Índice:

Ejercicio 3

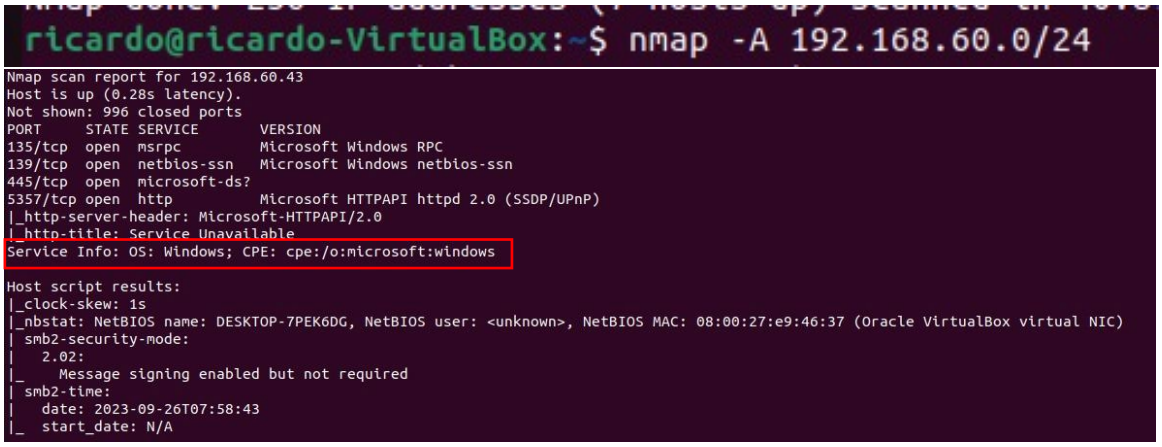
a) Barrido de ping

Solución:

IP del equipo Windows (Equipo amenazado)

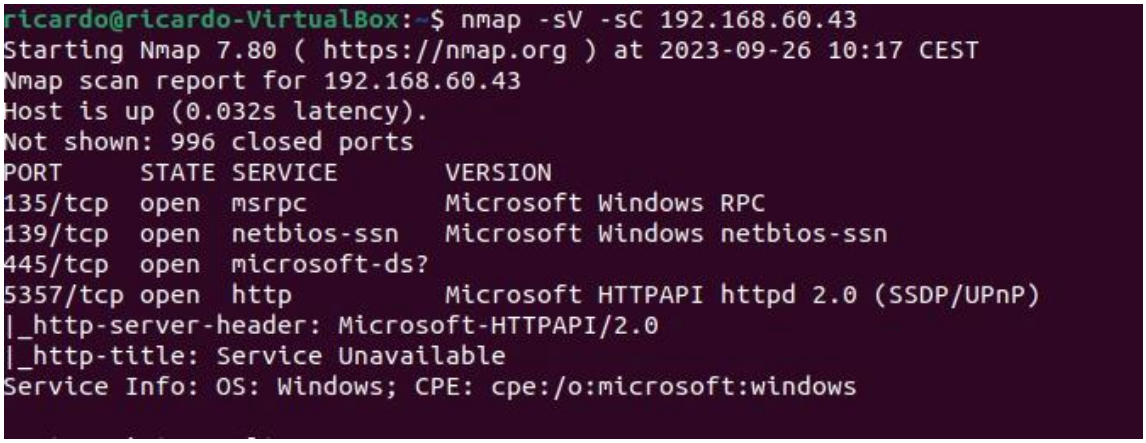
Escaneamos con nmap -A 192.168.60.0/24

Se puede ver que detecta que es un equipo Widows



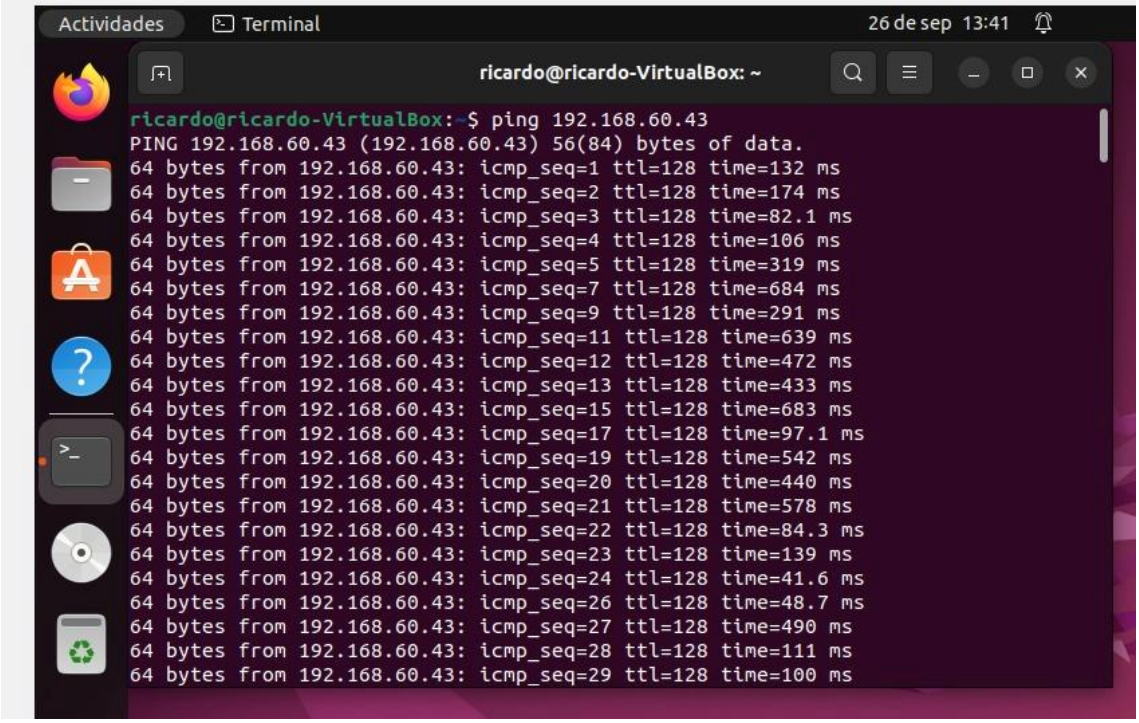
b) Visualizar puertos abiertos del equipo atacado

Solución:

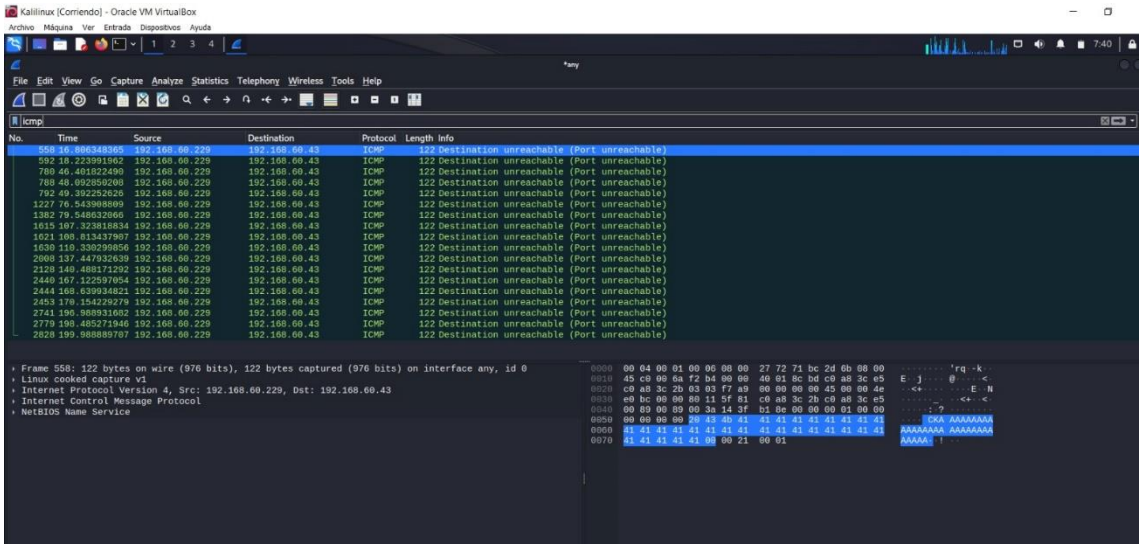


c) Captura los paquetes de la red

Creamos un flujo de paquetes ICMP con la máquina 1 a la 3



Y desde la maquina 2 Con Whire Shark capturamos los paquetes ICMP



d) Cerrar y abrir puertos en Linux y Windows

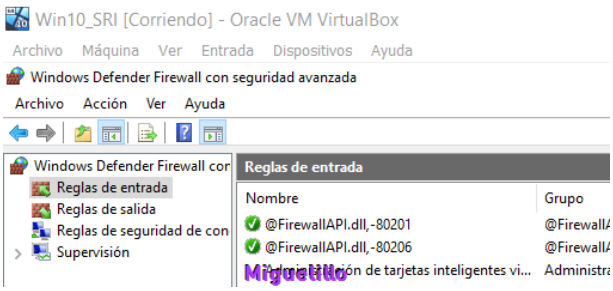
Solución:

Windows

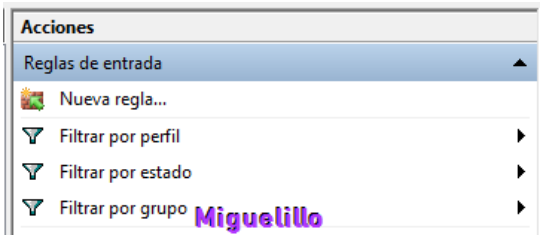
Para abrir y cerrar puertos en Windows

Vamos a **Panel de Control > Sistema y seguridad > Firewall de Windows Defender > Configuración Avanzada**

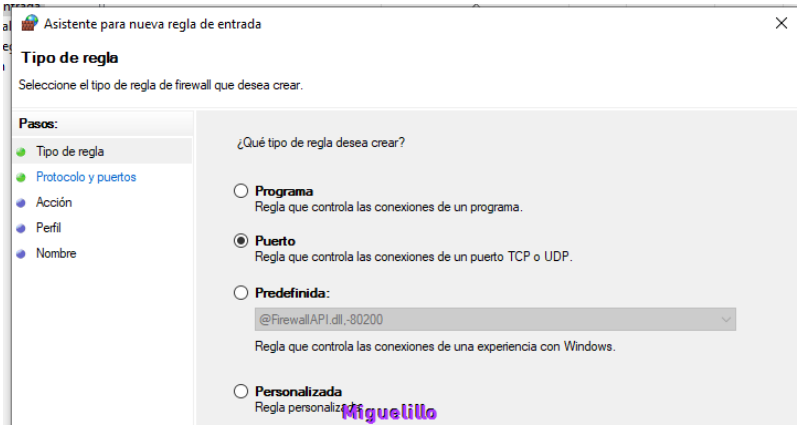
Una vez aquí podemos elegir entre reglas de entrada o de salida, dependiendo de si queremos activar o desactivar el puerto con un servicio que intente entrar o uno que quiera salir.



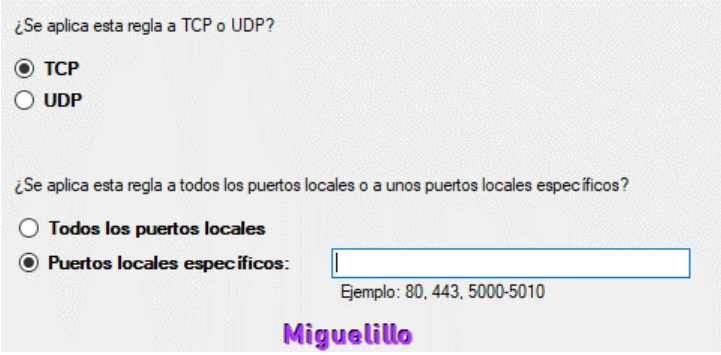
Seleccionamos por ejemplo Reglas de entrada y Clicamos en **Nueva Regla…**



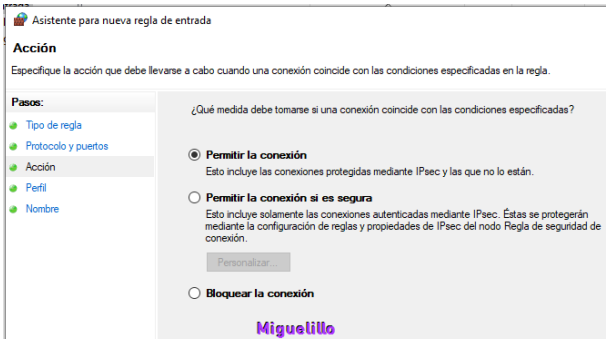
Seleccionamos **Puerto**



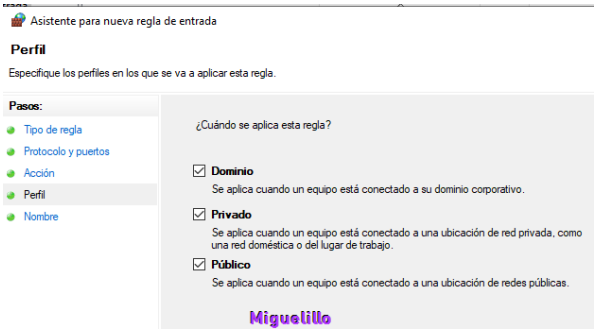
Especificamos si es TCP o UDP y el número de puerto que queremos abrir o cerrar



Decimos si queremos permitir o bloquear el puerto



Declaramos en que perfil de red queremos



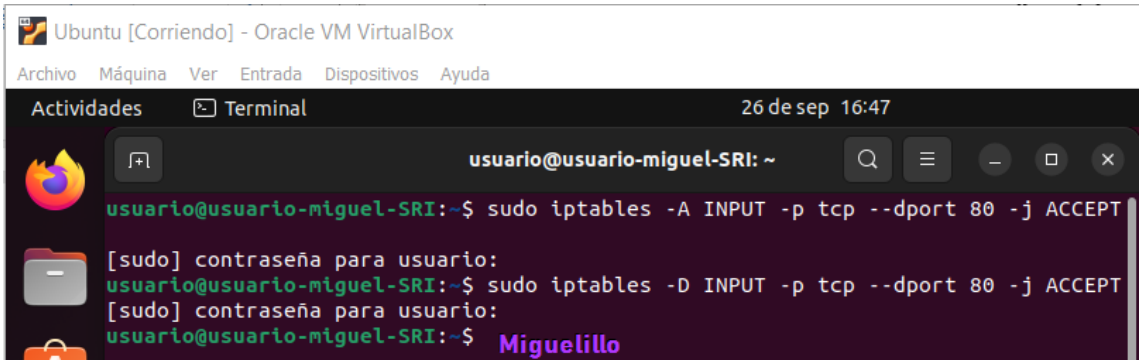
LINUX

Para abrir un puerto utilizaremos este comando dónde con **-A** indicamos que crearemos una **regla nueva** y pondremos **OUTPUT** o **INPUT** según si queremos que sea la regla de **entrada** o de **salida**, **-p** para especificar **tcp** o **udp**, con **--dport** especificamos el puerto en este caso el **80** y con **-j** especificamos si queremos **admitir** el tráfico con **ACCEPT**, **bloquearlo** sin dar mensaje de error con **DROP** o **bloquearlo** dando un **mensaje** de **error** con **REJECT**.

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Si queremos **desactivar** el **puerto** simplemente tendremos que **borra** la **regla** configurada ya que si la borras por **defecto** los puertos están **desactivados**. La opción para borrar la regla es **-D**

```
iptables -D INPUT -p tcp --dport 80 -j ACCEPT
```



e) Para detectar sniffers

Solución:

Para detectar sniffers en la red no he encontrado ninguna herramienta específica, pero a nivel interno si que existen herramientas que los detectan como medida de protección como puede ser un Antivirus. He encontrado programas con los cual puedes evitar los sniffers como son las VPN estas se encargan de cifrar tus mensajes y que no sean visibles en texto claro, por lo cual si un paquete cae en manos de un sniffer no pueda leerlo.