UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Disciplina: INE 5680 – Segurança da Informação e de Redes
Professora: Carla Merkle Westphall

Configurar Kali e OWASP Broken no VirtualBox + Atualizar aplicação Mutillidae na Kali para OWASP 2017

- OWASP Broken Web Applications Project (https://sourceforge.net/projects/owaspbwa/files/1.2/OWASP_Broken_Web_Apps_VM_1.2.ova/download): baixar esta máquina do link e no VirtualBox selecione a opção Importar Appliance (menu Arquivo – opção Importar Appliance). Login e senha aparecem na tela quando a máquina é carregada (login: root, senha: owaspbwa).

- Máquina Linux no VirtualBox: login: root, senha: toor
    - Se você já tem a máquina Kali não é necessário executar esse passo. A máquina Kali Linux a ser usada é uma máquina que será importada no VirtualBox. Você deve baixar a imagem da Kali **para VirtualBox** disponível: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/. Importar a máquina na opção Importar Appliance.

Configurar rede do VirtualBox

KALI LINUX

1. Menu Arquivo, opção “Host Network Manager” (ou Ctrl-W) na tela do VirtualBox (figura 1).

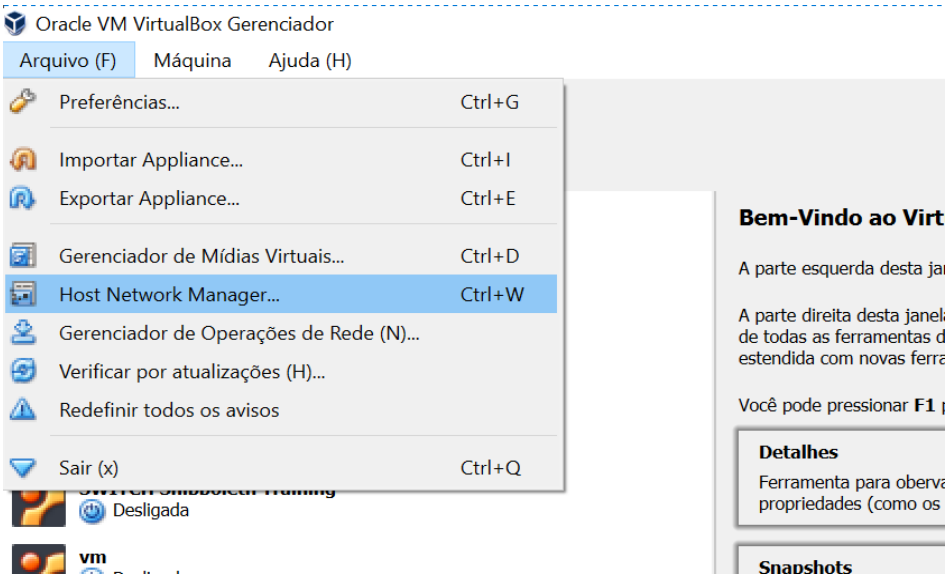

Figura 1 – Host Network Manager.

2. Na aba “Adaptador”, deixar a opção “Configurar Adaptador Manualmente” selecionada e colocar o valor 10.1.2.3 no campo Endereço IPv4 (figura 2).

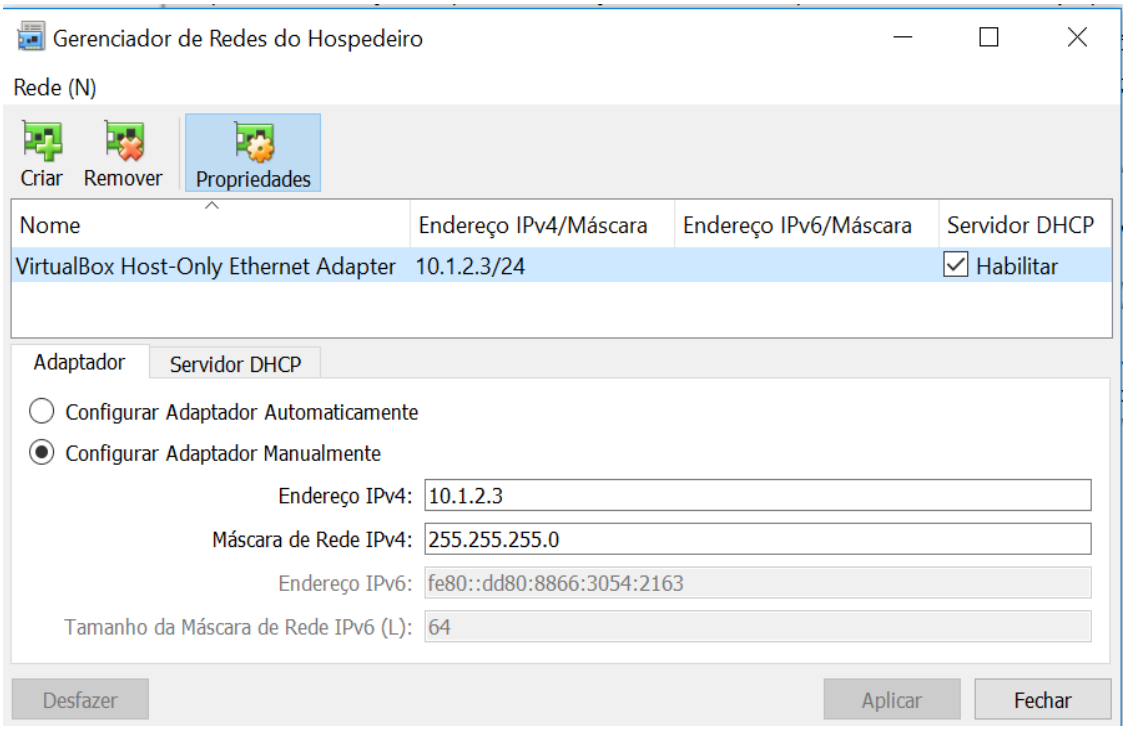

Figura 2 – Configurar Redes do Hospedeiro no VirtualBox.

3. Na aba “Servidor DHCP”, editar e colocar os valores da figura 3.

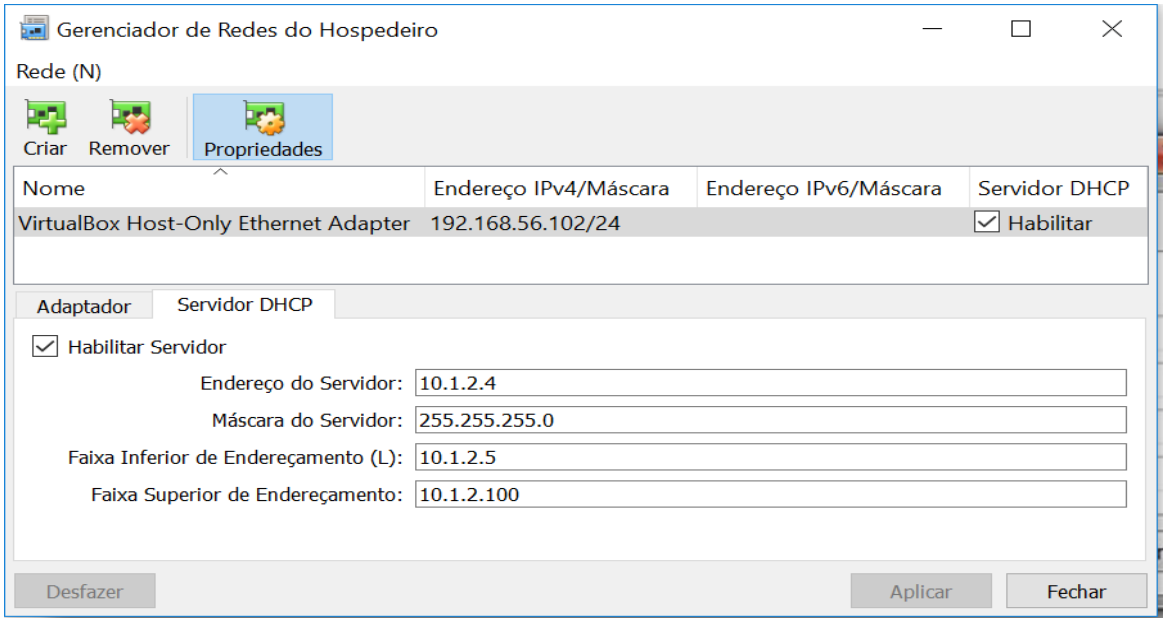

Figura 3 – Servidor DHCP.

3. Fechar o VirtualBox e abrir o programa novamente.

4. Configurar a rede no Adaptador 1 da máquina Kali-Linux como “NAT”, conforme a figura 4.

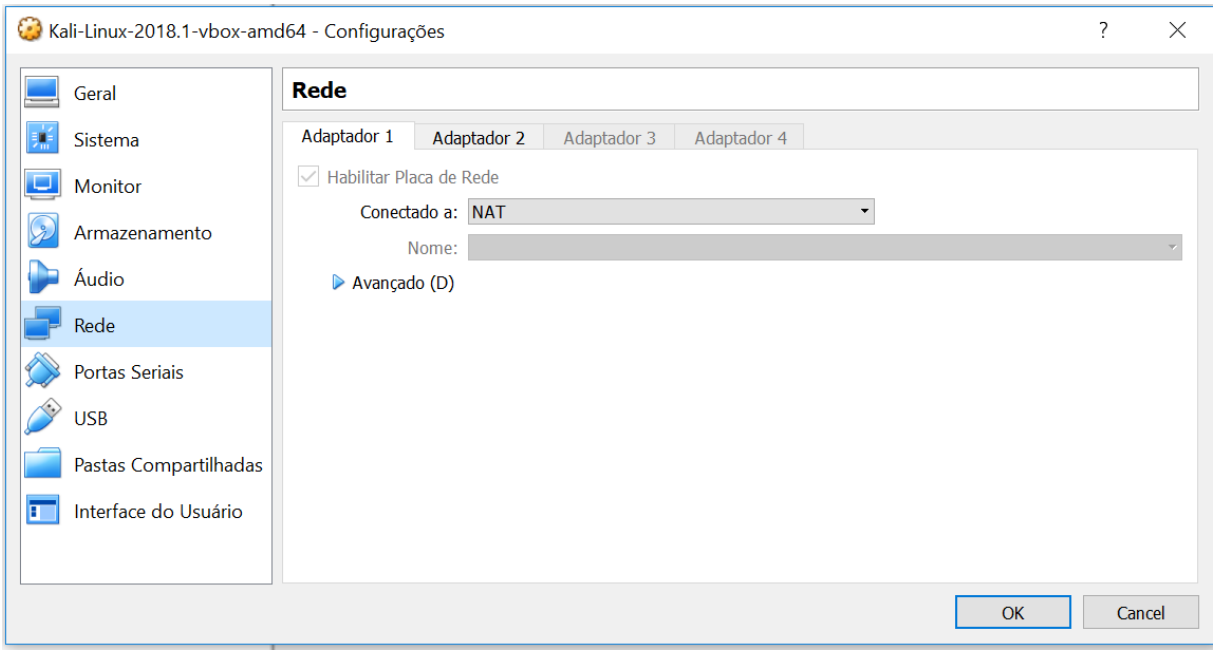

Figura 4 – Adaptador 1 da Kali.

5. Acrescentar na rede da máquina Kali-Linux uma outra placa (Adaptador 2) como “VirtualBox Host-Only Ethernet Adapter”, conforme a figura 5.

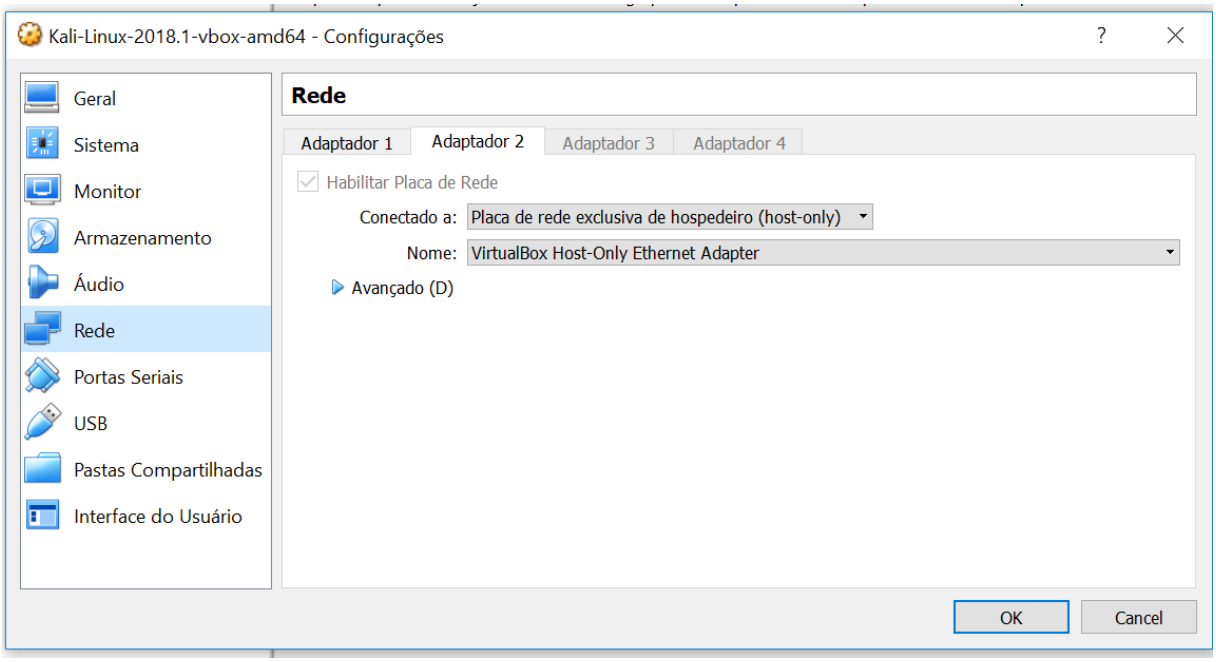

Figura 5 – Adaptador 2 da Kali.

5. Ao ligar a máquina, verifique se todas as interfaces de rede estão presentes e tem o IP correto com o comando **#ifconfig** (figura 6). NORMALMENTE UMA DAS INTERFACES ESTÁ DESLIGADA! Você pode não obter a mesma tela da figura 6.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::94d8:987:6ebd:6008  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c5:0d:1c  txqueuelen 1000  (Ethernet)
        RX packets 49  bytes 8231 (8.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84  bytes 7417 (7.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.2.5  netmask 255.255.255.0  broadcast 10.1.2.255
        inet6 fe80::a00:27ff:fecf:5824  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cf:58:24  txqueuelen 1000  (Ethernet)
        RX packets 113  bytes 27856 (27.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 54  bytes 5180 (5.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

Figura 6 – ifconfig da Kali.

6. Para ligar a interface desligada, você poderá ligar/desligar uma interface de rede pela interface gráfica na Kali, clicando no botão superior direito, conforme mostra a figura 7. Ao usar a interface gráfica, quando se liga uma placa, a outra desliga ☹. Por isso é preciso fazer os passos descritos abaixo.

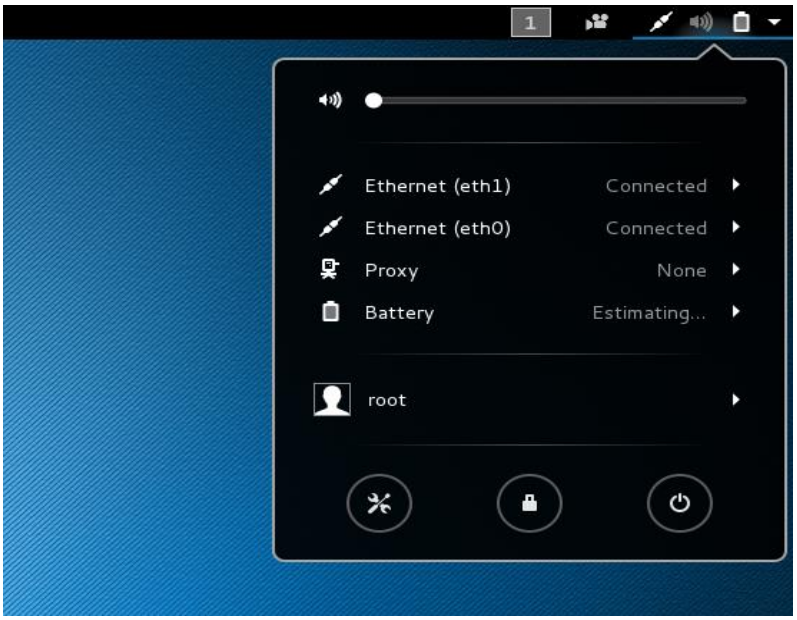

Figura 7 – Ligar placas de rede na interface gráfica da Kali.

O texto a seguir detalha como ligar/desligar as placas pela interface gráfica.

Pela interface gráfica, clique no ícone de rede no canto superior direito. Observe na figura 8 que a eth1 está Connected e a eth0 está Off.

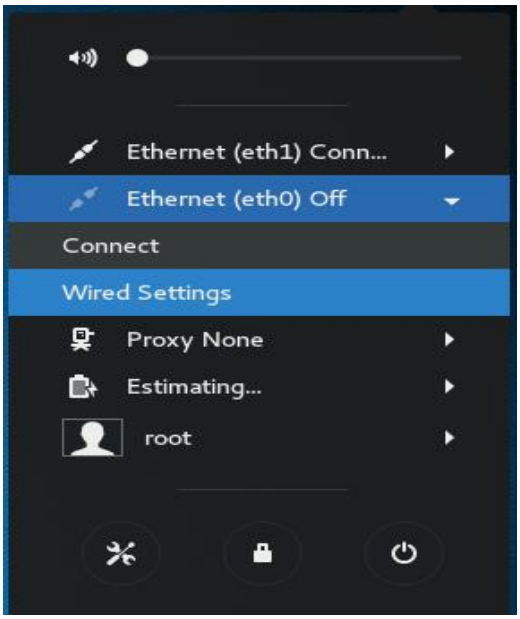

Figura 8 – Placas de rede na interface gráfica da Kali.

Clique na placa que está Off, depois clique em Wired Settings. Você deve estar visualizando a tela da figura 9.

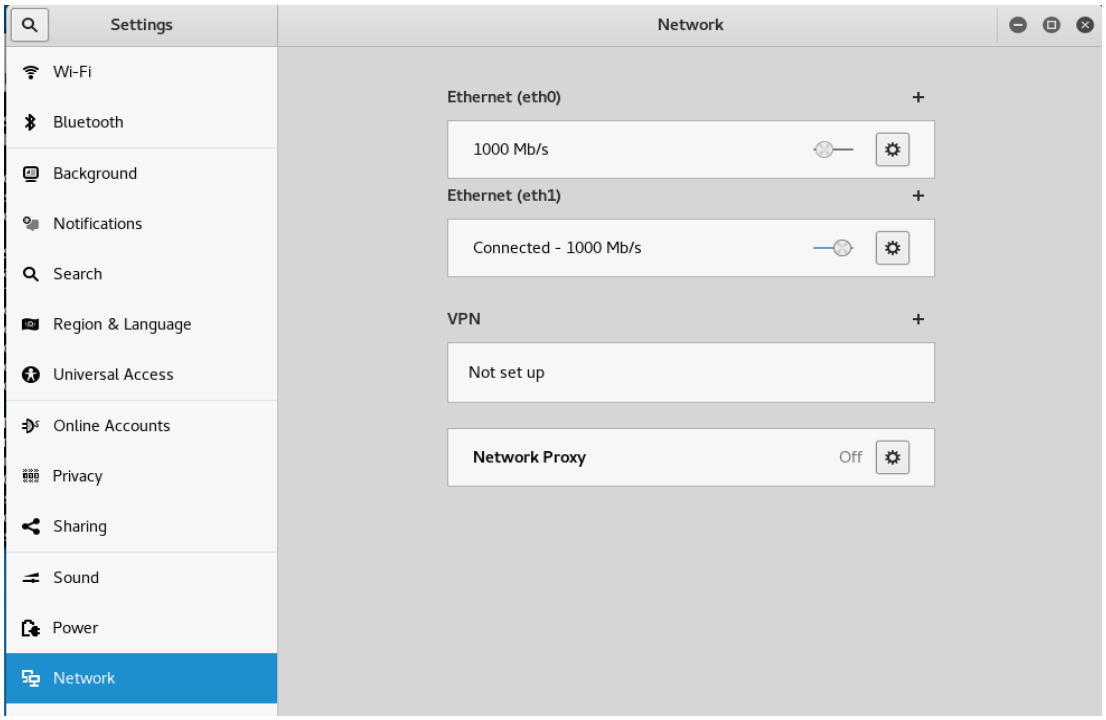

Figura 9 – Wired Settings.

Agora, você deve clicar no “sinal de +” na placa eth0 que está desligada e em seguida clicar em Add Profile (figura 10).

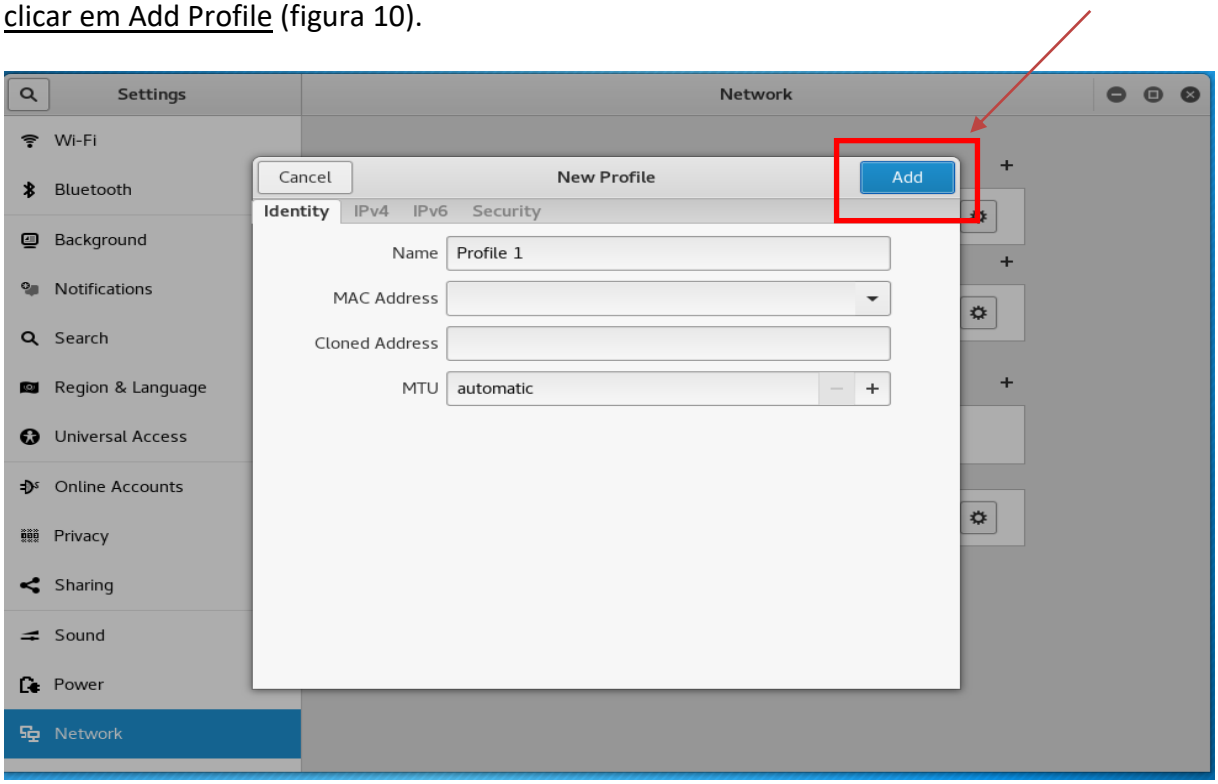

Figura 10 – Adicionar Profile.

Clique no botão Add e você terá o Profile 1 (perfil que indica que as duas placas ficam ligadas), conforme a figura 11.

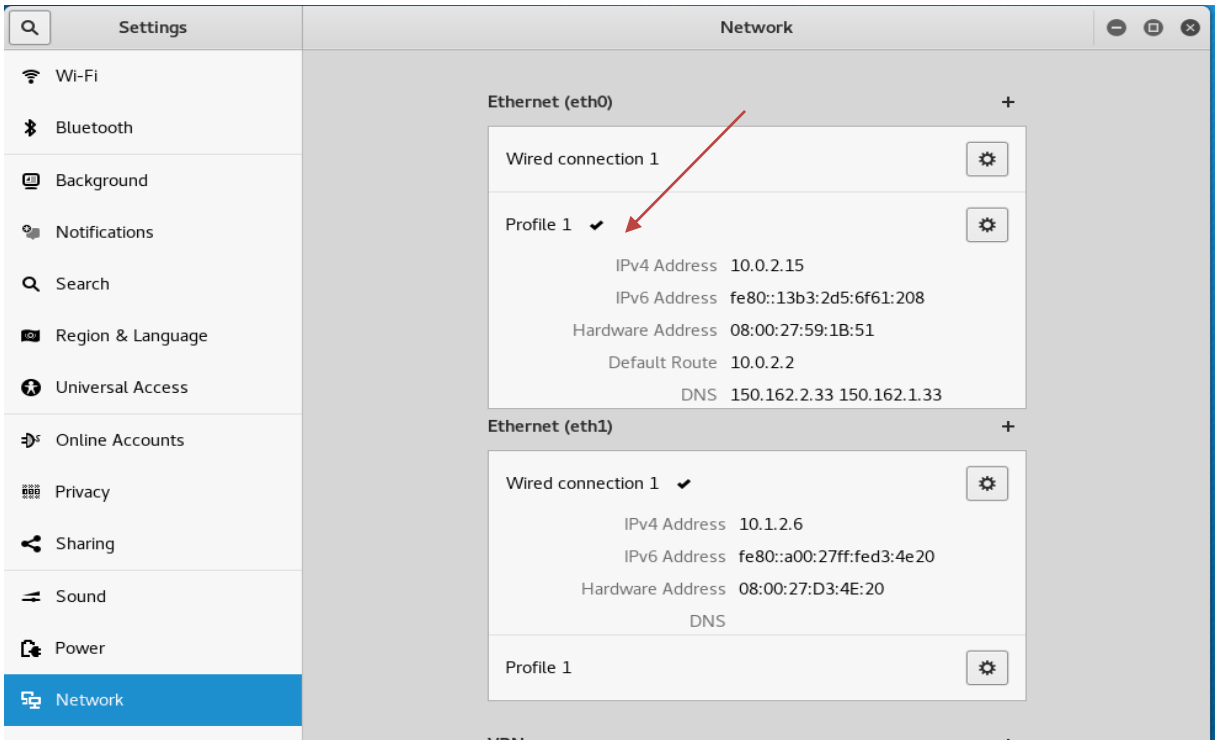

Figura 11 – Profile 1.

Depois disso, as duas placas devem estar no estado Connected e a próxima vez que a máquina for ligada, as duas placas estão ligadas. Agora, execute o ifconfig e verifique que as duas placas têm os seus endereços IP, similares aos encontrados na figura 6.

OWASP Broken

1. Configurar a rede no Adaptador 1 da máquina OWASP Broken como "Placa de rede exclusiva de hospedeiro (host-only)", conforme a figura 12.

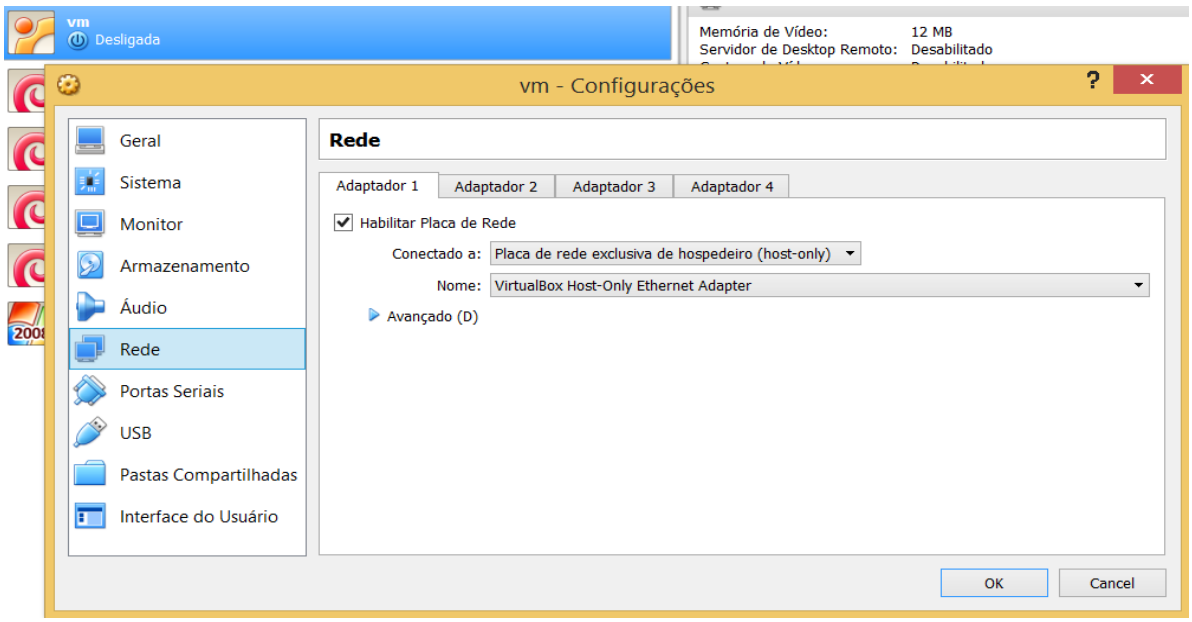

Figura 12 – Adaptador 1 da Owasp Broken.

Kali Linux – Instalar a aplicação Mutillidae na máquina Kali Linux

A aplicação Mutillidae II, versão 2.6.24, está instalada na máquina OWASP Broken, porém possui apenas suporte para teste da lista de vulnerabilidades TOP TEN do ano de 2013.

Você irá instalar a versão mais nova da Mutillidae II (versão 2.7.9) **na máquina Kali Linux** porque essa versão já possui suporte para testes da lista de vulnerabilidades TOP TEN do ano de 2017.

Para isso você deve:

1. Executar o script descrito no link https://miloserdov.org/?p=87.
   Siga as instruções descritas na parte "How to install OWASP Mutillidae II in Kali Linux". Você irá copiar e colar o script da página no arquivo upd_mutillidae.sh. Depois vai executar este script. O script instala a aplicação mutillidae na máquina Kali Linux.

```
#!/bin/bash

sudo apt update
sudo apt install php-xml php-fpm libapache2-mod-php php-mysql php-xml php-gd php-imap php-mysql php-gettext php-curl -y
sudo a2enmod proxy_fcgi setenvif
sudo systemctl restart apache2
sudo a2enconf php7.3-fpm
sudo systemctl reload apache2
sudo systemctl restart apache2.service
sudo service php7.3-fpm restart
sudo systemctl restart mysql

cd /tmp
git clone https://github.com/webpwnized/mutillidae
if [ $? -ne '0' ]; then
    exit 1
fi

if [ -d "/var/www/html/mutillidae.backup" ]; then
    sudo rm -rf /var/www/html/mutillidae.backup
fi

if [ -d "/var/www/html/mutillidae" ]; then
    sudo mv /var/www/html/mutillidae /var/www/html/mutillidae.backup
fi

sudo mkdir /var/www/html/mutillidae
sudo mv mutillidae*/* /var/www/html/mutillidae/

sudo chown -R www-data:www-data /var/www/html/mutillidae/

sudo rm -rf mutillidae*

cd
```

2. Executar os comandos na Kali para acertar login e senha da aplicação. Executar cada um desses comandos no terminal:

```
mysql -u root
use mysql;
update user set authentication_string=PASSWORD('mutillidae') where user='root';
update user set plugin='mysql_native_password' where user='root';
flush privileges;
quit;
```

3. Agora você poder acessar o browser no seguinte endereço da Kali: http://localhost/muttilidae/ ou no browser da sua máquina real: http://IP Kali/mutillidae/.

4. Na primeira vez que executar a aplicação é necessário, conforme listado em https://miloserdov.org/?p=87 clicar em **setup/reset the DB.**
5. Ao reiniciar a Kali, você deve executar os seguintes comandos no terminal antes de carregar a aplicação Mutillidae no browser:
   - service php7.3-fpm start
   - service mysql start
   - service apache2 start

==========FIM DA CONFIGURAÇÃO==========

As operações descritas a seguir são APENAS DICAS que PODEM ser feitas na máquina Kali Linux, não são obrigatórias

***** Copiar e colar na máquina virtual**

Habilitar "Área de transferência compartilhada" clicando no menu da janela da VM *Dispositivos > Área de transferência compartilhada*.

***** Instalar Adicionais para Convidado no VirtualBox (para poder compartilhar pasta com sua máquina real). Isso pode ser feito na máquina Kali Linux. Não modifique a máquina OWASP Broken pois é muito antiga e não tem interface gráfica.**

Instale os pacotes necessários:

```
apt-get install build-essential module-assistant
```

Configure seu sistema para a construção de módulos do kernel:

```
m-a prepare
```

No menu da janela da VM, clique em *Dispositivos > Inserir imagem de CD dos Adicionais para Convidado*. Isto colocará um CD virtual na VM o qual deve ser montado automaticamente. Caso não seja montado automaticamente, monte com o comando abaixo:

```
mount /dev/cdrom  /mnt
```

Agora copie o script de instalação dos Adicionais para Convidado para uma pasta do HD virtual:

```
cp /mnt/VBoxLinuxAdditions.run /tmp
```

Dê permissão de execução para o script:

```
chmod +x /tmp/VBoxLinuxAdditions.run
```

E execute-o:

```
/tmp/VBoxLinuxAdditions.run
```

O restante do processo de instalação é automático.

Para finalizar, reinicie o sistema:

```
shutdown –r now
```

***** Para montar a pasta compartilhada no VirtualBox:**

```
mount -t vboxsf nomePastaCompartilhada /mnt
```