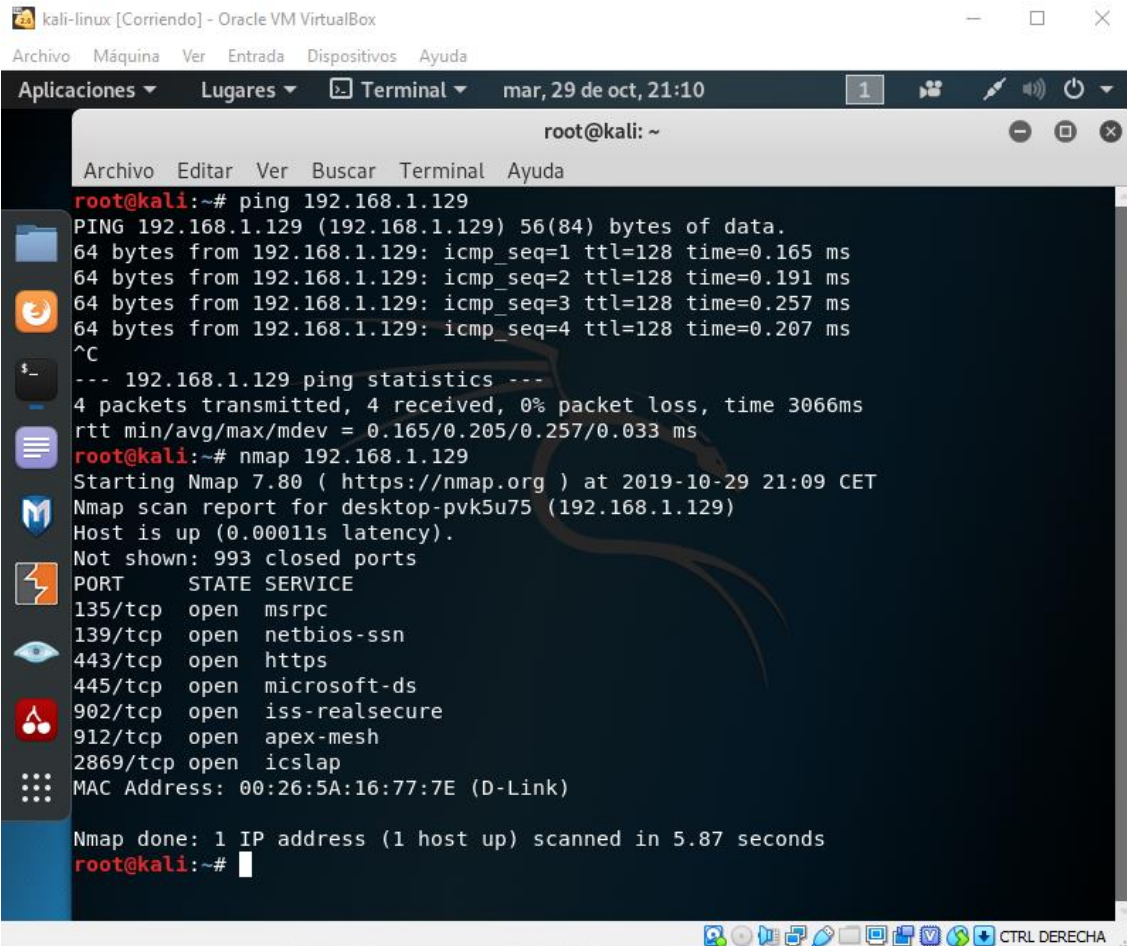


## Herramienta 1. NMAP

Nmap es una herramienta que sirve para escanear redes y permite identificar que servicios se están ejecutando en un dispositivo remoto, identificación de equipos activos, sistemas operativos en el equipo, existencia de filtros o firewalls entre otros...

Un comando sencillo sería nmap "la ip objetivo" :



```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# ping 192.168.1.129  
PING 192.168.1.129 (192.168.1.129) 56(84) bytes of data.  
64 bytes from 192.168.1.129: icmp_seq=1 ttl=128 time=0.165 ms  
64 bytes from 192.168.1.129: icmp_seq=2 ttl=128 time=0.191 ms  
64 bytes from 192.168.1.129: icmp_seq=3 ttl=128 time=0.257 ms  
64 bytes from 192.168.1.129: icmp_seq=4 ttl=128 time=0.207 ms  
^C  
--- 192.168.1.129 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3066ms  
rtt min/avg/max/mdev = 0.165/0.205/0.257/0.033 ms  
root@kali:~# nmap 192.168.1.129  
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-29 21:09 CET  
Nmap scan report for desktop-pvk5u75 (192.168.1.129)  
Host is up (0.00011s latency).  
Not shown: 993 closed ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
2869/tcp  open  iclap  
MAC Address: 00:26:5A:16:77:7E (D-Link)  
  
Nmap done: 1 IP address (1 host up) scanned in 5.87 seconds  
root@kali:~#
```

Aquí he hecho un nmap a la IP de mi pc, en el se muestran los puertos que tengo abiertos, hay varios comandos para hacer otro tipo de cosas como mostrar el sistema operativo del equipo, especificar los puertos que se desean escanear, escaneo omitiendo el ping, etc..

Aquí la página oficial : <http://nmap.org/>