

6.- nmap

`sudo nmap [parámetros] [dominio|IP/mascara] → muestra puertos abiertos`

- sV: open ports to determine service/version info
- sn: omit the default port scan
- Pn: Cuando sabemos que el host está activo. (útil para traceroute)
- traceroute: Muestra el salto de servers hasta el destino
- O: Muestra el SO

⇒obtener máquinas en la red:

```
$ ip addr → obtener ip/máscara
$ sudo nmap -sn [ip/máscara]
```

- OBTENER PUERTOS ABIERTOS E INFO DE UN DOMINIO (VERSIÓN/ESTADO)
- OBTENER RUTA DE PAQUETES (SALTOS DE h.ORIGEN--h.DESTINO)
- OBTENER PUERTOS DE MÁQUINAS ACTIVAS DE UNA RED
- OBTENER SISTEMA OPERATIVO DE UNA MÁQUINA

7.- iptables ([link](#))

Actúa de firewall ya que se encarga de filtrar los paquetes de datos que entran/salen.

```
$ sudo iptables-save > /home/alumno/Escritorio/fichero
$ sudo iptables-restore < /home/alumno/Escritorio/fichero
```

Posibles reglas para los paquetes:

- **ACCEPT:** El paquete será aceptado.
- **DROP/REJECT:** El paquete será descartado. Reject avisa de la circunstancia.
- **QUEUE:** Mueve el paquete a los procesos de usuario y requiere un intermediario (queue handler) que reenvía todos los paquetes a una aplicación.
- **RETURN:** El paquete se envía de nuevo a la cadena anterior en caso de que esta haya sido definida por el usuario. Las cadenas estándar se guían por la directriz (policy) de la cadena (por defecto y sin necesidad de configuración: ACCEPT).

Tipos de paquetes

- **INPUT:** Procesa paquetes entrantes al sistema
- **FORWARD:** Procesa los paquetes de datos entrantes que van a ser enviados
- **OUTPUT:** Controla el tráfico saliente generado.

Comando iptables	Ejemplo	Explicación
-N "Nombre de la cadena"	sudo iptables -N test	Crea una nueva cadena con el nombre "test".
-X "Nombre de la cadena"	sudo iptables -X test	Elimina la cadena vacía con el nombre "test"; no funciona con las cadenas INPUT, OUTPUT y FORWARD.
-L "Nombre de la cadena"	sudo iptables -L test	Muestra la lista de las reglas de la cadena con nombre "test".
-F "Nombre de la cadena"	sudo iptables -F test	Elimina todas las reglas de la cadena con nombre "test".
-P "Nombre de la cadena" "Acción"	sudo iptables -P INPUT ACCEPT	Establece las directrices de la cadena. En el ejemplo, el paquete es aceptado de forma automática cuando no se aplican las reglas de filtrado de la cadena INPUT.
-A "Nombre de la cadena" "Regla"	sudo iptables -A test -s 127.0.0.1 -j DROP	Añade una nueva regla a la cadena seleccionada. En el ejemplo, se agrega una regla a la cadena "test" para que descarte los paquetes provenientes de la dirección IP 127.0.0.1.
-D "Nombre de la cadena" "Regla"	sudo iptables -D test -s 127.0.0.1 -j DROP	Elimina la regla de la cadena seleccionada.
-I "Nombre de la cadena" "Position" "Regla"	sudo iptables -I test 1 -s 127.0.0.1 -j DROP	Añade una nueva regla a la cadena en la posición determinada; en el ejemplo es la posición 1.
-D "Nombre de la cadena" "Posición"	sudo iptables -D test 1	Elimina la regla de la cadena seleccionada mediante la especificación de la posición de la regla; en este ejemplo también es la posición 1.

Parámetros comunes:

- A: Añadir una nueva regla a la cadena seleccionada (INPUT/OUTPUT)
- s: Especifica el origen (ip o dirección) [solo para **INPUT**]
- i: Interfaz (dispositivo físico) de entrada [solo para **INPUT**]
- d: Especifica el destino(ip o dirección) [solo para **OUTPUT**]
- o: Interfaz (dispositivo físico) de salida [solo para **OUTPUT**]
FORWARD puede tener ambos parametros -i y -o
- p: protocolo usado (tcp,icmp,udp...)
- dport: puerto de DESTINO
- sport: puerto de ORIGEN
- j: Acción que se desea que realice (ACCEPT, FORWARD, DROP)

borrar todas las reglas existentes

```
sudo iptables -F
```

bloquear por defecto todos los paquetes

```
sudo iptables -P INPUT DROP
sudo iptables -P OUTPUT DROP
sudo iptables -P FORWARD DROP
```

Bloquear por defecto todos paquetes excepto localhost

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT
```

Aceptar paquetes de cierta ip

```
sudo iptables -A INPUT -s [dominio|ip] -j ACCEPT
sudo iptables -A OUTPUT -d [dominio|ip] -j ACCEPT
```

Habilita las conexiones HTTP y HTTPS salientes (puerto 80 y puerto 443) para los puertos de acceso 1024 a 65535:

```
sudo iptables -A OUTPUT -o eth0 -p tcp --dport 80 --sport 1024:65535 -j ACCEPT
sudo iptables -A OUTPUT -o eth0 -p tcp --dport 443 --sport 1024:65535 -j ACCEPT
```

<code>`INPUT'</code>	<code>`test'</code>
-----	-----
Rule1: -p ICMP -j DROP	Rule1: -s 192.168.1.1
-----	-----
Rule2: -p TCP -j test	Rule2: -d 192.168.1.1
-----	-----
Rule3: -p UDP -j DROP	

<https://www.ionos.es/digitalguide/servidores/herramientas/iptables-conoce-las-reglas-para-crear-paquetes-de-datos/>

<http://redesdecomputadores.umh.es/iptables.htm>