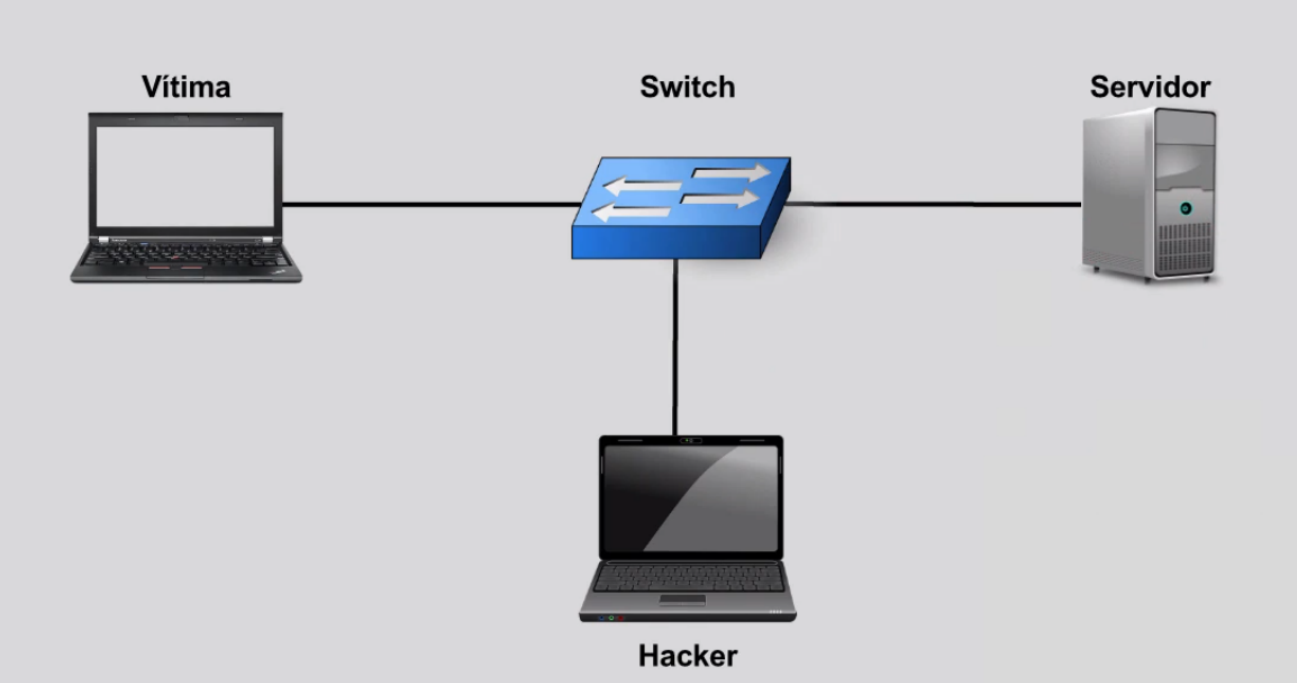
07

Switch Kali Linux

Transcrição

Já vimos que o hub apresenta limitações por não reconhecer qual máquina está em cada porta. Ele passa as informações para todas, e o hacker que estiver à espreita faz análise de protocolos e consegue colher dados, como e-mail e senha de sua vítima.

Com o objetivo de melhorar essa performance dos hubs, surgiram outros equipamentos. O que veio com o objetivo de substituir os hubs é o switch. A grande diferença entre eles é que o switch consegue detectar qual máquina está conectada a cada porta.



Ele detecta que a sua direita está o usuário, e que à sua esquerda está o servidor. E também percebe o computador do hacker, representado abaixo. Mas como ele consegue fazer essa distinção? Por meio do endereço físico de cada placa de rede, o endereço mac.

Toda placa de rede, ao sair do fabricante, possui um número de série, que a identifica; esse é o endereço mac. Abrindo o Prompt de Comando do Windows, podemos acessar esse endereço. Basta digitar o seguinte:

```
C:\Users\Alura>ipconfig/all
```

Dentre as muitas especificações que veremos, temos as da placa de rede:

```
Configuração de IP do Windows
    ...

Adaptador Ethernet Ethernet:

    Sufixo DNS específico de conexão......:
    Descrição.............................: Realtek PCIe GBE Family Controller
```

```
Endereço Físico: D8-CB-8A-C1-AA-7F
...
```

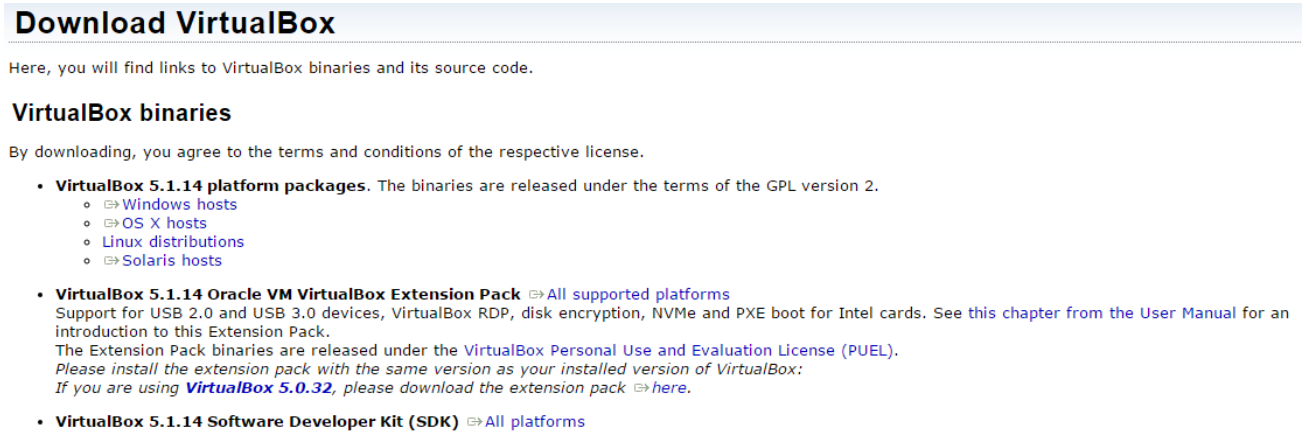
Quando um usuário faz o acesso passando pelo switch, este gravará o endereço mac na sua memória. Assim, saberá para quem precisa passar a informação. Não será necessário passar a informação para todas as portas (e usuários) como era feito com o hub.

Isso dificulta muito a vida de um hacker. O switch não passa a informação para ele tão facilmente - como seria feito pelo hub. Mas sabemos que hackers não desistem muito facilmente. Eles querem saber as informações que são passadas para outros usuários. Assim, ele encontrará uma forma de comprometer esse switch.

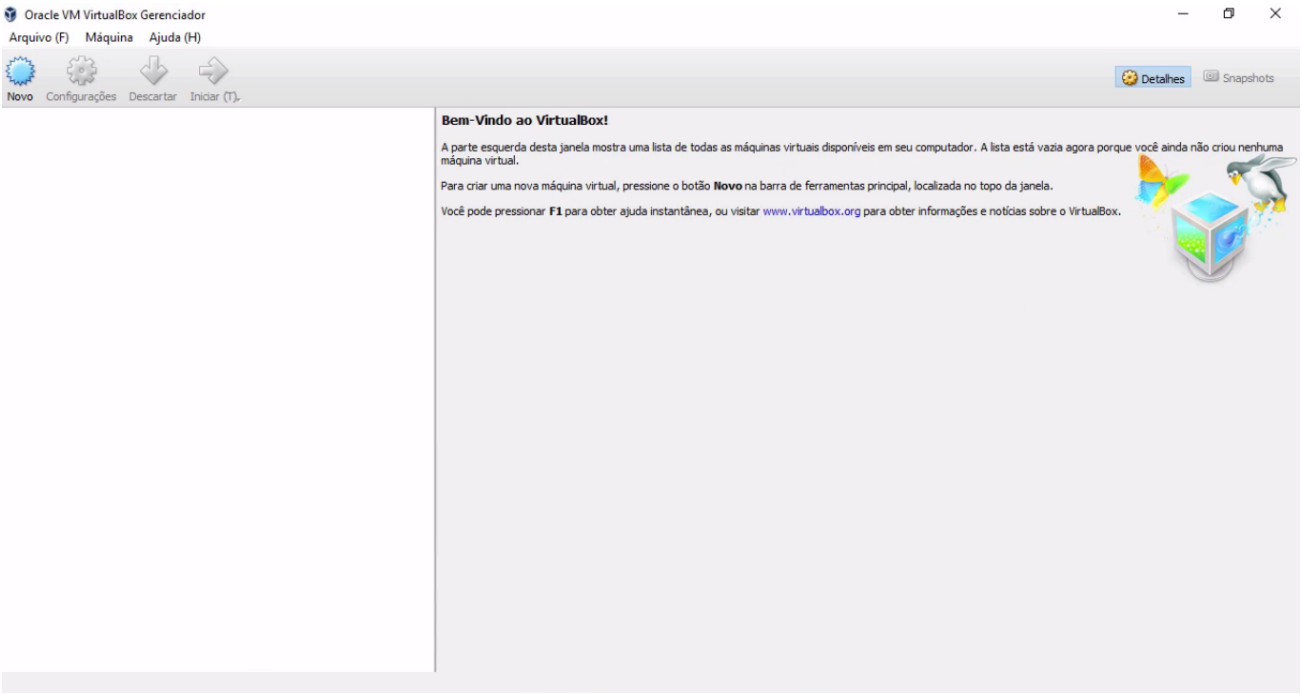
Para isso, o hacker usará um programa projetado para testes de penetração de redes, que é o Kali Linux. Mas, como eu estou usando apenas uma máquina, antes de instalar o Kali Linux, preciso colocar um ambiente virtualizado na minha máquina e fazer a simulação da plataforma que o hacker usaria. E é isso que faremos agora.

A primeira etapa será fazer o download no site do Virtual Box (https://www.virtualbox.org/).

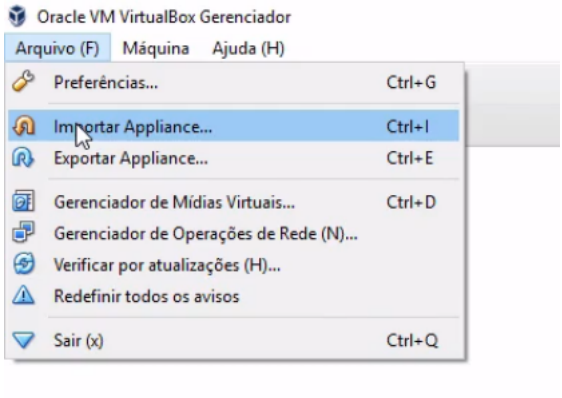
Ao clicar em `Download`, seremos redirecionados para uma página que nos permite escolher que sistema operacional estamos utilizando.



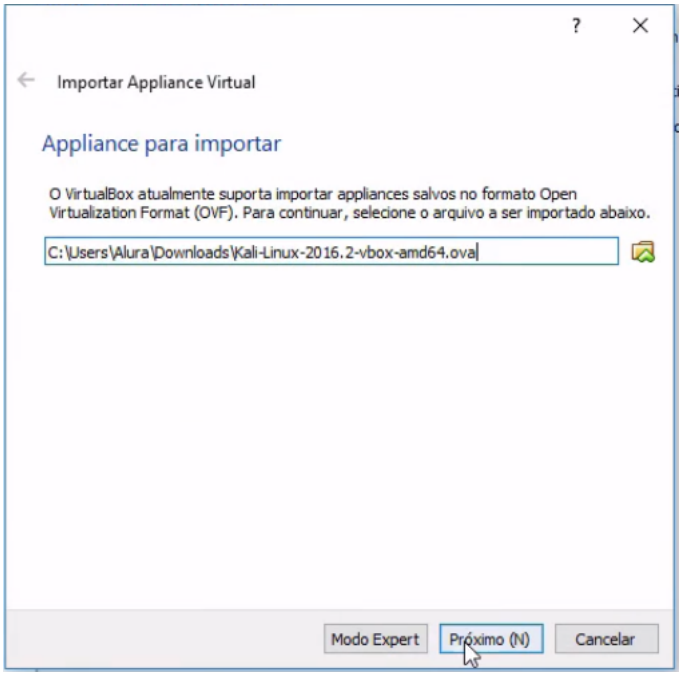
Basta escolher o seu e o download se iniciará automaticamente. Depois, é preciso executar o *installer*. A instalação não tem segredo: basta seguir como a anterior. Quando ela terminar, pode-se abrir o programa, que é assim:



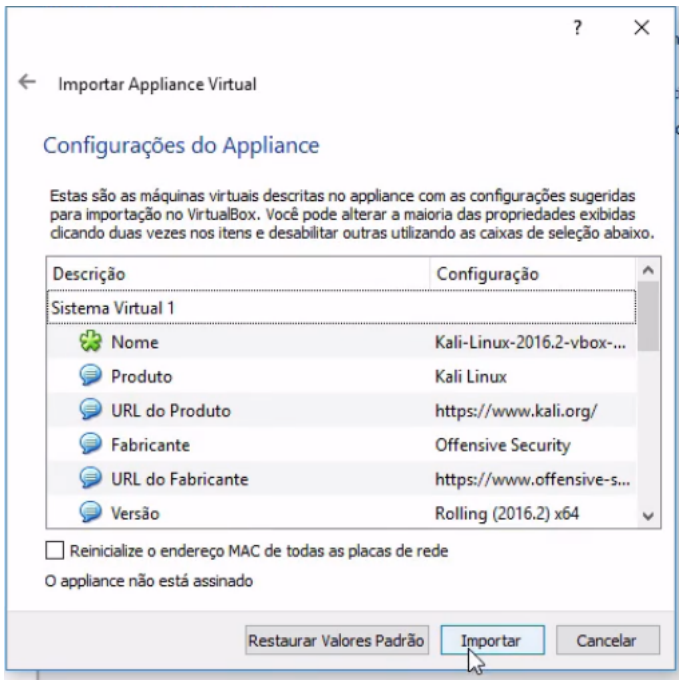
Agora podemos trazer a plataforma do hacker para ser gerenciada pelo Virtual Box. Para isso, clicaremos em `Arquivo > Importar Appliance .`



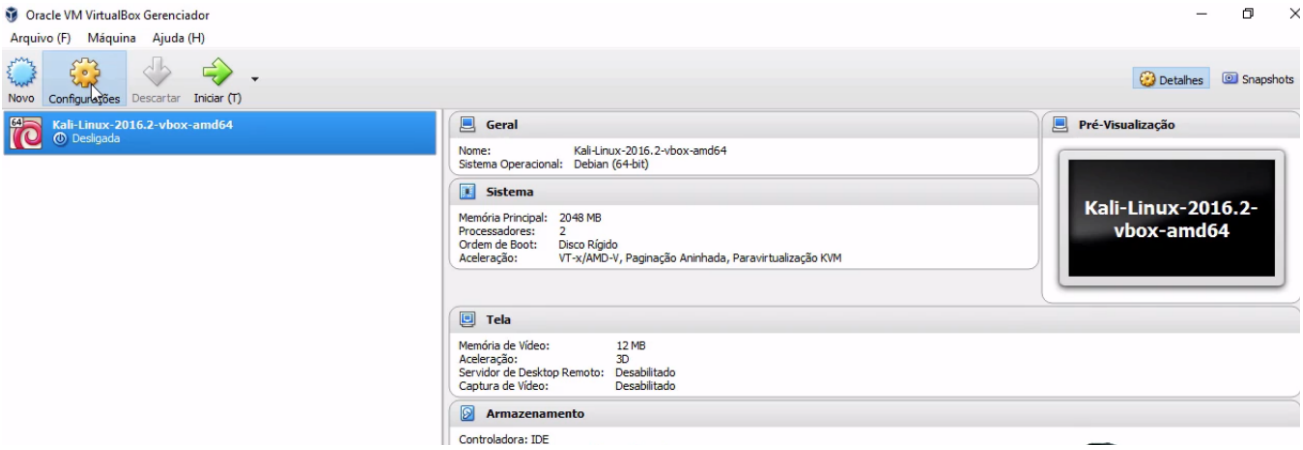
A máquina do hacker está disponível para download. Como já a tenho no meu computador vou selecioná-la dentre os meus arquivos.



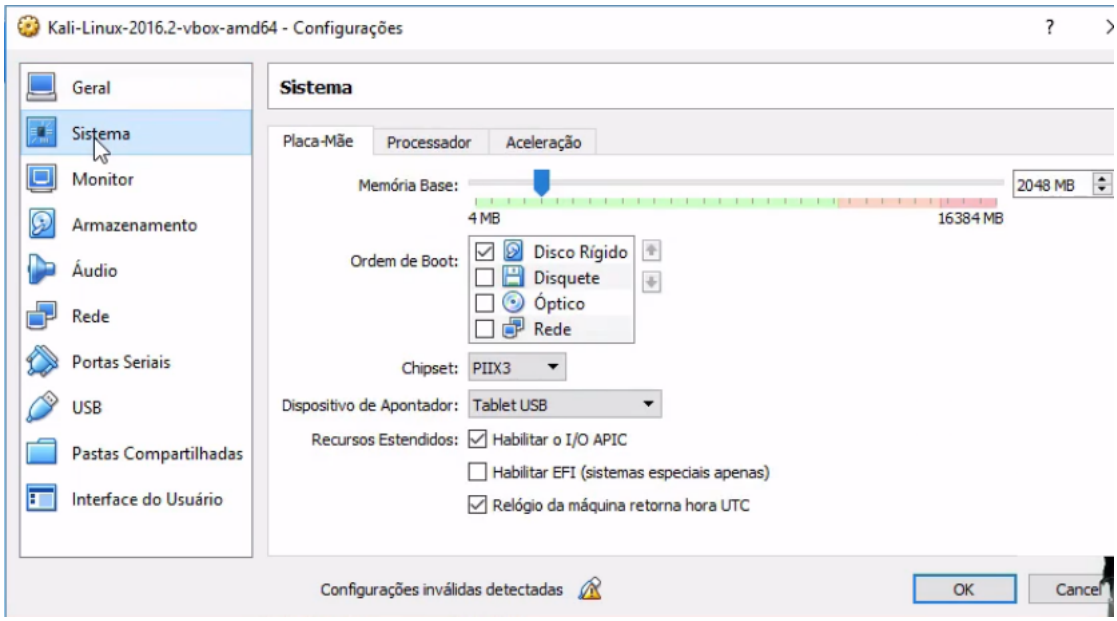
Basta clicar em `Próximo (N)`, e depois em `Importar`.



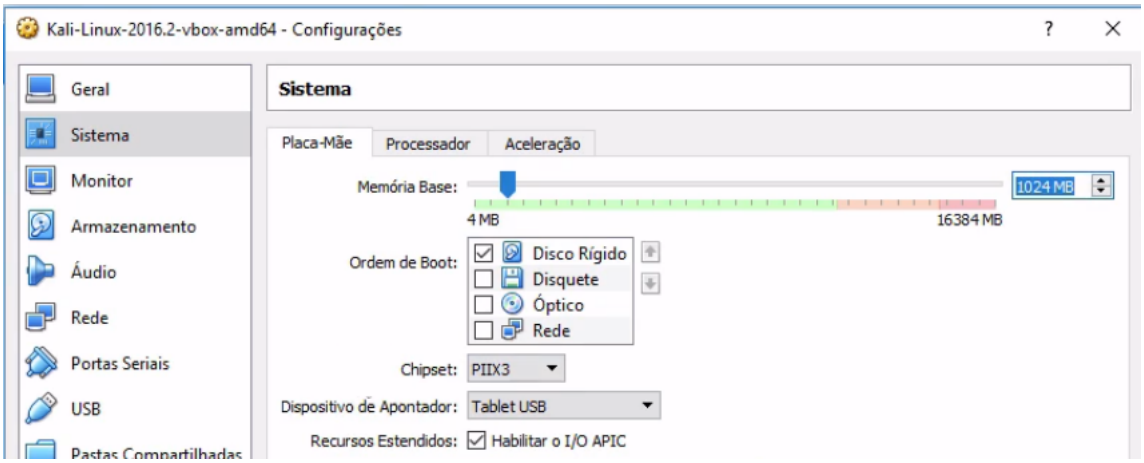
Assim que a importação terminar, podemos definir as configurações. É só clicar no ícone da máquina do hacker e a seguir em `Configurações`.



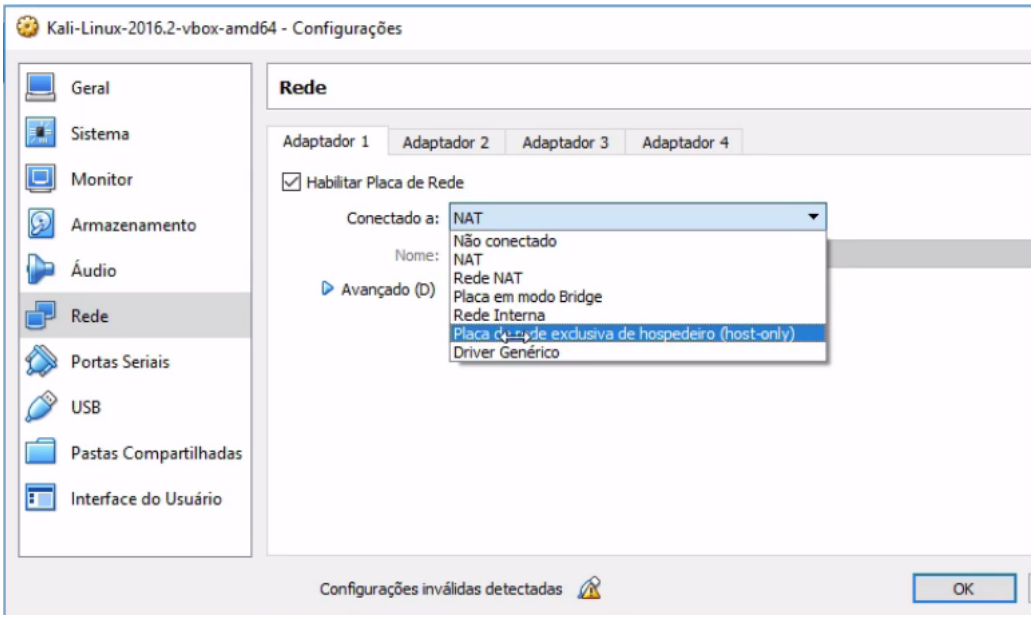
Faremos algumas alterações no painel que se abrirá.



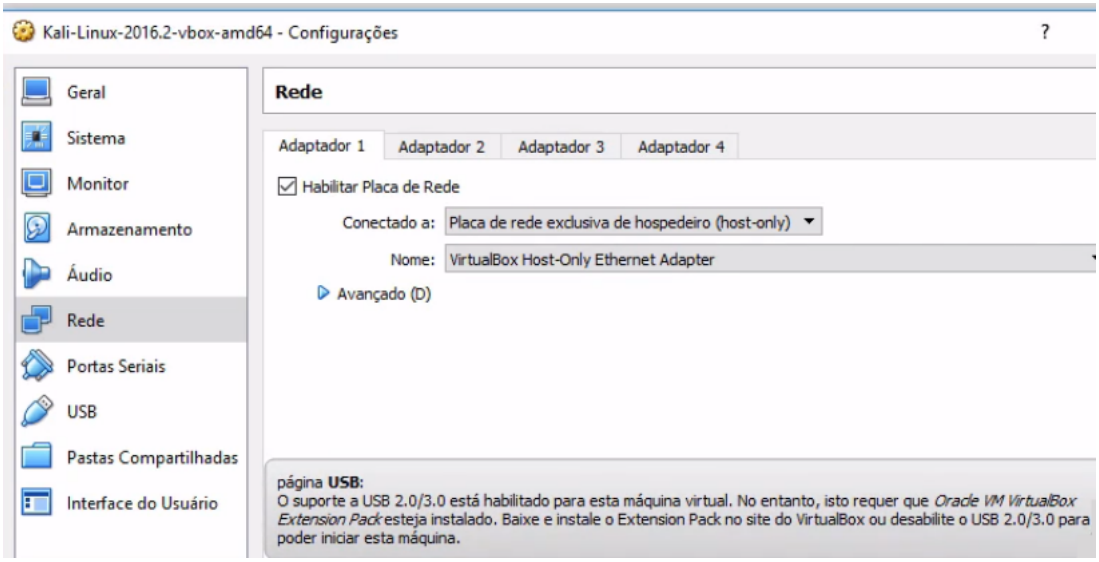
Essas alterações serão feitas de acordo com o seu computador. Eu recomendo 1 Gb como valor mínimo de uso de memória RAM, para ter uma performance razoável. Se o seu computador tiver mais capacidade, você pode colocar mais. Eu colocarei 2 Gb para o meu, que tem 16 Gb de memória.



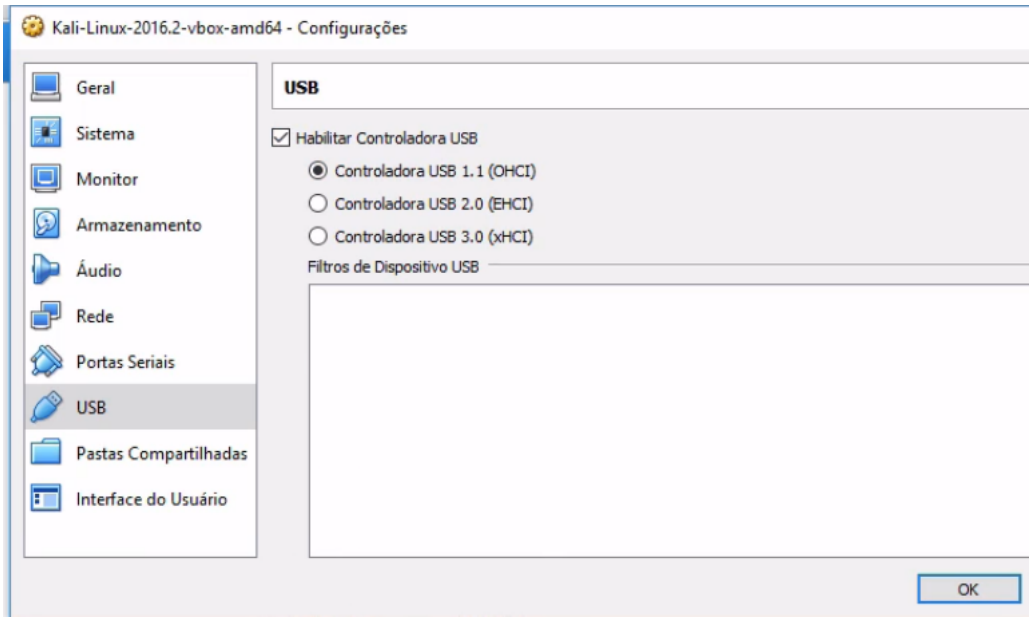
Agora mexeremos na aba `Rede`. Precisaremos colocar uma placa de rede no Kali Linux, para que ele trabalhe adequadamente. Usaremos a placa de vídeo do VirtualBox. Ela está listada como `Placa de rede exclusiva de hospedeiro(host-only)`.



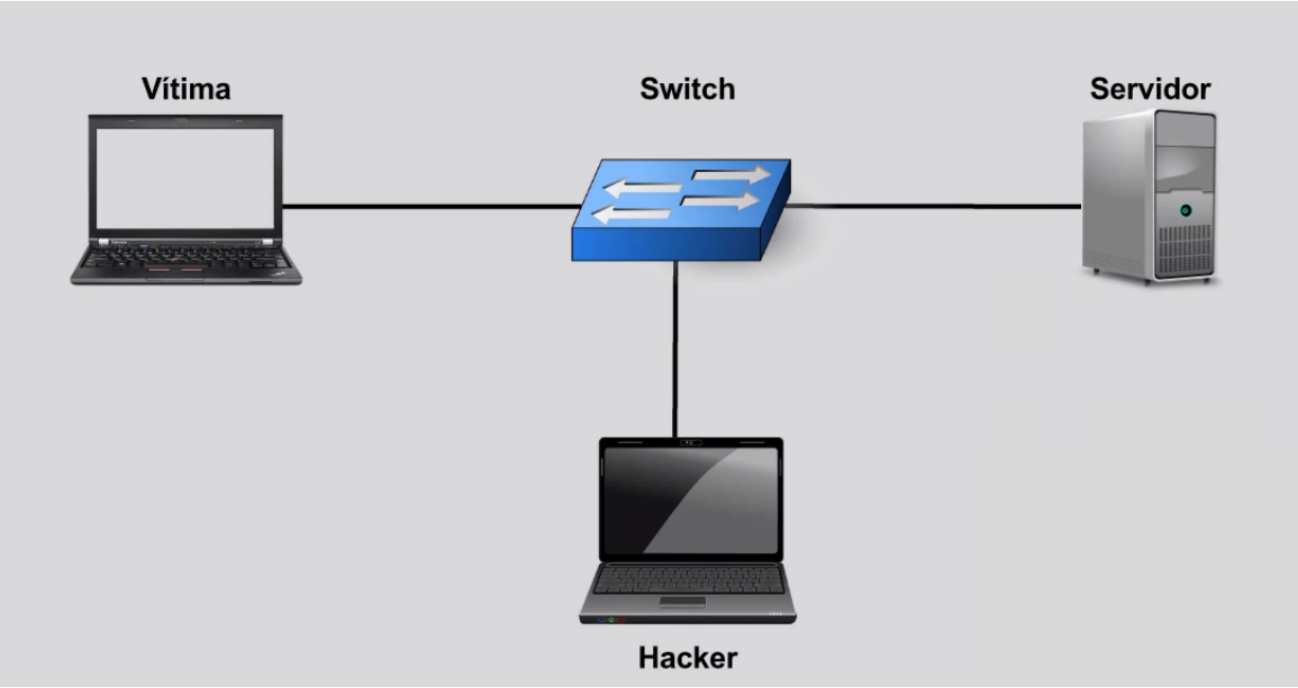
Perceba que no canto inferior consta o aviso `Configurações inválidas detectadas`. Ao clicarmos sobre ele, seremos informado que o problema está no suporte USB 2.0/3.0.



Para resolver esse problema, clicaremos na aba `USB`. Selecionaremos a `Controladora USB 1.1 (OHCI)`, e o aviso deve sumir.



Depois, basta dar `OK` na configuração e a máquina do hacker está pronta. Já temos a nossa própria máquina, a do João e o servidor.


Vítima
Switch
Servidor
Hacker