

## Configurando o ambiente

### Transcrição

O que acontece quando acessamos um site na Internet?

Primeiro abrimos o browser, na barra de endereço digitamos o site desejado. Por exemplo, o site do [www.itau.com.br](http://www.itau.com.br). Ao fazer isso a página desejada será carregada. Esse site está armazenado em alguma região do mundo. Ao mesmo tempo que realizamos essa ação, existem outras pessoas no mundo fazendo o mesmo procedimento, simultaneamente.

Nosso objetivo é aprender sobre segurança, entretanto, não podemos fazer testes de vulnerabilidade com sites reais da Internet, pois esse é um procedimento ilegal. Será preciso criar um cenário controlado por nós para que possamos realizar testes e exercícios desejados. Resumindo, teremos três elementos: Rafael, a vítima João, o hacker e o servidor web.

Como estamos utilizando apenas um computador, será preciso criar um ambiente virtual. Ou seja, instalar em uma mesma máquina um ambiente de servidor e outro de hacker. Existem várias maneiras de recriar um ambiente, por motivos didáticos optaremos pela máquina virtual.

Para construir esse ambiente utilizaremos o programa chamado **Virtual Box** que pode ser acessado clicando [aqui](https://www.virtualbox.org/wiki/Downloads) (<https://www.virtualbox.org/wiki/Downloads>). Na primeira página já visualizamos as versões disponíveis para os diferentes sistemas:

The screenshot shows the 'Downloads' page of the VirtualBox website. The page has a blue header with the 'VirtualBox' logo and navigation links like 'About', 'Screenshots', 'Downloads', 'Documentation', 'End-user docs', 'Technical docs', 'Contribute', and 'Community'. The main content area is titled 'Download VirtualBox' and contains information about where to find binaries and source code. It lists three main download categories: 1. 'VirtualBox 5.1.10 platform packages' for Windows, OS X, Linux, and Solaris hosts. 2. 'VirtualBox 5.1.10 Oracle VM VirtualBox Extension Pack' for all supported platforms, including details about USB support and licensing. 3. 'VirtualBox 5.1.10 Software Developer Kit (SDK)' for all platforms. There are also links to a changelog and instructions on how to verify the integrity of downloaded packages using SHA256 and MD5 checksums. A note at the bottom recommends upgrading guest additions after upgrading VirtualBox.

Selecione o pacote desejado e quando este estiver finalizado, basta clicar no arquivo baixado e seguir os passos da instalação. Clicaremos no botão *finish* assim que o programa for instalado, e o **Virtual Box** será rodado.

Com o **Box Virtual** aberto é preciso importar as máquinas virtuais: a do hacker (*Kali Linux*) e a do servidor web que conterà os site vulneráveis.

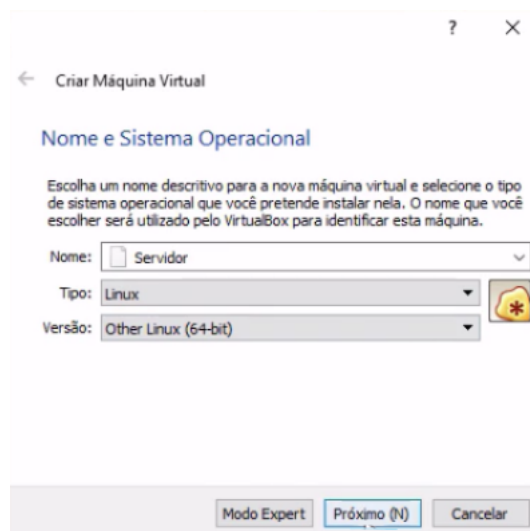
Para criar o ambiente do Kali Linux vamos em "Arquivo > Importar Appliance" e abrirá uma janela. Nela, nós importamos o arquivo para montagem da máquina virtual que está disponível [aqui](https://cursos.alura.com.br/course/seguranca-web-vulnerabilidades-do-seu-sistema/task/22162) (<https://cursos.alura.com.br/course/seguranca-web-vulnerabilidades-do-seu-sistema/task/22162>).

Basta selecionar o arquivo e clicar em "Importar". Esperando alguns segundos teremos o Kali Linux no *Virtual Box*.

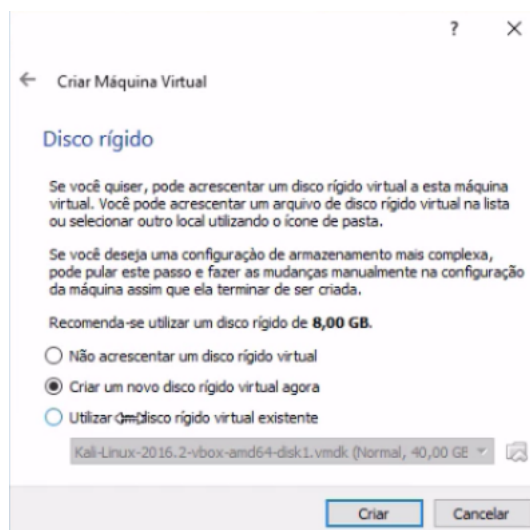
Falta trazer a máquina virtual do servidor, clicamos no ícone "Novo" localizado a esquerda no Menu:



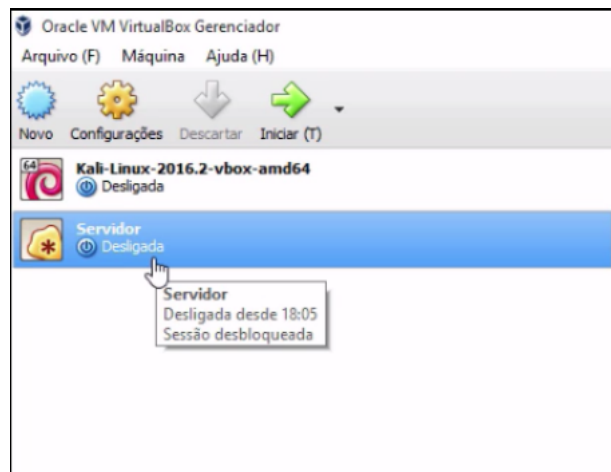
Abrirá uma nova janela pedindo para completar algumas informações. O "Nome", nós preenchemos apenas como "Servidor", o "Tipo" como *Linux* e a versão será "Other Linux (64-bit)":



Ao clicar em "Próximo" teremos uma segunda janela, a "Tamanho de Memória" que nós deixaremos como 512. A terceira janela é "Disco rígido" e nele selecionamos a opção "utilizar Disco Rígido virtual existente". Clicamos no ícone da pasta e selecionamos o arquivo referente ao servidor web e clicamos no botão "Criar":

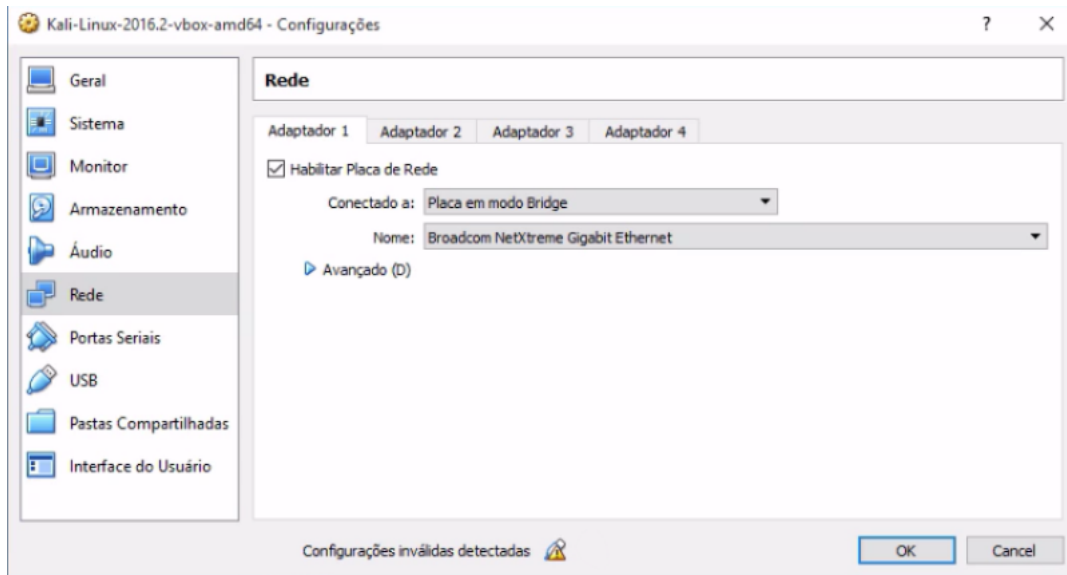


Seguindo esses passos, nós já teremos os ambientes virtuais do hacker e do servidor:

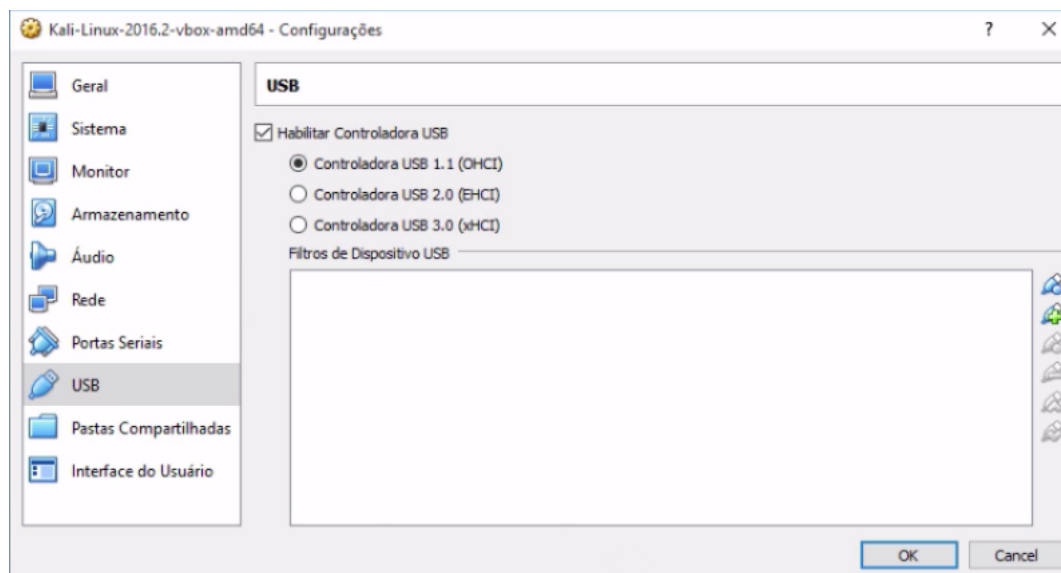


Antes de começar os testes fazemos uma extensão da rede para as máquinas, de maneira que contemple tanto o servidor quanto o *Kali Linux*. Nós selecionamos a máquina do *Kali Linux* e clicamos no botão "Configurações" que encontra-se no Menu superior.

Abre-se uma janela e nela nós selecionamos a aba **Rede**. No campo "Conectado a", nós vamos inserir "Placa em Modo Bridge". Essa opção faz uma ponte no computador para estender o *Kali Linux*.



Note que ao preencher essa janela aparece escrito em baixo o aviso: "configurações inválidas detectadas". Esse aviso aparece pois importamos a máquina virtual com as configurações do fabricante, ou seja, é preciso fazer ainda alguns ajustes referentes a porta USB. Selecionando a aba "USB" marcamos a primeira opção, "Controladora USB 1.1". Ao fazer isso, note que a mensagem desaparece automaticamente:



Agora, podemos dar um "Ok"!

Realizamos o mesmo procedimento para o Servidor-web. Vamos em "Configurações > Rede" e selecionamos a opção "Placa em Modo Bridge".

O que fizemos nessa aula foi preparar o ambiente. Conseguimos aprontar o **Kali Linux** que representa o hacker e o *Servidor web* que conterà os sites vulneráveis.