virtualbox Nesse Link](#), montar a máquina virtual e voltar ao passo **INSTALAÇÃO DO KALI LINUX** deste guia aqui."*



2.1 VAMOS AOS REQUISITOS PARA A INSTALAÇÃO DO KALI LINUX

- Pelo menos 10GB de espaço em disco, eu sugiro você separar mais.
- Pelo menos 512MB de ram, é interessante tem mais ram especialmente para ambientes gráficos.
- Suporte a inicialização USB ou CD / DVD
- Arquivo ISO do Kali Linux disponível em <https://www.kali.org/downloads/>





COMO CRIAR UM PENDRIVE BOOTÁVEL PARA INSTALAÇÃO DO KALI LINUX





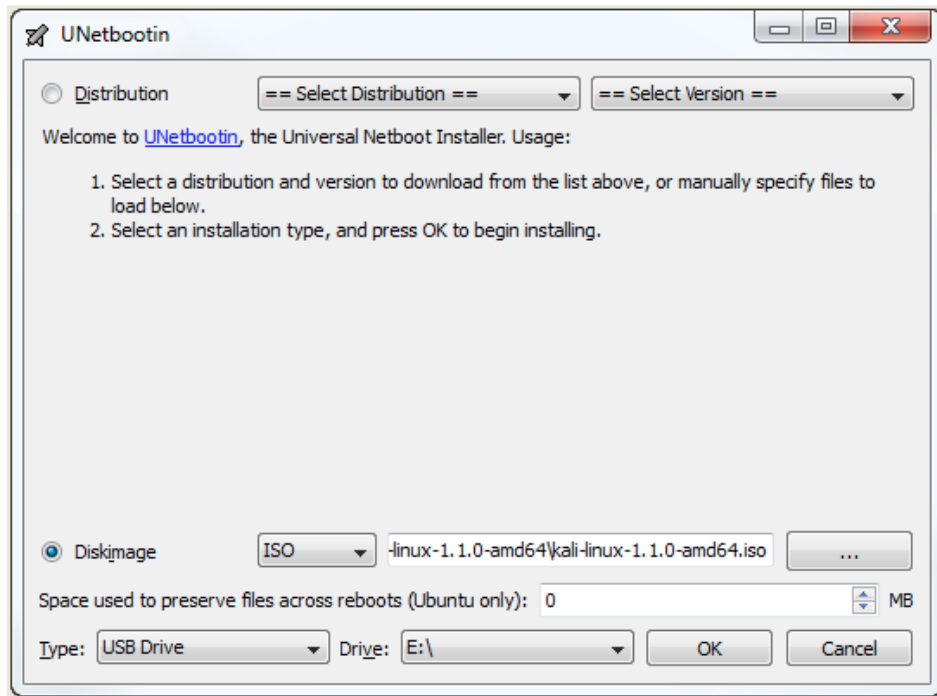
3. COMO CRIAR UM PENDRIVE BOOTÁVEL PARA INSTALAÇÃO DO KALI LINUX

Vamos baixar a ISO do Kali Linux, vamos usar a versão mais recente do Kali com o ambiente gráfico enlightenment, é o mais leve.

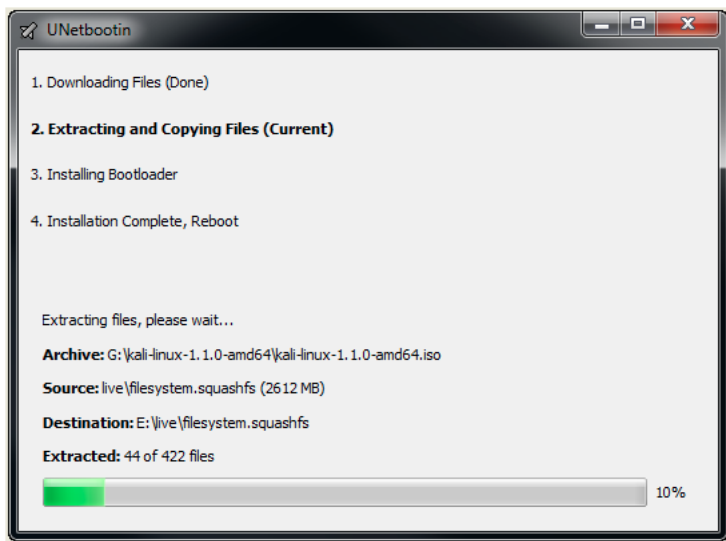
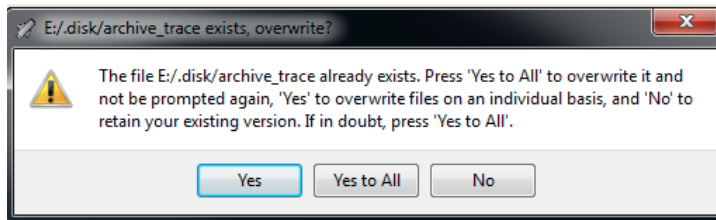
Pode acessar <https://www.kali.org/downloads/> e baixar o arquivo Kali Linux 64 bit e17, salve o arquivo no seu diretório downloads.

3.1 PARA QUEM NÃO UTILIZA LINUX

Caso você não tenha um ambiente já rodando LINUX, utilize o programa UNetbootin para criar o pendrive bootável com o Kali Linux, veja a seguir:



Pode fazer o [Downloads](#) do [UNetbootin](#), criar o pendrive bootável conforme acima, e voltar para o passo **INSTALAÇÃO DO KALI LINUX** deste guia aqui.



3.2) PARA QUEM JÁ UTILIZA LINUX

Vamos assumir que você tem um pendrive na unidade USB, e também é importante dizer que precisamos de um pendrive de 4 / 8GB e que **TODOS OS DADOS SERÃO REMOVIDOS!** Certifique-se de fazer backup de todos os dados antes de prosseguir. Vamos criar esse pendrive bootável com o Kali a partir de outra máquina Linux.

COMO CRIAR O PENDRIVE BOOTÁVEL COM O KALI LINUX

O próximo processo é gravar o arquivo ISO em uma unidade USB para inicializar o instalador. Para fazer isso, podemos usar a ferramenta 'dd', que já está dentro do Linux. Primeiro, vamos localizar com o comando lsblk em qual dispositivo está o nosso pendrive.

Digite o comando abaixo:

lsblk

```
h @1 ~ $ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0 465.8G  0 disk
├─sda1       8:1    0   25G  0 part
├─sda2       8:2    0  81.9G  0 part
├─sda3       8:3    0    1K  0 part
├─sda5       8:5    0 351.3G  0 part
├─sda6       8:6    0   7.6G  0 part
└─sdb        8:16   0 931.5G  0 disk
   └─sdb1     8:17   0 931.5G  0 part
sdc          8:32   1   7.4G  0 disk
├─sdc1       8:33   1   1.6G  0 part
└─sdc2       8:34   1   2.3M  0 part
sr0         11:0    1 1024M  0 rom
```


Pronto, agora já sabemos que o nosso pendrive está no dispositivo `/dev/sdc`, e já podemos gravar a ISO do Kali com a ferramenta `'dd'`.

```
$ sudo dd if=~/.Downloads/kali-linux-e17-2016.2-amd64.iso of=/dev/sdc
```

Importante: O comando acima requer privilégios de root, portanto utilize o `sudo` ou login como o usuário root para executar o comando. Além disso, este comando irá REMOVER TUDO da unidade USB. Certifique-se de fazer backup dos dados necessários.

Ao terminar esse processo, podemos iniciar a instalação do Kali Linux.



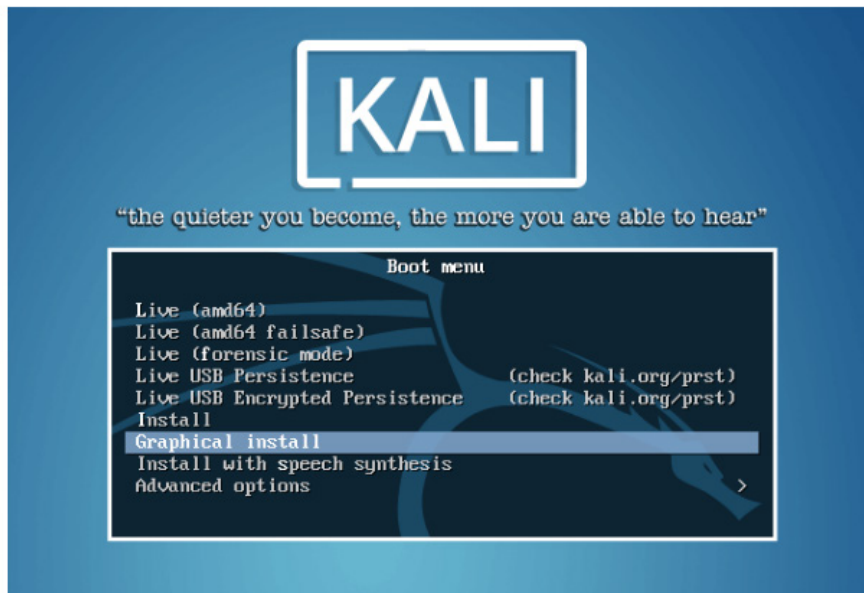
INSTALAÇÃO DO KALI LINUX



4) INSTALAÇÃO DO KALI LINUX

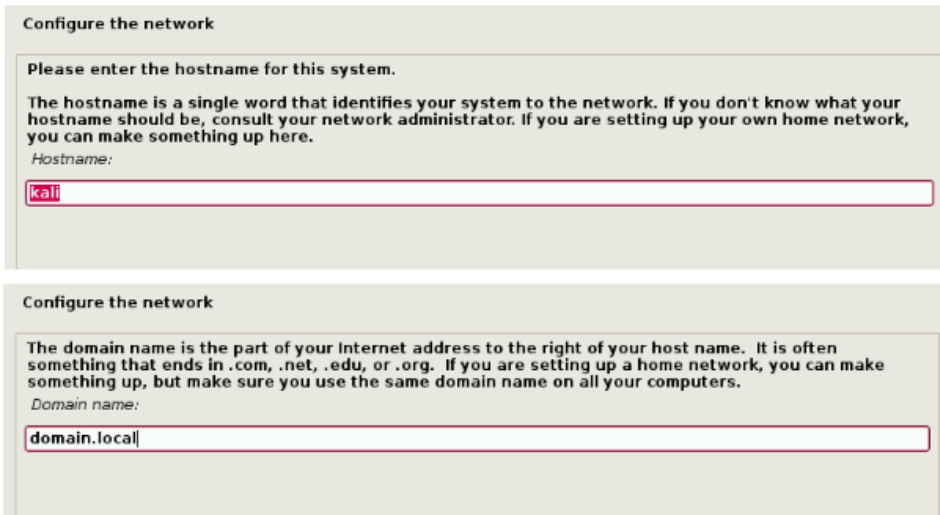
Em primeiro lugar, ligue o pendrive bootável na unidade USB do computador que o Kali deve ser instalado, e faça o boot pela unidade USB.

4.1) Após iniciar com unidade USB, o instalador será apresentado conforme a tela abaixo, você tem a opção “Instalar” ou “Instalação Gráfica”. Este guia usará o método ‘Instalação Gráfica’.



4.2) A próxima tela solicitará ao usuário para selecionar informações de localidade, como idioma, país e layout do teclado.

Uma vez que as informações de localidade sejam exibidas, o instalador solicitará um nome de host e um domínio para esta instalação. Forneça as informações apropriadas para o ambiente e continue instalando. Se tiver dúvidas sobre essas informações, pode utilizar conforme o exemplo abaixo:



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:

kali

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:

domain.local

4.3) Depois de configurar o nome do host e o nome do domínio, a senha do usuário root precisa ser definida. **NÃO ESQUEÇA ESTA SENHA.**

Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

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

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the 'sudo' command.

Note that you will not be able to see the password as you type it.

Root password:

☐ **Show Password in Clear**

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

Re-enter password to verify:

☐ **Show Password in Clear**

4.4) Depois de definir a senha, o instalador solicitará dados de fuso horário e, em seguida, entra no particionamento de disco.

Se o Kali for o único a operar na máquina, a opção mais fácil é usar Guided – Use Entire Disk’ e em seguida, selecionar o dispositivo de armazenamento que você deseja instalar no Kali.

Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk

Guided - use entire disk and set up LVM

Guided - use entire disk and set up encrypted LVM

Manual

Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI1 (0,0,0) (sda) - 21.5 GB ATA VBOX HARDDISK

4.5) A próxima pergunta solicitará ao usuário para determinar o particionamento no dispositivo de armazenamento. A maioria das instalações pode simplesmente colocar todos os dados em uma partição, conforme abaixo.

Partition disks

Selected for partitioning:

SCSI1 (0,0,0) (sda) - ATA VBOX HARDDISK: 21.5 GB

The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

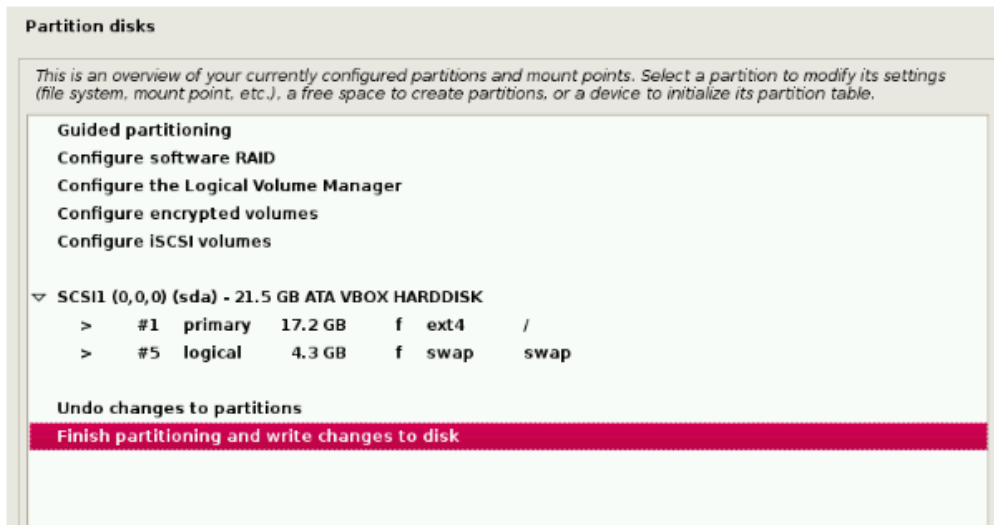
Partitioning scheme:

All files in one partition (recommended for new users)

Separate /home partition

Separate /home, /var, and /tmp partitions

4.6) A etapa final vai pedir ao usuário para confirmar todas as alterações a serem feitas no disco da máquina. Esteja ciente de que continuar irá **APAGAR TODOS OS DADOS DO DISCO**.



4.7) Depois de confirmar as alterações de partição, o instalador irá passar para o processo de instalação dos arquivos. Uma vez concluído, o sistema vai querer configurar um espelho de rede para obter futuras atualizações de software. Certifique-se de ativar essa funcionalidade se desejar usar os repositórios Kali, conforme imagem abaixo.

Configure the package manager

A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

Use a network mirror?

☐ No

☒ Yes

4.8) Depois de selecionar um espelho de rede, o sistema pedirá para instalar o grub. Mais uma vez este guia está assumindo que o Kali é o único sistema operacional neste computador ou que você está instalando em uma máquina virtual do VirtualBox.

Selecionar 'Sim', nesta tela permitirá que o usuário escolha o dispositivo para gravar as informações necessárias do gerenciador de inicialização, utilize a opção conforme imagem abaixo.

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 the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

☐ No

☒ Yes

Install the GRUB boot loader on a hard disk

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB on the master boot record of your first hard drive. If you prefer, you can install GRUB elsewhere on the drive, or to another drive, or even to a floppy.

Device for boot loader installation:

Enter device manually

`/dev/sda (ata-VBOX_HARDDISK_VB30f017a0-5b6c875a)`

4.9) Quando o instalador terminar de instalar o GRUB no disco, ele alertará o usuário para reiniciar a máquina, para em fim o Kali recém instalado entrar em ação.

Finish the installation



Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

OBS.: Como neste guia instalamos o Enlightenment como ambiente de trabalho Kali, ele provavelmente será inicializado por padrão em um shell.

Para iniciar o Enlightenment, inicie sessão como a root, e uma vez logado tudo que precisa fazer para iniciar o Enlightenment é digitar o comando 'startx'.

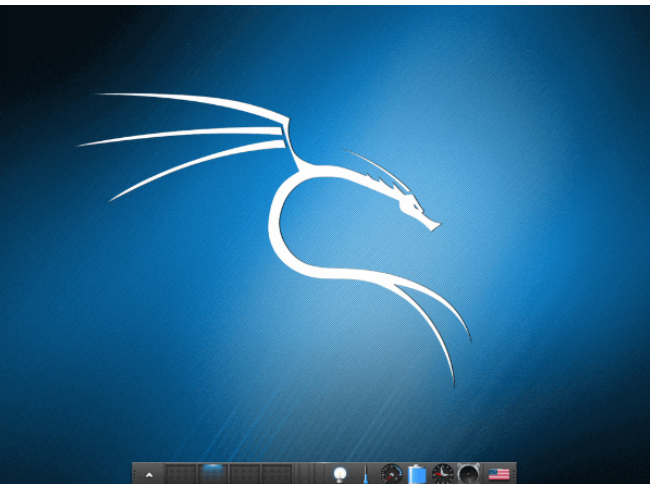
startx

A primeira vez que o Enlightenment for executado, ele pedirá ao usuário algumas preferências de configuração e, em seguida, iniciará o ambiente gráfico.

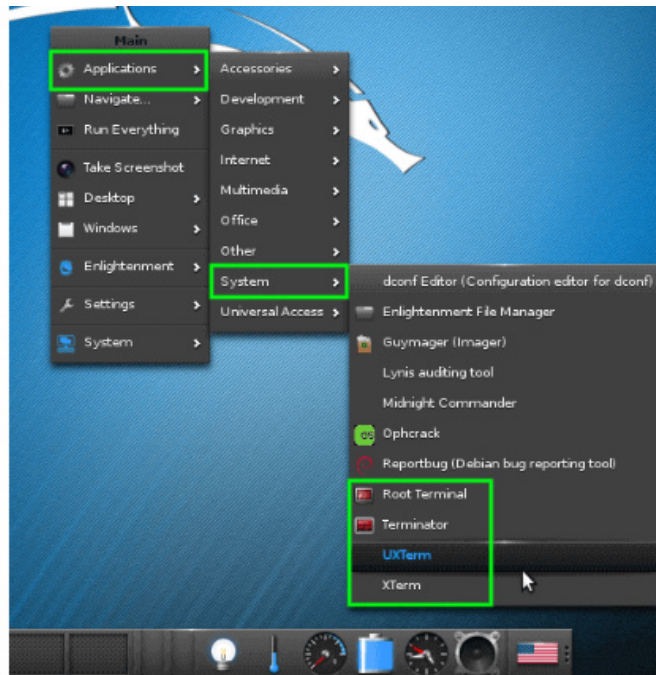
```
Kali GNU/Linux Rolling kali tty1
kali login: root
Password:
Last login: Tue Oct 25 14:47:56 EDT 2016 on tty1
Linux kali 4.6.0-kali1-amd64 #1 SMP Debian 4.6.4-1kali1 (2016-07-21)

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@kali:~# startx_
```



Neste ponto, o Kali está instalado e pronto para ser usado.



```
Nmap done: 256 IP addresses (0 hosts up) scanned in 0.07 seconds
root@kali:~# nmap -sL 192.168.56.0/24
```

```

ap scan report for 192.168.56.100
st is up (0.00029s latency).
1 1000 scanned ports on 192.168.56.100 are filtered
c Address: 08:00:27:98:62:C4 (Oracle VirtualBox virtual NIC)

ap scan report for 192.168.56.102
st is up (0.00025s latency).
c shown: 977 closed ports
RT      STATE SERVICE
1/tcp   open  ftp
2/tcp   open  ssh
3/tcp   open  telnet
4/tcp   open  smtp
5/tcp   open  domain
6/tcp   open  http
7/tcp   open  rpcbind
8/tcp   open  netbios-ssn
9/tcp   open  microsoft-ds
10/tcp  open  exec
11/tcp  open  login
12/tcp  open  shell
13/tcp  open  rmiregistry
14/tcp  open  ingreslock
15/tcp  open  nfs
16/tcp  open  ccproxy-ftp
17/tcp  open  mysql
18/tcp  open  postgresql
19/tcp  open  vnc
20/tcp  open  X11
21/tcp  open  irc
22/tcp  open  ajp13
23/tcp  open  unknown
c Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)

```

CONCLUSÃO

Desenvolvido pela Offensive Security, na verdade foi feita uma reescrita do BackTrack.

Dos melhores sistemas operacionais para hackers, com toda certeza é o mais famoso de todos.

O Kali Linux é um sistema operacional baseado em Debian, vem com mais de 600 ferramentas de testes pré-instaladas, ele é literalmente uma caixa de ferramentas para quem trabalha com segurança da informação.

Estas ferramentas versáteis são atualizadas regularmente e estão disponíveis para diferentes plataformas como ARM e VMware.

Para um trabalho forense, este sistema operacional de hacking vem com uma capacidade de iniciar via LIVE, é sim um ambiente perfeito para a detecção de vulnerabilidades.



E-TINET é um projeto pessoal de Pedro Delfino, profissional com mais de 14 anos de experiência em sistemas Linux. A E-TINET tem como objetivo treinar e capacitar os profissionais de tecnologia a trabalharem com o Linux profissionalmente.

[Veja aqui](#) como começar uma formação Linux profissional e domine, de uma vez por todas, esse sistema tão importante para a sua carreira.