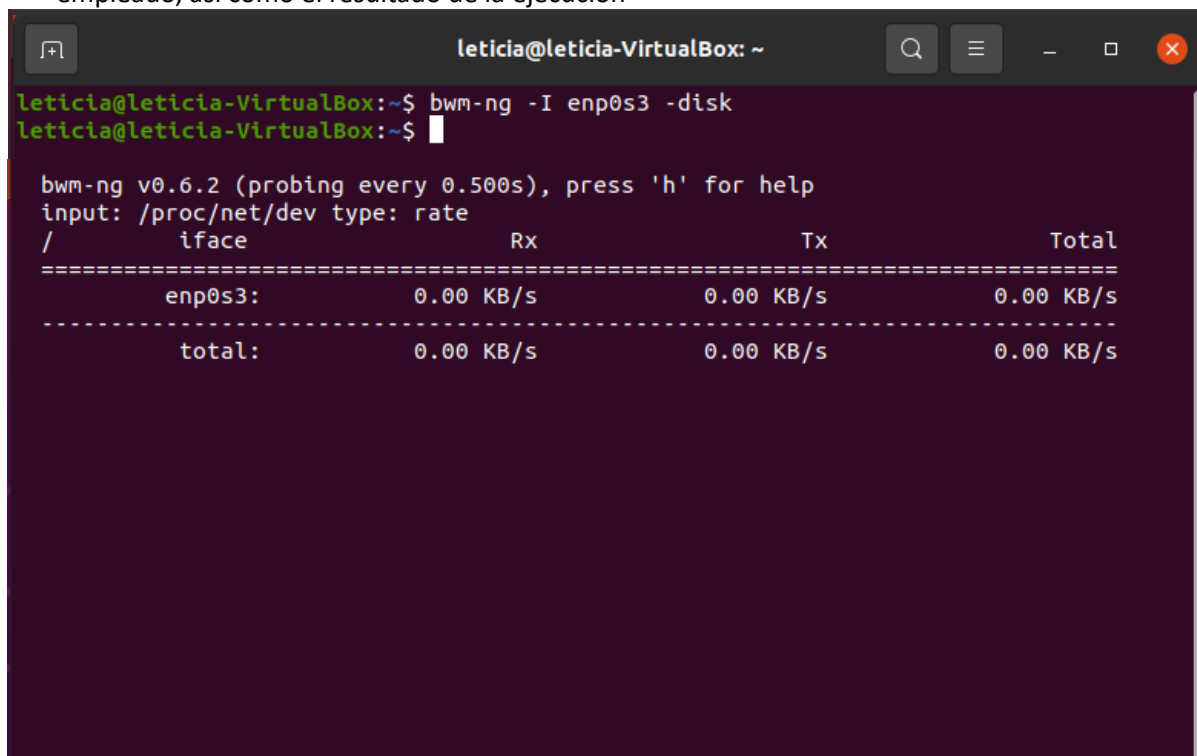




2. Monitoriza en tu interfaz de red los Kbs transferidos en el sistema de discos. Muestra el comando empleado, así como el resultado de la ejecución



```
leticia@leticia-VirtualBox: ~  
leticia@leticia-VirtualBox:~$ bwm-ng -I enp0s3 -disk  
leticia@leticia-VirtualBox:~$  
  
bwm-ng v0.6.2 (probing every 0.500s), press 'h' for help  
input: /proc/net/dev type: rate  
/  
=====
```

iface	Rx	Tx	Total
enp0s3:	0.00 KB/s	0.00 KB/s	0.00 KB/s
total:	0.00 KB/s	0.00 KB/s	0.00 KB/s

```
-----  
total: 0.00 KB/s 0.00 KB/s 0.00 KB/s
```

### **Ejercicio 2 (2 puntos)**

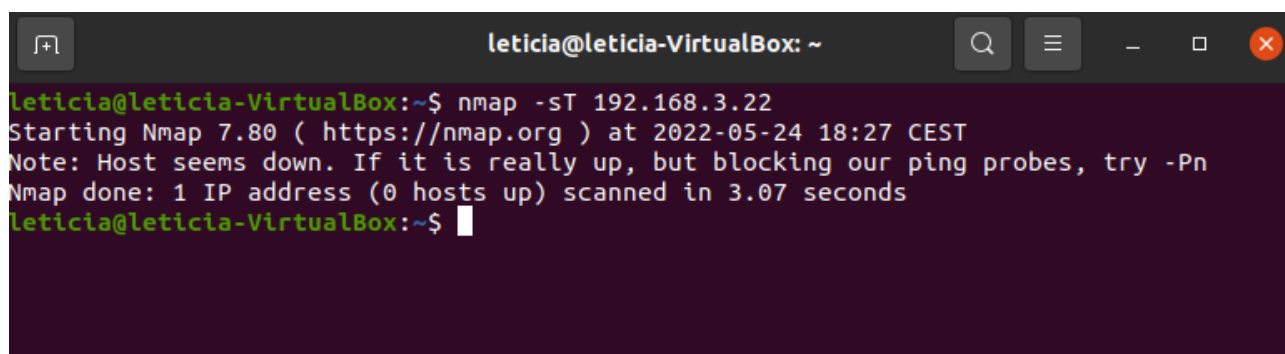
En esta tarea instalaremos la herramienta Microsoft Network Monitoring en Window  
Aplicaremos el filtro para que solo muestres aquellas IPs que son la de Google  
Indicar cómo aplicar el filtro y mostrar una captura de pantalla con el resultado del mismo

### **Ejercicio 3: Nmap (3 puntos)**

Instala Nmap en un equipo con Ubuntu y realiza los siguientes tipos de escaneos de puertos contra una máquina virtual con dir. IP 192.168.3.2X.

A continuación, copia los comandos empleados para cada uno de los escaneos, así como una captura con la salida del mismo

1. Escaneo tipo Connect



```
leticia@leticia-VirtualBox: ~  
leticia@leticia-VirtualBox:~$ nmap -sT 192.168.3.22  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-24 18:27 CEST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds  
leticia@leticia-VirtualBox:~$
```

## 2. Escaneo tipo TCP SYN 192.168.3.20

```
leticia@leticia-VirtualBox: ~  
leticia@leticia-VirtualBox:~$ sudo nmap -sS 192.168.3.22  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-24 18:29 CEST  
Nmap scan report for 192.168.3.22  
Host is up (0.027s latency).  
All 1000 scanned ports on 192.168.3.22 are filtered  
  
Nmap done: 1 IP address (1 host up) scanned in 16.03 seconds  
leticia@leticia-VirtualBox:~$
```

## 3. Escaneo tipo UDP (hacerlo contra la propia máquina)(sudo nmap -sN)

```
leticia@leticia-VirtualBox:~$ sudo nmap -sU 192.168.3.23  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-18 10:05 CEST  
Nmap scan report for leticia-VirtualBox (192.168.3.23)  
Host is up (0.0000040s latency).  
Not shown: 998 closed ports  
PORT      STATE      SERVICE  
631/udp   open|filtered ipp  
5353/udp  open|filtered zeroconf  
  
Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds  
leticia@leticia-VirtualBox:~$
```

## 4. Escaneo tipo Stealth FIN Scanning. (sudo nmap -sN)

```
leticia@leticia-VirtualBox:~$ sudo nmap -sN 192.168.3.22  
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-18 10:05 CEST  
Nmap scan report for 192.168.3.22  
Host is up (0.00022s latency).  
Not shown: 998 closed ports  
PORT      STATE      SERVICE  
111/tcp   open|filtered rpcbind  
2049/tcp  open|filtered nfs  
MAC Address: 08:00:27:73:AA:5C (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds  
leticia@leticia-VirtualBox:~$
```

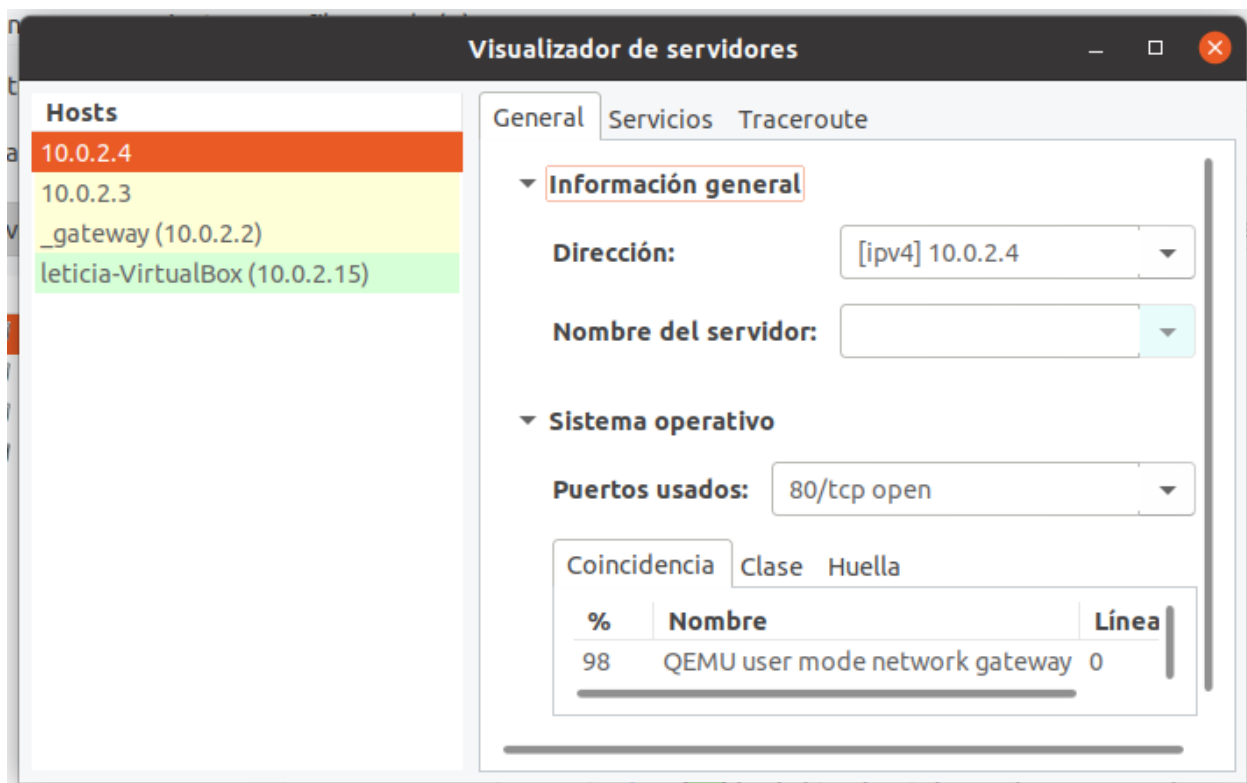
Básate en <http://paraisolinux.com/que-es-y-como-usar-nmap/>

**Ejercicio 4: Zenmap (3 puntos)**

En esta tarea escanearemos los puertos abiertos en los equipos de la red empleando la herramienta gráfica Zenmap (elige Ubuntu o Windows)

Instala la herramienta en uno de los sistemas operativos y muestra

- Los equipos activos



- Los servicios activos en alguno de los equipos

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: 10.0.2.15/24 Perfil: Intense scan Escaneo Cancelar

Comando: nmap -T4 -A -v 10.0.2.15/24

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

Servicio

- http
- http-proxy
- microsoft-ds
- msrpc
- ms-wbt-server
- vnc

Visualizador de servidores El efecto ojo de pez Controles

Leyenda Guardar gráfico

Acción

Interpolación

Plano

Vista

- ☒ address
- ☒ hostname

Navegación 225.0

Zoom 221

Huevo aro 30

Reducir hueco aro

Fisheye sobre el aro 1,00 con un factor de interés 2,01 y un factor de difusión 0,50



- La distribución gráfica de la red

