
Linux Essentials 010-160 + Bônus

Este curso é uma atualização da conhecida certificação do [Linux Essentials 010-160](#) mais **LPI 101 (LPIC-1)** com ênfase em **segurança da informação e preparação para OSCP**.



Este curso é supervisionado pelo Linux Professional Institute (LPI) e dá descontos ao aluno para o exame LPIC considerado internacionalmente!

Este curso é adequado para adolescentes e iniciantes no mundo do Linux, o Linux é um sistema operacional necessário no gerenciamento de redes e segurança da informação e no mundo cibernético.

Neste curso, trabalharemos com os sistemas operacionais Kali Linux e Ubuntu.

Aula - 1 - Instalação do sistema operacional e operação básica

Linux é um ótimo exemplo de código aberto e, ao contrário do Windows, é um sistema operacional gratuito. O Linux é um sistema multiusuário que permite que muitos usuários trabalhem no mesmo sistema operacional de maneira conveniente e eficiente; esse sistema operacional é muito fácil de trabalhar com os comandos de interface gráfica e de interface da CLI (Comandos de texto).

Existem muitas versões do sistema operacional Linux que podem ser adaptadas a qualquer tipo de necessidade ou hardware e é por isso que muitas máquinas escolheram esse sistema operacional (Embedded Systems).

Linus Torvalds Richard Matthew Stallman

Em 1991, durante seus estudos, Torvalds tentou encontrar um jeito de trabalhar com o sistema Unix também de casa, em seu computador pessoal. A única opção naquele momento era o Minix que não era vendido sob uma licença gratuita, Torvalds decidiu criar sua própria versão.

A reescrita do Minix gradualmente se tornou um projeto em si que não era mais especificamente associado ao Minix, Torvalds desenvolveu o núcleo e, quando sentiu que tinha código suficiente, voltou-se para o fórum do Minix e o anunciou. Pouco tempo depois, o Linux estava disponível para qualquer pessoa que exigisse um diretório privado no servidor FTP atribuído a ele.

É importante notar que o Torvalds continua sendo o principal mantenedor do núcleo do Linux até hoje.

Paralelamente ao Linus, Richard Matthew Stallman é um programador americano judeu. Em 1983, ele iniciou o projeto GNU para criar um sistema operacional livre, semelhante ao Unix, e desde então serviu como seu principal arquiteto. Os princípios conceituais de Stallman, quando ele fundou o GNU, formam a base de um movimento social chamado movimento de Open Source(código aberto).

Open Source - Código aberto

Produto ou software que permite que qualquer pessoa que queira visualizar o código fonte do software, faça o download do código fonte e o examine.

No mundo da segurança da informação. Utilizamos o código fonte da empresa para detectar e relatar falhas de segurança no código.

No mundo do código aberto, às vezes é até possível alterar o código da fonte do software e adaptá-lo às necessidades pessoais do programador, hoje a maior plataforma de código aberto é o GitHub no qual pode-se encontrar código fonte para vários projetos em todos os mundos da programação em geral e também no mundo de segurança cibernética.

Exemplo de software de código aberto:

- Httpd & Apache - <https://github.com/apache/httpd>
- WordPress - <https://github.com/WordPress/WordPress>
- MySQL e MariaDB - <https://github.com/mysql/mysql-server>

O objetivo do módulo de código aberto é liberar o código fonte do software livre para todos. Mas ao mesmo tempo:

- Prover suporte ao código.
- Solicitação de recurso ou alteração de código.
- Curso ou certificação do software.

É importante observar que, de acordo com o módulo de código aberto, por um lado, o código é legível e visível para todos, por outro lado, nem todo software de código aberto contém a mesma licença e permite que você faça alterações no código e redistribua o software modificado.

Tipos de licenças de código aberto:

- **Copyright** - É a proteção concedida ao criador ou proprietário de uma obra contra o uso não autorizado de uma obra que é de propriedade intelectual. [Saiba mais](#)
- **Copyleft** - Conteúdo gratuito é um nome geral para conteúdo (escrita, software, imagem, som etc.) que nenhum organismo possui controle completo sobre sua distribuição e uso. O nome é aceito como um nome de movimento social que busca incentivar o uso de conteúdo gratuito.

Ao usar o software livre, os usuários têm a liberdade de:

- Usar o conteúdo e se beneficiar do mesmo
- Estudo do conteúdo e aplicar o que aprendeu
- Criar e distribuir cópias do software
- Modificar e/ou melhorar o conteúdo e distribuir trabalhos derivados dele

[para obter mais informações](#)

- **GNU General Public License (GPLv3)** - é uma licença **copyleft** no qual seus derivados terão as mesmas condições de licença. Esta licença Concede direitos de software livre para garantir que a liberdade seja preservada, mesmo que o trabalho tenha sido alterado ou atualizado. **(O código fonte do software deve estar acessível a todos e não pode ser patenteado)**
- **Licença Apache** - Uma licença compilada pela empresa apache, todo o software distribuído por esta instituição ou por um de seus projetos, é registrada sob esta licença. Observe que esta licença não é **copyleft** e permite o uso e a distribuição do código fonte em software de código aberto e fechado. **(Qualquer pessoa pode pegar o código e construir com ele um software de código fechado e vendê-lo, mas não pode patentear o código ou a idéia.)**
- **Licença MIT** - Uma licença do MIT Institute of Technology, é uma licença gratuita licenciada e também permite a reutilização de software proprietário, desde que a cópia da licença esteja anexada às cópias do software. Esta licença também permite a conversão em licença GPL e distribuição de software. **(Qualquer pessoa pode pegar o código e construir com ele um software de código fechado e vendê-lo, essa licença significa pode fazer o que você deseja com o código).**
- **Unlicensed (não licenciado)** -Um software não licenciado é perigoso porque é impossível saber quem escreveu o software e pode danificar seu computador.

Para colocar ordem nas coisas, eis um excelente site que explica detalhadamente todas as licenças, [clique aqui](#).

Diferentes tipos de sistemas Linux

Neste curso, trabalharemos com o sistema operacional Ubuntu e com o Kali Linux, que na verdade é (Debian), mas modificado com várias ferramentas de hacking convenientes.

No mundo Linux, existem várias opções de sistemas operacionais, por exemplo:

- **Servidor** - Sistema operacional sem interface gráfica e todo o trabalho com o sistema operacional é realizado apenas por comandos.
- **Desktop** - Um sistema operacional gráfico semelhante ao sistema operacional Windows que pode ser operado sem o uso de nenhum comando.
- **Embedded System (Sistema incorporado)** - Sistema operacional para criação de amostra de hardware personalizado Raspberry Pi/Arduino. É comum usar esse sistema operacional ao desenvolver um produto inteligente, por exemplo, uma câmera IP.

Distribuições Linux

No mundo Linux, existem inúmeras distribuições diferentes que atendem a diferentes necessidades, [abaixo está a lista de distribuições no mundo Linux.](#)

As distribuições líderes e reconhecidas são:

- Debian, Ubuntu (LTS), Kali Linux
- Gentoo
- Red Hat, CentOS, Fedora
- Raspberry Pi, Raspbian
- Android

Outro termo para se familiarizar antes de começar a aprender Linux é **Distribution Life Cycle (Ciclo de Vida da Distribuição)**, para qualquer distribuição, você pode baixar várias versões:

- **Release** - A versão estável do software para o usuário comum.
- **Pre-Release**
 - **Alpha** - Uma nova versão cheia de bugs para desenvolvedores que desejam atualizar seu software antes do lançamento.
 - **Beta** - uma versão mais estável do Alpha Quando a maioria dos erros foi corrigida, neste momento o desenvolvedor deve verificar o código que ele escreveu no Alpha antes de ser lançado com o **Release**.
- **Rolling Release Schedule (Programação de lançamento sem interrupção)** - Atualizações atuais que chegam ao sistema operacional, geralmente são atualizações de segurança e de correção de bugs.
- **Support Versions (Versões de suporte)**
 - Short-term (Curto prazo) - Intermediário
 - Long-term -LTS (Longo prazo) - Muito estável por um longo período
 - End of life (Fim da vida) - Sem suporte

Comparação de diferentes sistemas operacionais:

- **Windows**
 - 90% of home users
 - Widely-available and widely-supported
 - Most prone to malware
 - Requires a license
 - GUI-based
- **Mac OSX**
 - 7% of home users
 - Free but only works on Apple systems
 - GUI-based
- **Linux**
 - Less than 2% of home users
 - More than 75% of enterprise server environments
 - Known as the OS for computer experts and hackers
 - Source code is available for modification
 - Open source
 - Can run from the command line only

Instalação do sistema operacional Linux:

Você pode escolher uma das três opções de instalação:

- **Oracle VirtualBox e Virtualization** - Instalar o sistema operacional em um ambiente virtual, e não o sistema operacional central, é o método mais fácil e conveniente. Portanto, neste curso, optamos por instalar o sistema operacional em um ambiente virtual.
- **LiveCD** - Esse método permite que o Linux seja executado sem instalá-lo diretamente de uma unidade de disco.
- **Instalação completa** - Instalação completa do sistema operacional no disco rígido do seu computador.

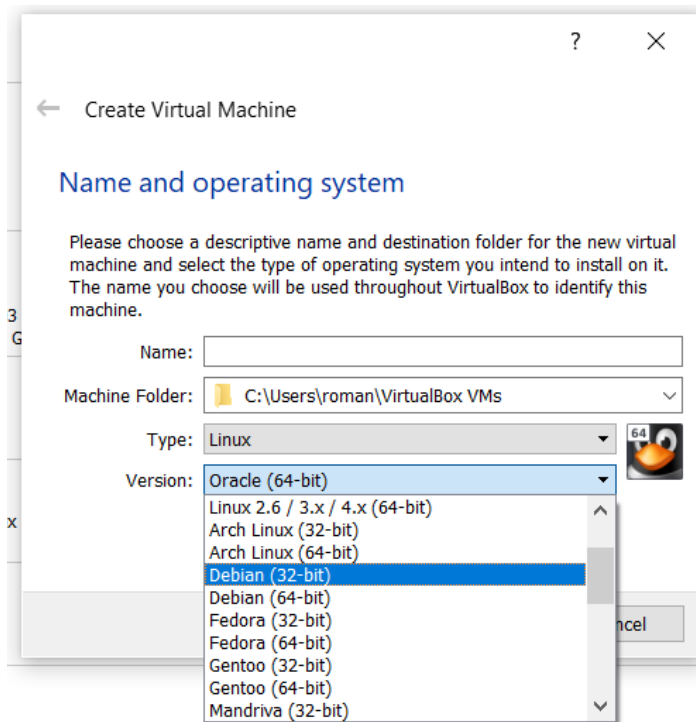
No curso, trabalharemos com o **Ubuntu** e o **Kali Linux**, baixamos as 2 máquinas nos seguintes sites:

- [Ubuntu](#)
- [Kali](#)

Instalaremos as máquinas usando o software da máquina virtual - Oracle Virtual Box, que pode ser baixado [aqui](#).

Observe que a virtualização deve estar ativada no BIOS do seu computador, de acordo com o modelo do seu computador; portanto, neste curso, trabalharemos no modo mais amplo e instalaremos apenas máquinas de 32 bits.

Se o software permitir que você instale máquinas de 64 bits, tudo ficará bem se você vir apenas as opções de 32 bits, saberá que a virtualização deve ser aberta no BIOS.



Após a instalação, observe que você deve trabalhar no usuário root com uma das duas opções a seguir:

1. Execute o comando **sudo su**
2. Execute o comando **sudo** antes de cada comando que exige permissões de exemplo:

```
sudo apt install vim
```

Se você tiver um problema de cor, conforme mostrado no vídeo, O comando:

```
alias ls = "ls --color = auto"
```

[Softwares comuns e trabalhando com o Sistema operacional.](#)

No mundo Linux, você pode escolher quais configurações de tela escolher. Existem vários tipos de

- **Unity**
- **KDE**
- **Gnome**
- **Cinnamon**
- **Xface**
- **LXQt**
- [para a lista completa de](#)



softwares comuns que devem ser familiares ao usuário comum:

- **Librawriter** - este software substitui o Office Word.
- **Libracalc** - este software substitui o Office Excel.
- **Libraoffice express** - Este software substitui o Office PowerPoint.
- **Vlc** - Player de filme.
- **Gimp** - software que substitui o Photoshop.
- **Kdenlive** - software que substitui o Windows Movie Maker.
- **Audacity** - Software de gravação de som.
- **Firefox** - o navegador recomendado no mundo Linux.

Software de gerenciamento de rede:

- **Wireshark** - Monitoramento de rede
- **Gparted** Software para trabalhar com o disco rígido da máquina.
- **Timeshift** - Excelente software de backup, como restauração do sistema no Windows.
- **Atom** - este é o notepad++ do Linux
- **gedit** - outra versão de um estilo mais conveniente e simples do estilo de bloco de notas.
- **Putty** - Nosso software de gerenciamento de servidores.

Linguagens de programação geral e seu uso:

- **PHP** - Linguagem do lado do servidor no mundo da web.
- **JavaScript** - Linguagem de desenvolvimento do lado do cliente no mundo da Internet
- **Python** - a linguagem de script recomendada nas áreas de segurança da informação e alta tecnologia.
- **Bash** - A linguagem de programação no mundo Linux.
- **Java** - uma linguagem útil de desenvolvimento de software com um mecanismo gráfico que funcionará em todos os tipos de sistemas operacionais.
- **C** - Um dos primeiros idiomas para o desenvolvimento de software de alto desempenho.

Gerenciamento e instalação de pacotes

No Linux não é comum baixar softwares dos sites das empresas como no Windows, no linux existe um gerenciador de pacotes.

A loja de aplicativos Ubuntu OS é chamada - Ubuntu Software Store.

- É importante observar que as instalações têm dependências no Linux; portanto, o gerenciador de pacotes instala tudo para nós, para que não seja necessário fazer o download de dez softwares diferentes para que o que você quer instalar funcione.
- Assim como um aplicativo Android tem uma extensão, **.apk** o software Linux tem uma extensão **.deb** ou **.rpm**
 - **.deb** - indica uma distribuição do tipo debian.
 - **.rpm** - Marca de distribuição do red Hat material LPI101.
 - **.tgz** - apenas um formato linux universal, é um formato compactado como zip.
- O processo de instalação é realizado da seguinte maneira:
 - Executar instalação do comando

- O comando procura todas as dependências e as instala
- O comando instala o software necessário
- Um dos benefícios mais significativos do Linux na instalação de software é poder atualizar o sistema geral, sem a necessidade de atualizar cada software individualmente. **Todos eles podem ser atualizados com apenas um comando.**

Comando apt-get

Comandos possíveis para o **apt-get** ou **apt**:

- **dist-upgrade** - Atualiza pacotes para os quais novos pacotes precisam ser atualizados, o que atualiza o sistema operacional.
- **upgrade** - atualiza todos os pacotes instalados
- **install** - instalar um pacote, você também pode instalar uma versão específica para qualquer pacote por exemplo **vsftpd=2.3**
- **remove** - apenas exclui pacote sem tocar nos arquivos de configuração e suas dependências
- **purge** - exclui o pacote e suas configurações
- **autoremove** - também exclui as dependências, este comando sem especificar o pacote exclui todos as dependências e pacotes defeituosos.
- **update** - atualiza os repositórios
- **download** - Efetua download porém não instala o pacote
- **check** - sem especificar o pacote verifica se há pacotes que não tem dependentes e não funcionará
- **build-dep** instala todas as dependências novamente para alguns pacotes

Exemplo:

```
apt update
apt install ssh
apt autoremove --purge ssh
```

Outros parametros:

--download-only source

```
apt --download-only source ssh
```

Exercício

Baixe o seguinte software para sua máquina Ubuntu:

1. git
2. nmap
3. ssh



Repositórios

O software que instalamos a partir dos repositórios, que está no seguinte arquivo:

```
/etc/apt/sources.list
```

deb - Pacotes configurados para uso

deb-src - o código fonte dos pacotes para desenvolvedores, se necessário.

No mundo do, **red-hat** o comando apt é substituído pelo comando **yum**.