Metasploitable – Hacker Lab

13 de abril de 2015 / maximoz

Introdução

Você já deve ter ouvido falar sobre o Metasploit, um poderoso Framework com várias funcionalidades e muito útil para um pentester. Existe uma ferramenta que pode te ajudar a brincar um pouco com o metasploit (ou até o Nmap). Vou dar uma dica aqueles que tem um medo assíduo de fazer testes de penetração em redes desconhecidas no qual podem ser pegos por fazer muito barulho ou por caírem em algum tipo de honeypot, ou mesmo aqueles que são White Hat e não querem ferir a privacidade alheia. Venho apresentar-lhes a Metasploitable, uma VM (máquina virtual) que foi projetada e desenvolvida propositalmente para ser vulnerável e possibilitar a uma vasta exploração em um mar de vulnerabilidades. Existem algumas plataformas desenvolvidas com o mesmo propósito para você testar localmente suas habilidades, como DVWA (Damn Vulnerable Web Application) e WebGoat, mas hoje falarei somente sobre ela.

Ela foi desenvolvida pela equipe do Metasploit (Rapid7) diante da dificuldade causada pelos problemas encontrados ao aprender a usar o Metasploit na hora de encontrar alvos, escaneá-los e atacá-los. No entanto, não ajuda somente aos usuários do Metasploit, mas auxilia no aprendizado de qualquer outra ferramenta de exploração que seja um pouco complexa e que se precise de alvos para usar todas as suas funções. Em meu artigo anterior sobre o Nmap Scripting Engine (veja aqui), eu utilizei essa máquina virtual como vítima, o que acaba voltando ao Metasploit pois é possível usar o Nmap integrado à ele.

Chega de papo e vamos ao objetivo do post.

Instalação

É possível baixar a Metasploitable pelo SourgeForge sem nenhuma burocracia, mas eu baixaria pelo site oficial da Rapid7 para ter a certeza de que será a versão mais atualizada, só é preciso preencher alguns formulários, se quiser informe seus dados nos formulários mas as informações não precisam ser verdadeiras pra fazer o download. De qualquer maneira, deixarei os dois links para sua livre escolha.

Metasploitable SourceForge

Metasploitable Rapid7

Passo 0

Uma vez baixado, faça a extração do arquivo .zip no diretório que desejar, verifique se no que foi extraído contém o arquivo *Metasploitable.vmdk*, iremos precisar dele mais tarde.

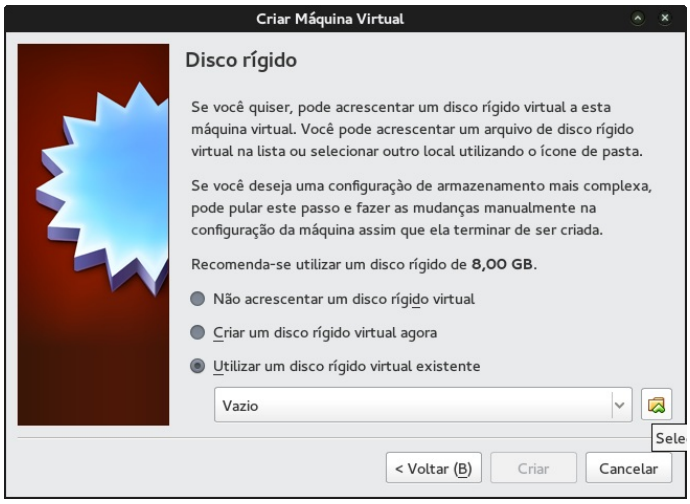
Execute seu VirtualBox; ao abrir, clique em ***Novo*** e na janela que aparecerá coloque as seguintes configurações:

Passo 1

Clique em ***Próximo*** e regule a quantidade de RAM que será dedicada à máquina na hora da sua execução, cuidado para não colocar tanto causando a perca de desempenho da sua máquina física. Nessa VM não há interface gráfica, somente linha de comando, então não há muita necessidade de muita memória RAM para funcionar. 512 MB é mais do que suficiente, ficará da seguinte forma:

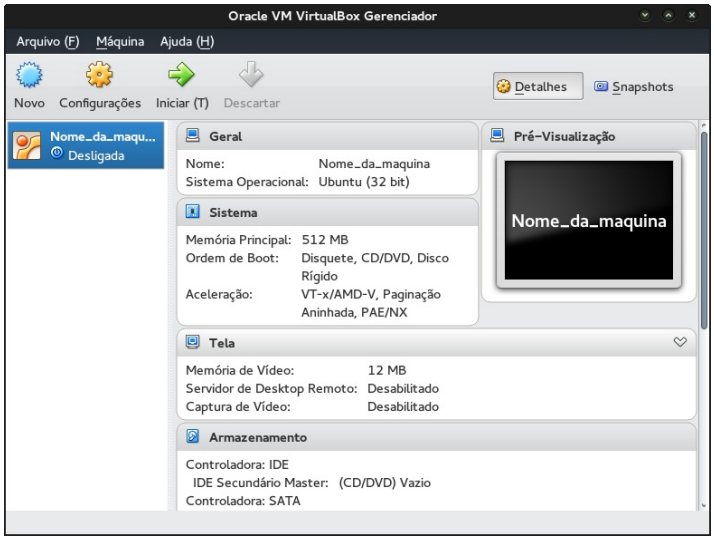
Passo 2

A seguir clique em ***Próximo*** novamente. Para quem já está familiarizado com o VirtualBox, deve estar acostumado em deixar marcado a opção ***Criar um disco rígido virtual agora***. Mas isso é pra quando você vai instalar um sistema num disco rígido virtual vazio, normalmente usando um arquivo de imagem ISO. No nosso caso, já temos uma máquina pronta, lembras de quando falei do arquivo *Metasploitable.vmdk*? Pois é, ele é nossa máquina pronta. Por esse motivo, escolheremos a opção ***Utilizar um disco rígido virtual existente***.



E então clique no ícone de escolha de diretório e vá até onde você fez o download e extraiu e escolha o arquivo *Metasploitable.vmdk*. Deverá ficar assim:

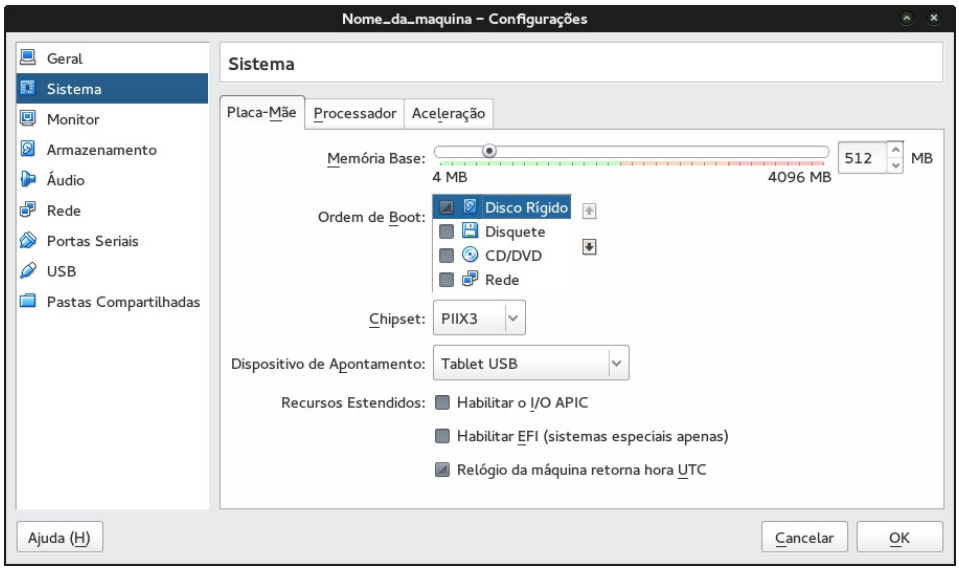
Ao clicar em ***Criar*** sua máquina já estará pronta para uso, mas pera aí! Como não é uma máquina com interface gráfica e, basicamente, é só ligá-la e deixá-la rodando sem nenhuma necessidade de ficar mexendo nela (mas, é claro, pra certas coisas, é preciso mexer nela através da linha de comando), vamos configurá-la antes tirando as opções que serão inúteis em seu uso.



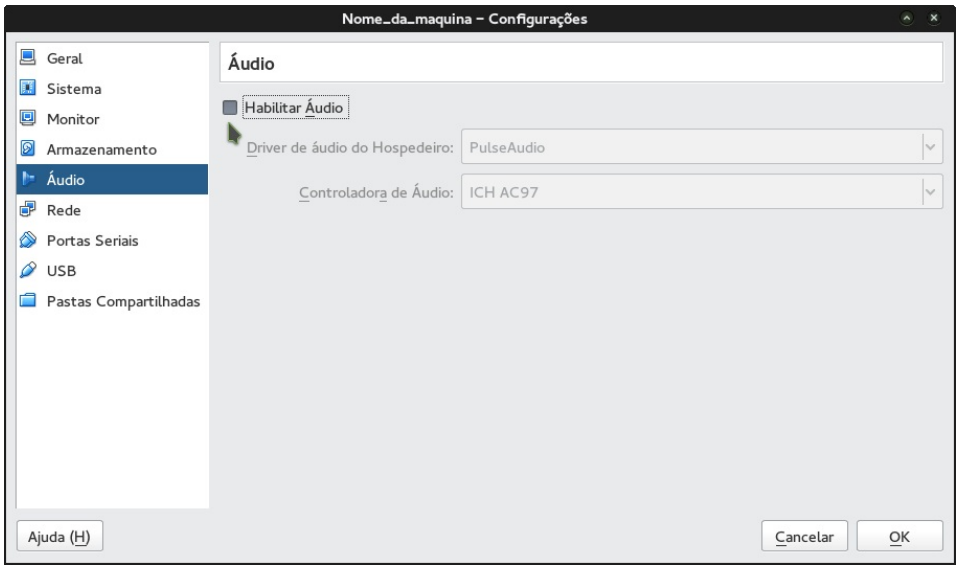
Passo 4: Configurando

Deixe a Metasploitable selecionada e vá na aba ***Máquina > Configurações***

Na aba ***Sistema***, em ***Ordem de Boot***, desmarque as opções ***Disquete*** e ***CD/DVD***, deixando somente a opção ***Disco Rígido*** marcada, pois os outros recursos não serão usados. Ficará dessa forma:



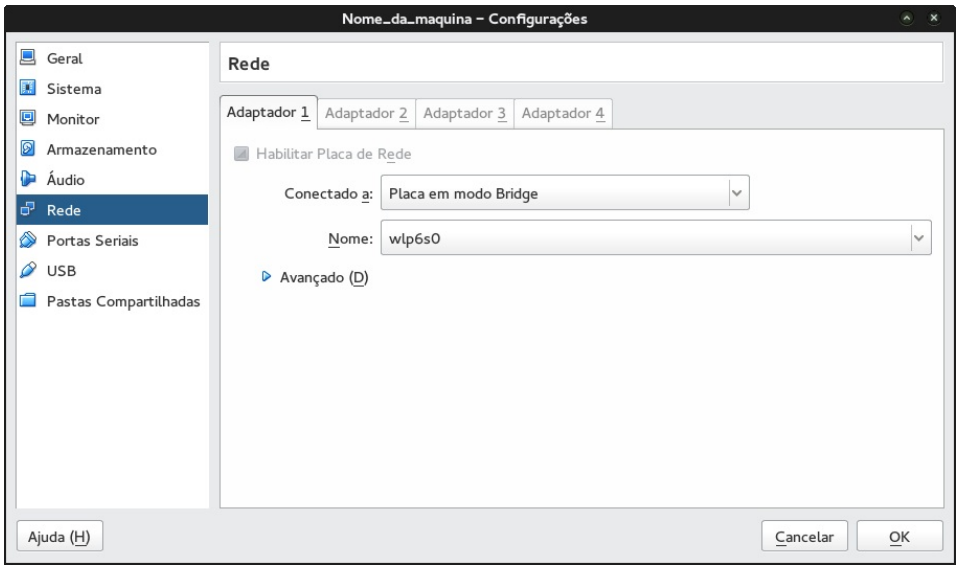
Vá na aba ***Áudio*** e desabilite-o também, é outro recurso obsoleto para essa máquina. Ficará assim:



Passo 5: Rede

Algo muito importante que deve ser ressaltado é que uma vez que você instala essa máquina, ela se torna pertencente a sua rede local, tudo bem por isso, o problema é que estamos falando de uma máquina vulnerável, se você deixar ela com livre acesso à rede externa ela estará praticamente com uma placa dizendo "Por favor, me invadam". Portanto esse é um passo e uma dica importante a se seguir.

Vá na aba ***Rede***, abaixo da opção ***Habilitar Placa de Rede*** no campo '***Conectado a:***', coloque ou ***Rede Interna*** ou ***Placa de rede exclusiva de hospedeiro (host-only)*** para limitar o acesso de estranhos. Em alguns casos, o ip interno da máquina não aparecerá com o comando *ifconfig* com essas opções de placa de rede mas aparece se você trocar por ***Placa em modo Bridge***, que é o meu caso. Ficará assim:

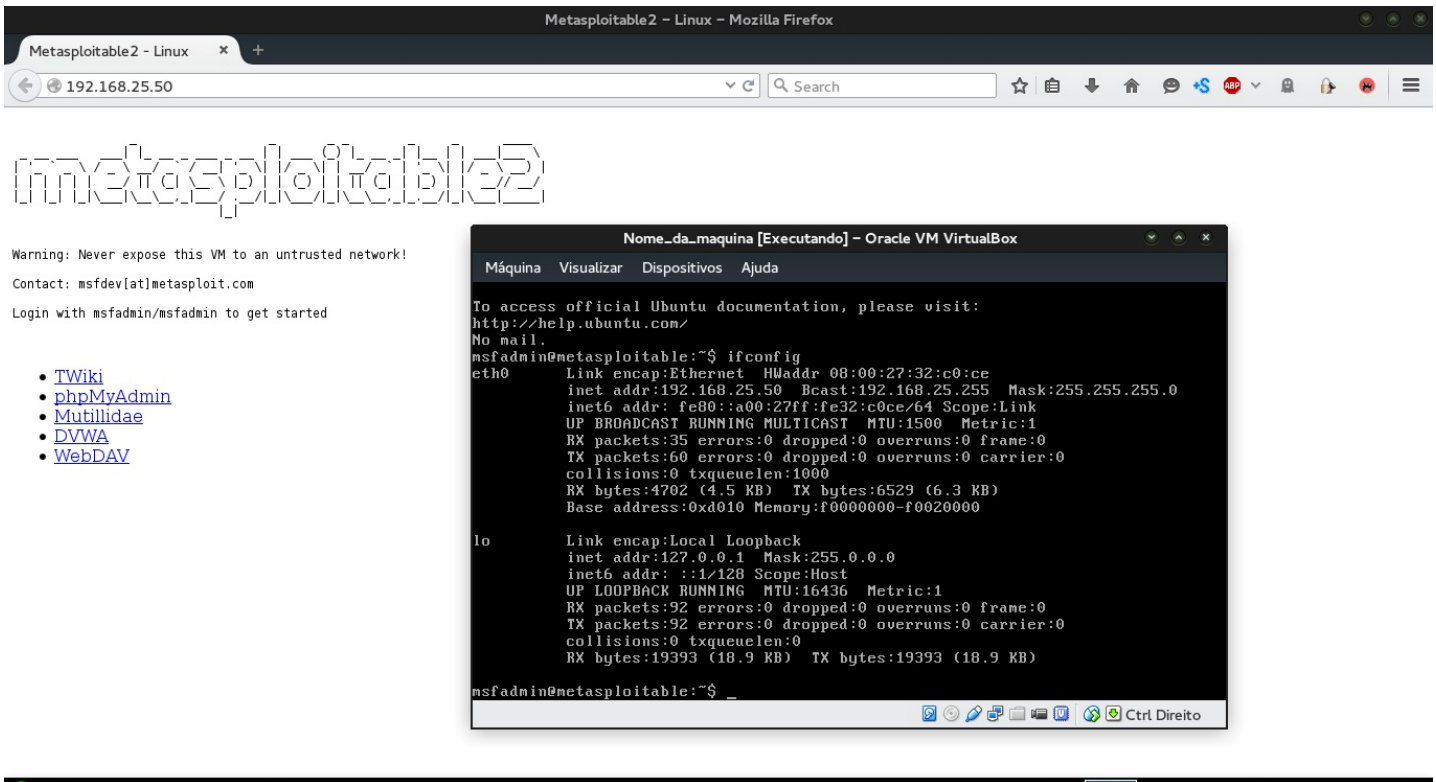


Iniciando a Máquina

Agora sim está tudo pronto para a inicialização da Metasploitable. Com ela selecionada, clique em ***Iniciar***.

A inicialização pode demorar um pouquinho mas não se preocupe, é porque são muitos serviços pra iniciar. Uma vez a máquina completamente inicializada, você se deparará com uma tela pedindo login e senha que são, por padrão, **login:msfadmin password:msfadmin**

E sua máquina já está disponível na rede para ser acessada, explorada e atacada. Para saber o ip interno dela é só digitar no terminal da máquina *ifconfig*, será o número que está seguido da expressão *inet addr*.



Agora você pode ficar à vontade para fazer testes de penetração com qualquer ferramenta de exploração e, acima de tudo, sem nenhum risco da CIA bater na sua porta pois você estará trabalhando em um ambiente local e legal.

Conclusão

Esse foi mais um tutorial ensinando a instalar o Metasploitable corretamente com um breve comentário sobre a mesma na introdução. É isso aí, muito obrigado à quem leu tudo e chegou até aqui. Deixarei alguns links a seguir que podem ser de ajuda.

Links Úteis

Documentação Metasploitable

Guia Metasploitable PDF

,