Tutorial para criar um container com REMnux

Utilizar o REMnux em um contêiner do Docker oferece uma maneira flexível e isolada de acessar e usar as ferramentas de análise de malware do REMnux sem a necessidade de configurar uma máquina virtual dedicada, poupando tempo e recursos. Vamos apresentar um tutorial passo a passo para começar a usar o REMnux em um contêiner Docker.

1 - Pré-requisitos

Ter o Docker instalado em seu sistema. Se você ainda não tem o Docker, visite o site oficial para instruções de instalação específicas para sua plataforma.

2 - Passo a Passo

Passo 1: Baixar a Imagem do REMnux Docker

Abra um terminal e execute o seguinte comando para baixar a imagem oficial do REMnux Docker:

```
docker pull remnux/remnux-distro
```

Este comando puxa a imagem mais recente do REMnux para o seu sistema local.

Passo 2: Criar e Iniciar um Contêiner REMnux

Após baixar a imagem, você pode criar e iniciar um contêiner usando essa imagem com o seguinte comando:

```
docker run -it --name remnux_instance remnux/remnux-distro
```

Aqui, -it permite a interação com o contêiner através do terminal, --name remnux_instance dá um nome ao seu contêiner para facilitar a referência futura, e remnux/remnux-distro especifica a imagem a ser usada para criar o contêiner.

Passo 3: Usar o REMnux no Contêiner

Após iniciar o contêiner, você será colocado no prompt de comando do REMnux dentro do contêiner. Agora, você pode começar a usar as ferramentas do REMnux. Por exemplo, para verificar as atualizações das ferramentas, você pode executar:

```
sudo remnux update
```

Passo 4: Sair do Contêiner

Para sair do contêiner, você pode simplesmente digitar exit. Isso o levará de volta ao prompt de comando do sistema hospedeiro.

Passo 5: Gerenciando o Contêiner

Para iniciar o contêiner novamente após sair, use:

```
docker start -ai remnux_instance
```

Para ver todos os seus contêineres (ativos e inativos), execute:

```
docker ps -a
```

Para remover o contêiner completamente (caso você queira começar do zero ou não precise mais dele), primeiro certifique-se de que o contêiner está parado e então execute:

```
docker rm remnux_instance
```

Passo 6: Atualizar a Imagem do REMnux

Para atualizar a imagem do REMnux para a versão mais recente no futuro, primeiro remova a imagem antiga e depois puxe a nova versão usando o comando docker pull mencionado no Passo 1.

3 - Ferramentas

Para um tutorial sobre as principais ferramentas para análise de malware, leia o arquivo [VM] Malware Analysis.