**IF Goiano Campus Ceres**

**Bacharelado em Sistemas de Informação**

**Disciplina**: Segurança da Informação

**Professor**: Roitier Campos Gonçalves

**Valor**: 2 Pontos

**Tipo**: Individual

**Entrega**: GIT e SUAP

**Data da Entrega:** 05/11/2023

**Aluna:** Laura Sousa Lima

**Implantação e monitoramento de uma rede virtualizada usando Vagrant, roteamento e Tcpdump.**

Criei a pasta do trabalho, iniciei o cmd dentro da pasta e dei um ‘vagrant init’, editei o arquivo adicionando as configurações:

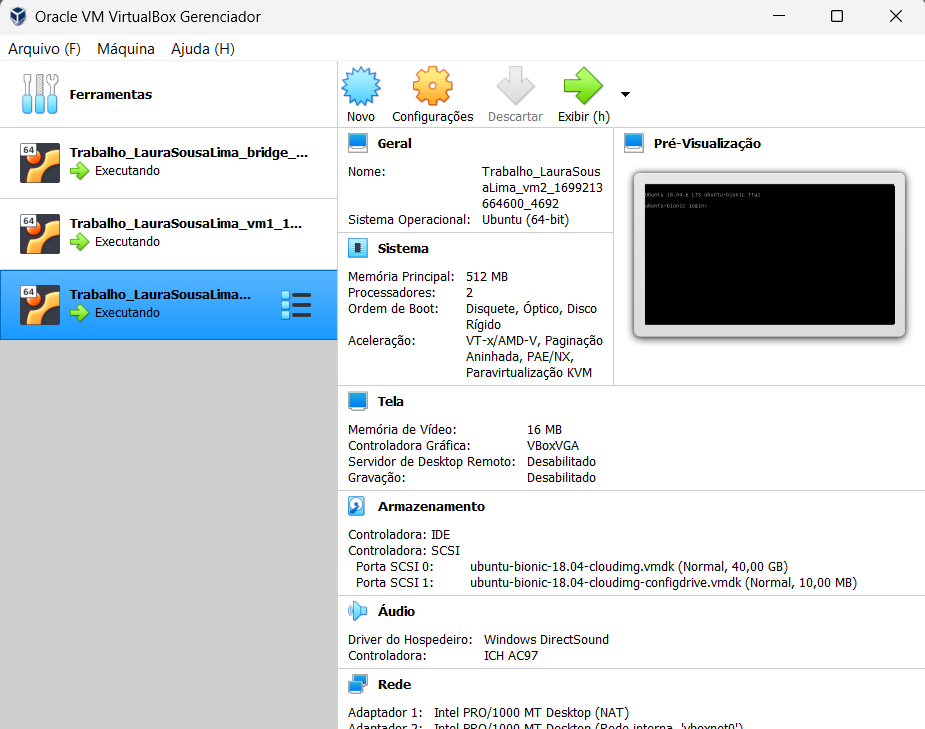
Na hora de dar o “vagrant up” estava aparecendo um erro relacionado a um conflito com as configurações de rede do VirtualBox. Parece que as configurações do host-only estavam causando um problema.

No virtual box criei uma única interface de host-only e atribuí-la a todas as máquinas virtuais:

VirtualBox > "Arquivo" > "Preferências" > "Rede".

Crie uma única interface de host-only "vboxnet0"

As máquinas virtuais já estarão na mesma rede virtual devido à configuração da rede privada em cada uma delas.



Configurando a máquina Brigde como ponte:

Tive que baixar o Wls w Ubuntu, abri o terminal do ubuntu executei o seguinte comando para instalar o pacote bridge-utils:

sudo apt-get update

sudo apt-get install bridge-utils

Acessei a máquina bridge usando o comando “vagrant ssh bridge”

Depois configurei as interfaces de rede:

sudo nano /etc/network/interfaces

adicionei essas configurações:

auto br0

iface br0 inet static

address 192.168.1.1

netmask 255.255.255.0

bridge\_ports enp0s3

bridge\_stp off

bridge\_fd 0

depois disso é só executar para criar e ativar a interface de bridge com as seguintes atualizações:

sudo brctl addbr br0

sudo brctl addif br0 eth0

sudo ifconfig br0 up

Após isso foi feito a configurações do roteamento estático nas máquinas virtuais restantes ("vm1" e "vm2"), fazendo o mesmo processo anterior, definindo o endereço IP das máquinas virtuais dentro da mesma sub-rede, mas diferentes dos endereços da máquina bridge:

sudo nano /etc/network/interfaces

vm1:

auto eth0

iface eth0 inet static

address 192.168.1.2

netmask 255.255.255.0

gateway 192.168.1.1 # O gateway deve apontar para o endereço da interface de bridge

vm2:

auto eth0

iface eth0 inet static

address 192.168.1.3

netmask 255.255.255.0

gateway 192.168.1.1 # O gateway deve apontar para o endereço da interface de bridge

Após isso testei a conectividade entre as máquinas:

vagrant ssh

ping

ping 192.168.1.3 – Acessei a máquina virtual "vm1" e testei o ping

Por fim, para realizar a captura de pacotes usando tcpdump, você pode executar o seguinte comando nas máquinas virtuais para monitorar o tráfego de rede:

O tcpdump será instalado nas máquinas virtuais (arquivo Vagrantfile)

Para realizar uma análise de tráfego usando o tcpdump entre as máquinas virtuais "vm1" e "vm2," é necessário acessar a maquina, exemplo, a vm1:

sudo tcpdump -i br0 -n -vvv -s0 -w captura\_vm1\_vm2.pcap

o comando a cima instrui o tcpdump a capturar pacotes na interface "br0" e salvar a captura em um arquivo chamado "captura\_vm1\_vm2.pcap"

Depois fiz ele abrir o navegador web e fazer um ping pra vm2 , para gerem tráfego de rede

Após esse processo, parei a captura do tcpdump dei Ctrl + C

Transferi o arquivo de captura da "vm1" para a máquina host para análise posterior

Depois acessei a vm2 e fiz a mesma coisa.

**Roteamento Estático**: Nessa abordagem, os caminhos da rede são configurados manualmente. É como um mapa onde você coloca as direções para chegar a um lugar e não muda automaticamente. É simples e previsível, tem menos trabalho para o processador, e é mais seguro, mas não é bom para redes grandes e complexas.

**Vantagens:**

* Simplicidade e controle.
* Menos uso de recursos do computador.
* Maior segurança.

**Desvantagens:**

* Não é bom para redes grandes.
* Manutenção manual trabalhosa.
* Menos resistente a problemas de rede.
* Não se adapta a mudanças na rede.

**Comparação com o Roteamento Dinâmico**: Roteamento dinâmico é como usar GPS, ele se adapta automaticamente às mudanças na estrada. É ótimo para redes grandes e em constante mudança, mas é mais complexo e requer mais recursos.

A escolha entre os dois depende do tamanho e complexidade da rede. Às vezes, é bom usar uma combinação dos dois para diferentes partes da rede.