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

Tarefa Prática – NMAP (http://www.nmap.org)

O nmap é uma ferramenta de varredura de portas (*port scanner*) bastante utilizada. É muito útil para testes de rede e detecção de problemas, mas também muito utilizada como ferramenta de ataque (pois permite o mapeamento dos serviços remotos). Deve ser utilizada somente na rede sob sua jurisdição, pois seu uso pode ser visto como uma tentativa de ataque por parte de outro administrador.

Além da detecção de portas abertas, o nmap usa técnicas de "*TCP/IP Fingerprinting*" para tentar detectar diversos outros aspectos de uma máquina remota. O "*TCP/IP Fingerprinting*" consiste de coleta de atributos obtidos pelas implementações durante a comunicação com as máquinas remotas considerando as camadas do protocolo (TCP, IP). Cada implementação do protocolo TCP/IP em cada sistema operacional define valores diferentes para vários parâmetros: tamanho inicial do pacote, TTL inicial, tamanho da janela, tamanho máximo do segmento e outros. Assim, com as respostas dos valores default, o nmap consegue descobrir:

- Versão do sistema operacional
- *Uptime* da máquina: mede desde quando a máquina está funcionando
- Informações adicionais a respeito dos serviços em execução

Várias opções do nmap consideram os pacotes SYN, ACK/SYN e ACK que são trocados entre duas partes para o estabelecimento de uma conexão TCP/IP (Figura 1).
Veja a explicação do estabelecimento da conexão no site: (http://pt.wikipedia.org/wiki/Transmission_Control_Protocol#Estabelecimento_da_liga.C3.A7.C3.A3o).

Handshake do TCP/IP

```
A → B: SYN; meu número é X
B → A: ACK; agora X+1
       SYN; meu número é Y
A → B: ACK; agora Y+1
       (inicia a conversa)
```

Figura 1 – Handshake do TCP/IP

Sintaxe geral:

```
nmap [Tipos de Scan] [Opções] {especificação do alvo}
```

Alguns exemplos de utilização do nmap:

```
nmap scanme.nmap.org
nmap –sP www.inf.ufsc.br
```

Sinopse de algumas opções do nmap:

-s<tipo>	Tipo de varredura usada. Algumas varreduras procuram evitar que o sistema destino registre as tentativas de acesso. Tipos: S(SYN), T(Connect), A(ACK), W(Windows), U(UDP), N(Null), F(FIN), X(Xmas), I(Idle), Y(SCTP), O(protocolo IP).
-sS	Varredura TCP SYN. Ativa o scan do tipo "Stealth SYN Scan", onde a conexão não chega a ser completada para que a porta seja testada. Esse tipo de scan é mais difícil de ser detectado.
-sT	Varredura TCP Connect. Usa conexões TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS.
-sV	Ativa o scan do tipo detecção de serviços, onde é detectada a versão do serviço em execução em cada porta aberta. Esse scan envolve um conexão TCP completa, portanto fica registrado nos logs da máquina remota.
-sP	*Somente* executa um scan usando o ping (descoberta de hosts), e então mostra os hosts disponíveis que responderam ao scan.
-PO	Realiza a varredura da máquina mesmo que ela não responda ao ping, sendo útil em servidores que estão sendo filtrados por firewalls. Vê se o host está "vivo", sem usar o "ping". A opção –P0 (o 0 é um zero) diz ao nmap para fazer um scan do endereço IP desconsiderando se o IP permite tráfego do protocolo Internet Control Message Protocol (ICMP).
-O	Ativa detecção de versão do sistema operacional e uptime.
-p <portas>	Especifica uma lista (separada por vírgulas) ou um intervalo de portas a ser varrido. Exemplo: 22,25,1024-2000,5499.
-v	Modo "verboso", mostra informações adicionais, geralmente úteis.
-A	Detecta versão de SO, usa script de scanning e traceroute.
-T4	Execução mais rápida.

Tabela 1 – Opções de uso do nmap

Nas referências você encontra uma lista de locais para procurar os significados de outras opções dos comandos (Guia de referência do nmap: http://nmap.org/man/pt_BR/, Exemplos de comandos com suas explicações em http://nmap.org/man/pt_BR/man-examples.html, Explicações sobre opções em http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas).

Os comandos do nmap serão testados em ambiente virtual, usando duas máquinas: a máquina Kali Linux e a máquina Metasploitable2. Você deve baixar as máquinas, importá-las no VirtualBox, configurar a rede e usar os comandos para responder as perguntas.

Baixar as máquinas virtuais e importar cada uma das máquinas no VirtualBox

- Máquina Linux no VirtualBox: login: root, senha: toor
    - Nesta máquina você tem o nmap já instalado e pode ser usado em linha de comando, abrindo um terminal Linux
        - 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 em (+-3.0 GiB): https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/. Importar a máquina na opção Importar Appliance. Sugiro fazer o download da imagem Kali Linux 32 bit VBox Pae. É uma máquina 32 bits (Figura 2). Também está disponível no google drive: https://drive.google.com/file/d/0B3iGhd--qDpcYS1HRXpKeHpxUlE/view?usp=sharing.

Prebuilt Kali Linux VMware Images | Prebuilt Kali Linux VirtualBox Images

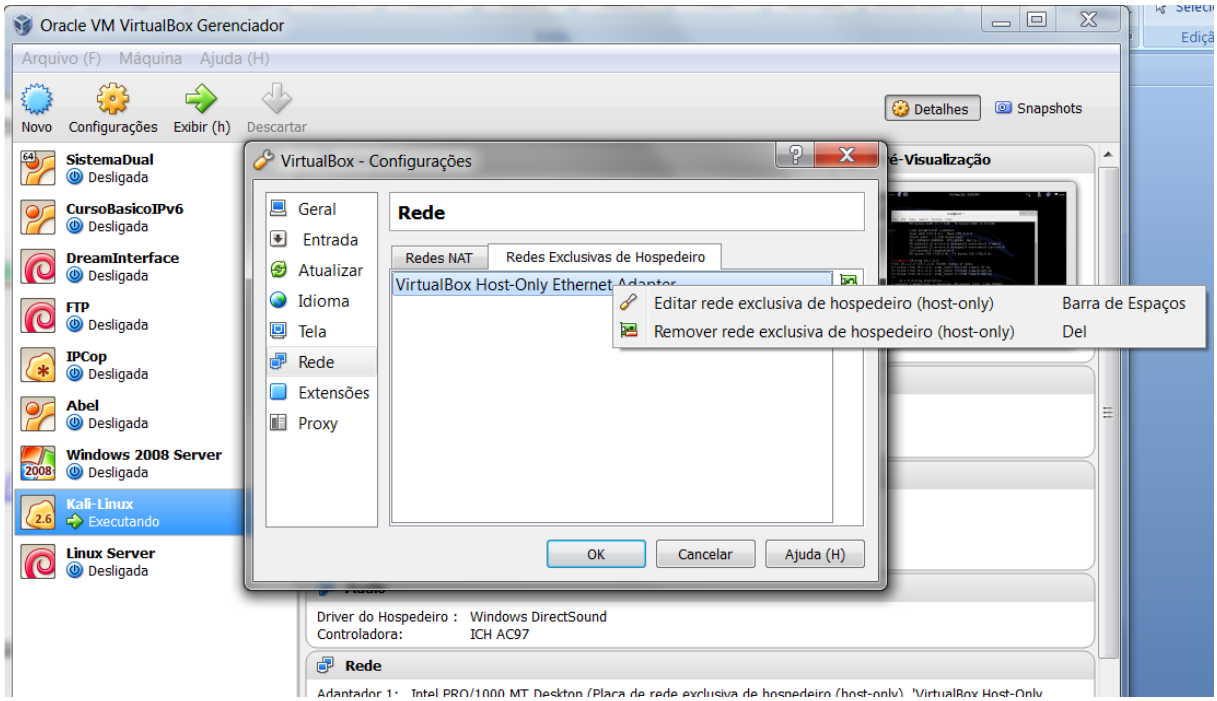
Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VBox	Torrent	3.0G	2016.1	f1f59b09b97903f5d4a3f47fa2e13896daf3c2ef
Kali Linux 32 bit VBox PAE	Torrent	3.0G	2016.1	987f2c04a4d595b1716ecfe61ce4074d1adac303

Figura 2 – Download da imagem da Kali para VirtualBox

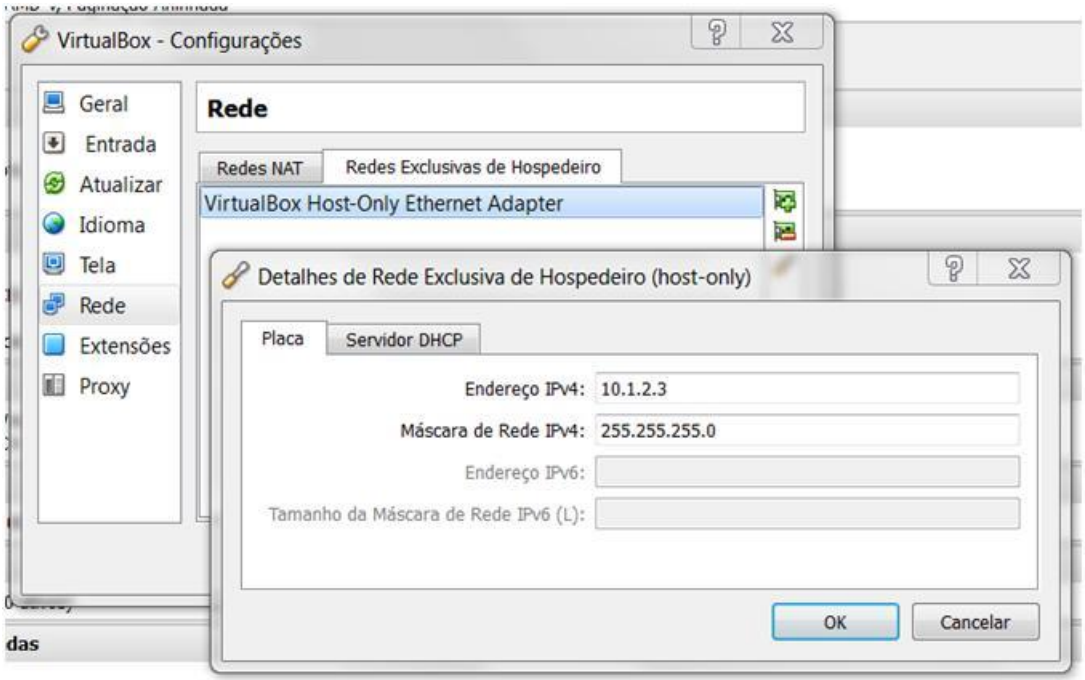
- Máquina Metasploitable2: login: msfadmin, senha: msfadmin
    - A máquina Metasploitable2 é uma máquina propositalmente instalada com serviços antigos, mal configurados e com aplicações a serem usadas para ataques e estudos na área de segurança. Você pode baixar a máquina Metasploitable2 (+-861 MiB) a ser importada no VirtualBox do seguinte link do google drive: https://drive.google.com/open?id=0B3iGhd--qDpcMFlwb3pGejE1LVU. Importar a máquina no VirtualBox na opção Importar Appliance.

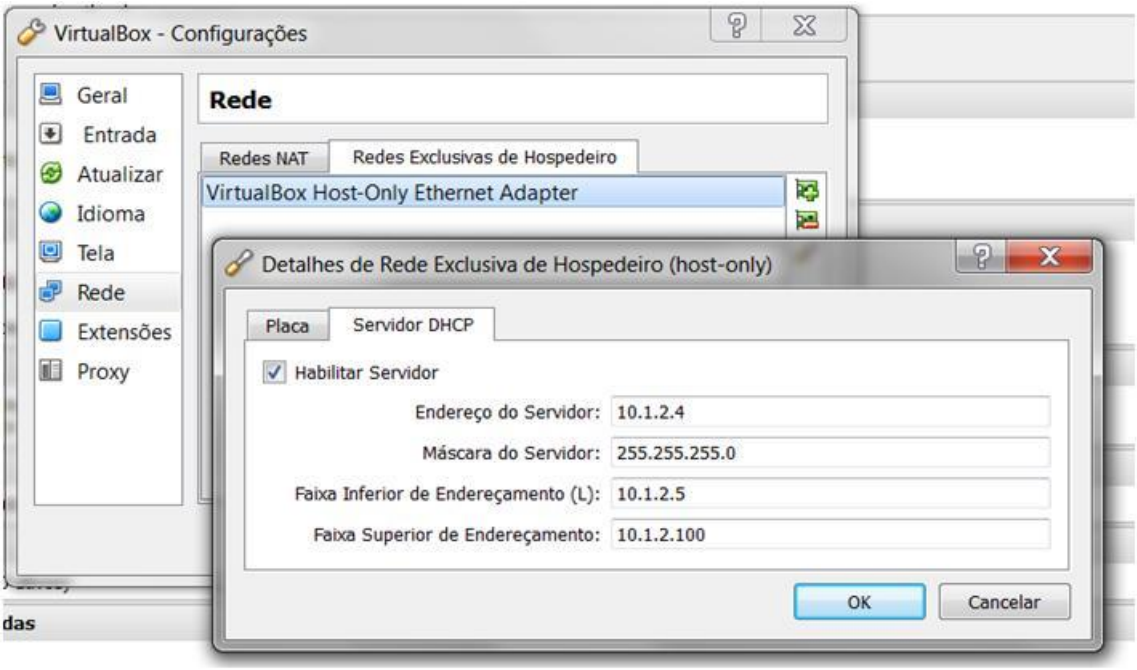
Configurar rede do VirtualBox

1. Clicar em Ctrl-G na tela do VirtualBox para encontrar “Redes Exclusivas de Hospedeiro”

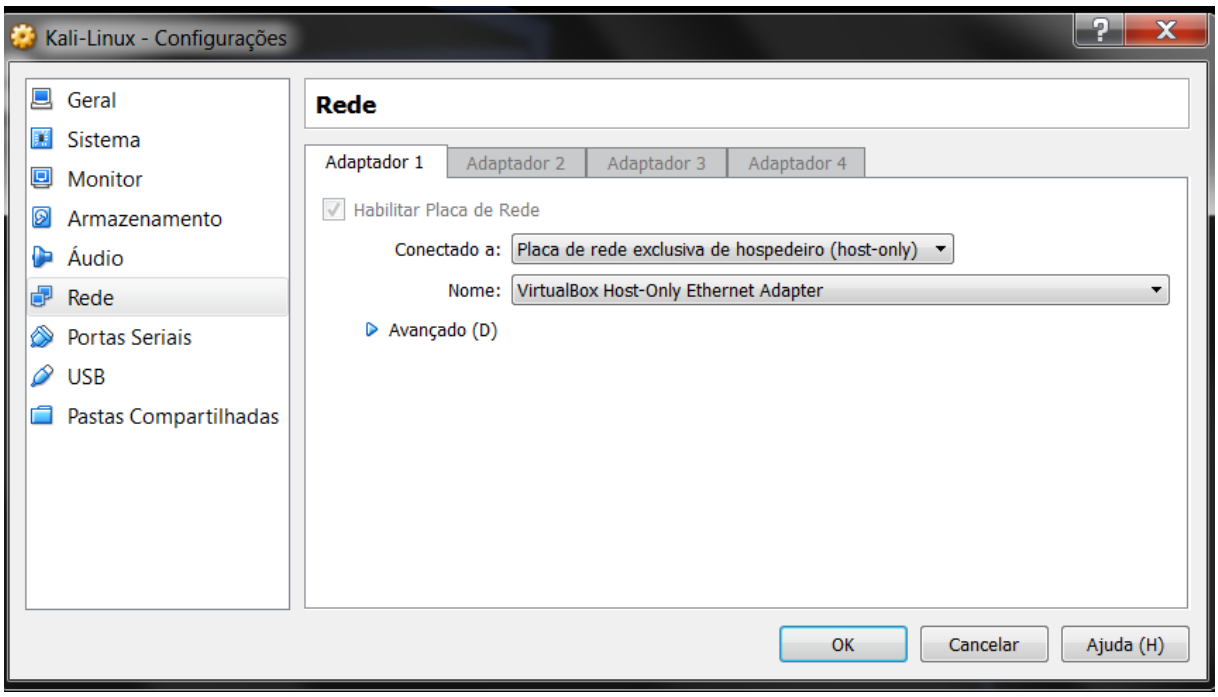


2. Editar e colocar os valores das figuras

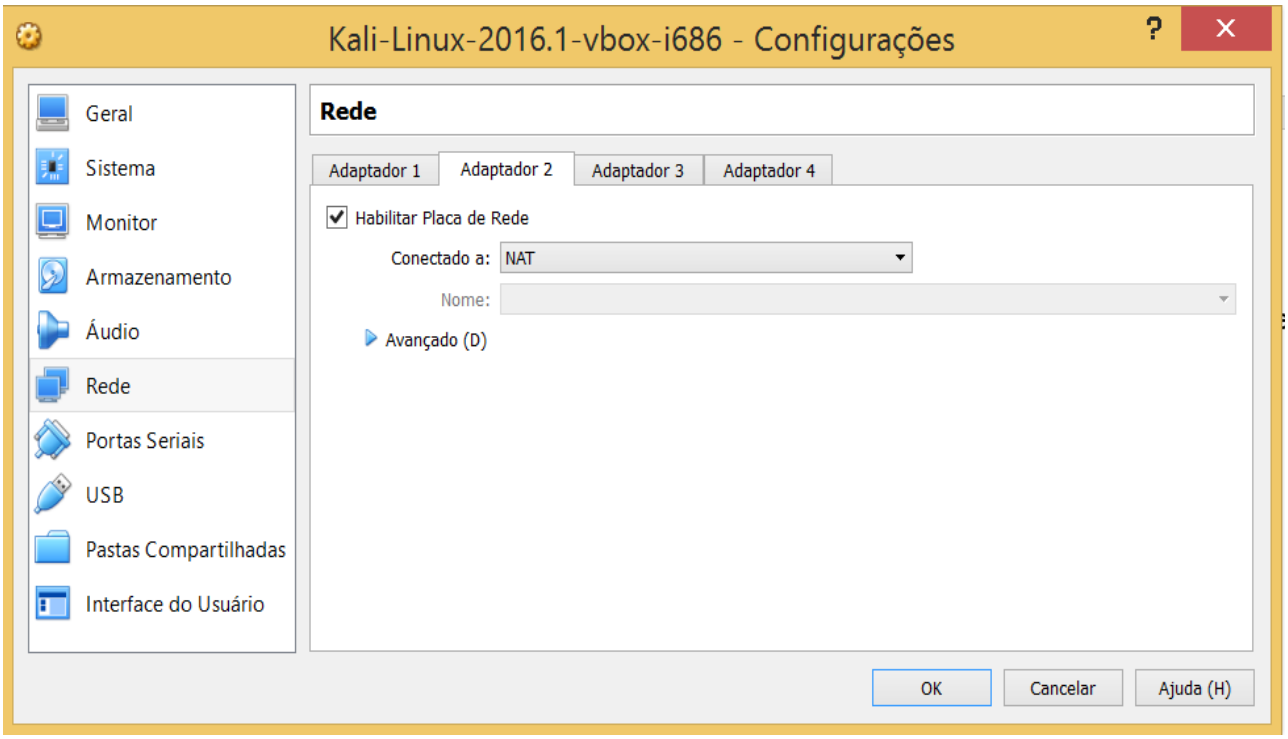




3. Configurar a rede no Adaptador 1 da máquina Kali-Linux e da máquina Metasploitable 2 como “Placa de rede exclusiva de hospedeiro (host-only)”, conforme a próxima figura



4. Acrescentar na rede da máquina Kali-Linux uma outra placa (Adaptador 2) como “NAT”, conforme a próxima figura. Assim a máquina Kali-Linux terá acesso a Internet.

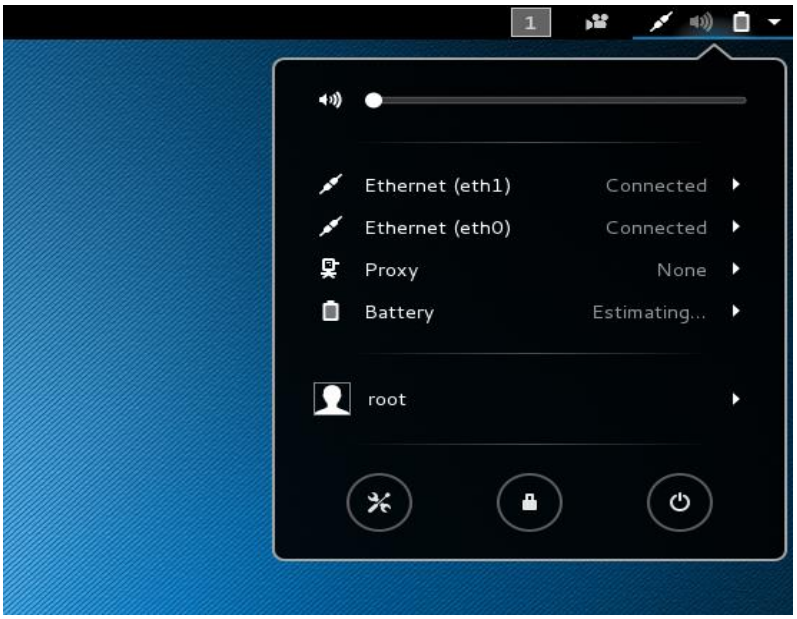


Ao ligar as máquinas, verifique se todas as interfaces de rede estão presentes e tem o IP correto com o comando **#ifconfig**.

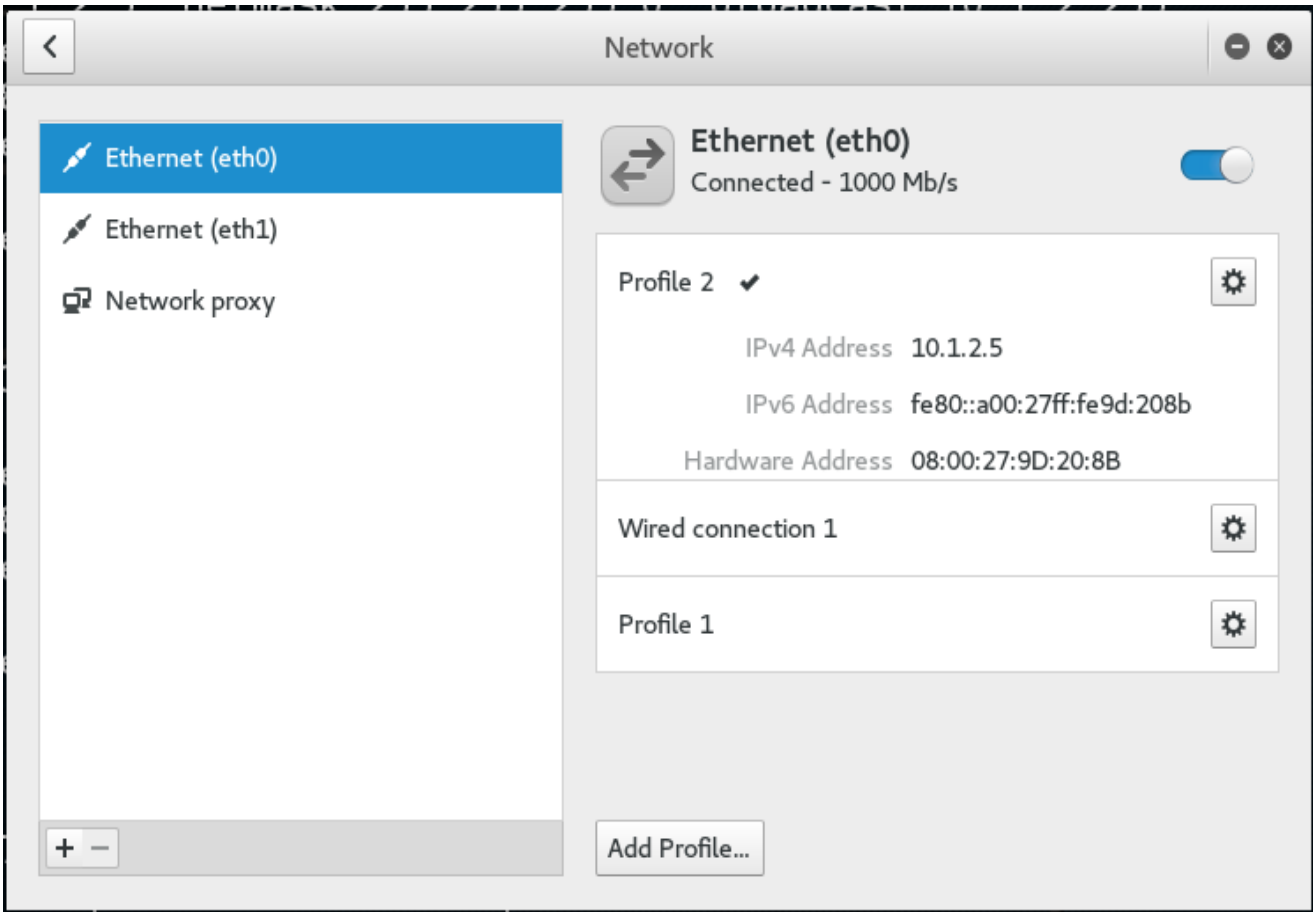
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.2.5  netmask 255.255.255.0  broadcast 10.1.2.255
        inet6 fe80::a00:27ff:fe9d:208b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:20:8b  txqueuelen 1000  (Ethernet)
        RX packets 28  bytes 8179 (7.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1884 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::a00:27ff:fe11:e70a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:11:e7:0a  txqueuelen 1000  (Ethernet)
        RX packets 6  bytes 1660 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 2278 (2.2 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 0  (Local Loopback)
        RX packets 20  bytes 1200 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1200 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c7:0a:1b
          inet addr:10.1.2.7  Bcast:10.1.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec7:a1b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5930 errors:1 dropped:0 overruns:0 frame:0
          TX packets:4354 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:479258 (468.0 KB)  TX bytes:276080 (269.6 KB)
          Interrupt:10 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:252 errors:0 dropped:0 overruns:0 frame:0
          TX packets:252 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:97801 (95.5 KB)  TX bytes:97801 (95.5 KB)

msfadmin@metasploitable:~$ _
```

Você poderá ligar/desligar uma interface de rede pela interface gráfica na Kali, clicando no botão superior direito, conforme a figura seguinte.



Se necessário, LIGUE AS INTERFACES PELA INTERFACE GRÁFICA, conforme a figura seguinte.



Para testar a conectividade entre as duas máquinas, use o ping. Na Kali: **ping 10.1.2.7** (configure o ping usando o IP da metasploitable2). Na Metasploitable2: **ping 10.1.2.5** (configure o ping usando o IP da Kali). O ping deve funcionar de uma máquina para outra.

Tarefa (responder as questões marcadas em azul e gerar um relatório em pdf a ser postado no moodle):

1) Abra um terminal na Kali-Linux e veja as opções do nmap digitando: # **nmap** <Enter> ou # **nmap --help**

2) Execute o nmap e teste os seguintes comandos. Para responder:

I. Copie e cole o *screenshot* da execução de cada comando;
II. Interprete os resultados obtidos em cada comando (pesquise nas referências para interpretar da melhor forma possível).

a) nmap –sV 10.1.2.7 (IP da Metasploitable2)

b) nmap -v –A 10.1.2.7 (IP da Metasploitable2)

Identifique pelo menos dois serviços vulneráveis que podem ser identificados a partir desse resultado. Pesquise qual a vulnerabilidade dos serviços.

c) nmap –sP 10.1.2.0/24

d) nmap –sS –O –v www.inf.ufsc.br

e) **nmap -sT -Pn -n --top-ports 10 --reason -oA hhs_5_tcp hackerhighschool.org**

f) nmap -sV scanme.nmap.org

g) nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 www.inf.ufsc.br

h) nmap -sS -P0 -p 20-100 -O -v -T3 webmail.lrg.ufsc.br

i) nmap –n –O www.inf.ufsc.br

j) nmap –sP –PA --packet-trace www.inf.ufsc.br

k) nmap –p 80 –v -iR 5 -Pn

l) Responda: Qual a diferença entre um scan de uma conexão TCP e um SYN scan ?

m) Responda: Qual o nível de certeza na estimativa do tipo de sistema operacional que o nmap fornece com a diretiva –O ? Pode-se confiar 100% na estimativa ?

n) Crie dois comandos (baseado nos exemplos de http://www.hackerhighschool.org/lessons/HHS_en5_System_Identification.v2.pdf e de http://nmap.org/man/pt_BR/man-examples.html), explique o objetivo dos comandos e teste os comandos. O comando NÃO PODE ser igual a nenhum comando anterior listado aqui.

3) Faça: Abra a interface gráfica do nmap, chamada Zenmap. Crie os comandos para cada uma das questões. Depois comente e analise os resultados obtidos para entregar como resposta. Os comandos também podem ser testados na linha de comando (modo texto do nmap).

   a) Realize a varredura de um site listando as portas abertas e os serviços identificados.

   b) Realize a varredura de uma rede inteira que está sob sua responsabilidade para identificar todas as máquinas da rede. Observe o desenho da topologia criada pelo Zenmap. **(Exemplo: nmap –sP 10.1.2.0/24)**

   c) Realize a varredura de uma rede inteira que **não** está sob sua responsabilidade para identificar todas as máquinas da rede. Tente usar opções que não possam identificar facilmente a varredura. **(Exemplo: nmap –PS 10.1.2.0/24)**

   d) Escolha um alvo e crie o comando para identificar o sistema operacional e também se o alvo responde na porta 80 e 443 (HTTPS). Lembre de usar uma opção que não seja facilmente detectada pelo firewall.

   e) Para o alvo da questão anterior, identifique o tipo de serviço que executa na porta 80 (**Exemplo a ser adaptado: nmap –sV –p80 ipDoAlvo**). Essa informação servirá para que?

   f) Realize uma varredura decoy para se esconder. Veja a descrição e sintaxe na figura abaixo. Em que situação você usaria essa varredura?

Varreduras Decoy	Realiza varreduras em um alvo utilizando endereços falsos. O objetivo é "esconder" o verdadeiro alvo de sistemas de detecção de intrusos (IDS).	`# Nmap -s S -D 101.102.103.104, 1.1.1.1, 2.2.2.2, 3.3.3.3 ip_alvo`

Comentários sobre o Nmap (prof. Bosco)

Utilitários como o Nmap estão em constante atualização e podem passar despercebidos por firewalls ou IDS. O que pode diminuir os riscos é a configuração de firewalls com regras bem definidas, diminuição dos serviços ativos no gateway deixando apenas aqueles indispensáveis ao seu funcionamento e análise constante de seus arquivos de log. Um sistema de detecção de intrusos, como o SNORT, é indicado também.

O Nmap pode e deve ser usado para averiguação do estado do seu host, principalmente se for um servidor. Use, constantemente, para monitorar o estado das portas e se elas pertencem a algum serviço legítimo ou não.

Se um serviço não é legítimo, é porque existe um *"backdoor"* associado à porta, colocado por algum atacante, e isto significa um ataque na forma de uma intrusão. Pode ter sido instalado por programas maliciosos chamados "*rootkit*".

O Nmap pode ser considerado uma ferramenta auxiliar na intrusão ou um excelente utilitário para consultores de segurança e administradores de rede.

==========

1. Instalar o nmap:

- Linux (Ubuntu):

```
sudo apt-get install nmap
sudo apt-get install zenmap
```

No Linux, executar o zenmap como root `(pode ser: gksu zenmap)`

- Windows (já instala o nmap e a interface gráfica, chamada Zenmap):

http://nmap.org/download.html

==========

Referências:

1. Guia de referência do nmap: http://nmap.org/man/pt_BR/
2. Exemplos de comandos com suas explicações em http://nmap.org/man/pt_BR/man-examples.html
3. Segurança de Redes e Sistemas da RNP - http://pt.scribd.com/doc/57585030/Seguranca-de-Redes-e-Sistemas
4. Hacker High School: http://www.hackerhighschool.org/lessons.html
5. Material do Prof. João Bosco Mangueira Sobral