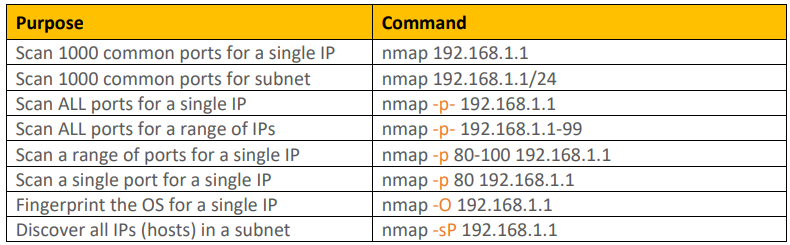
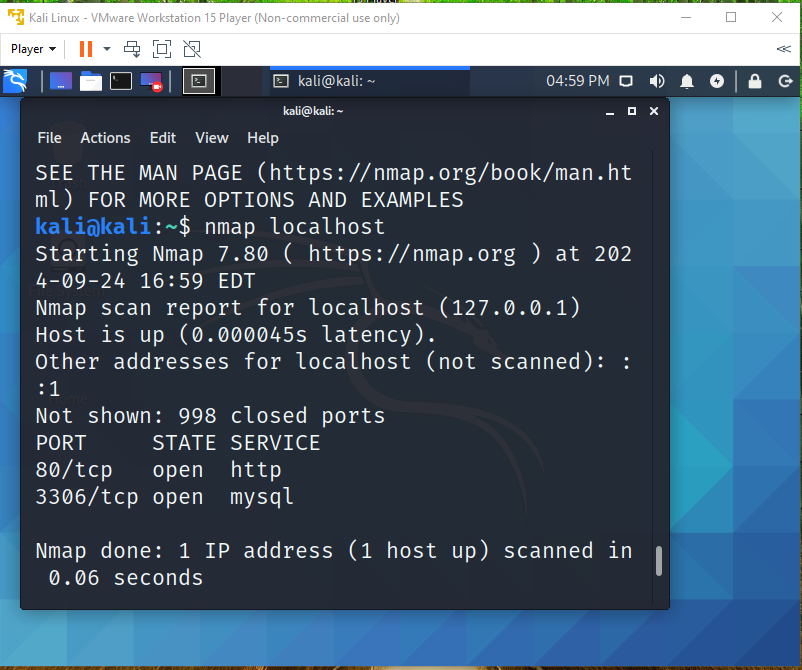
**PORT SCANNING**

****

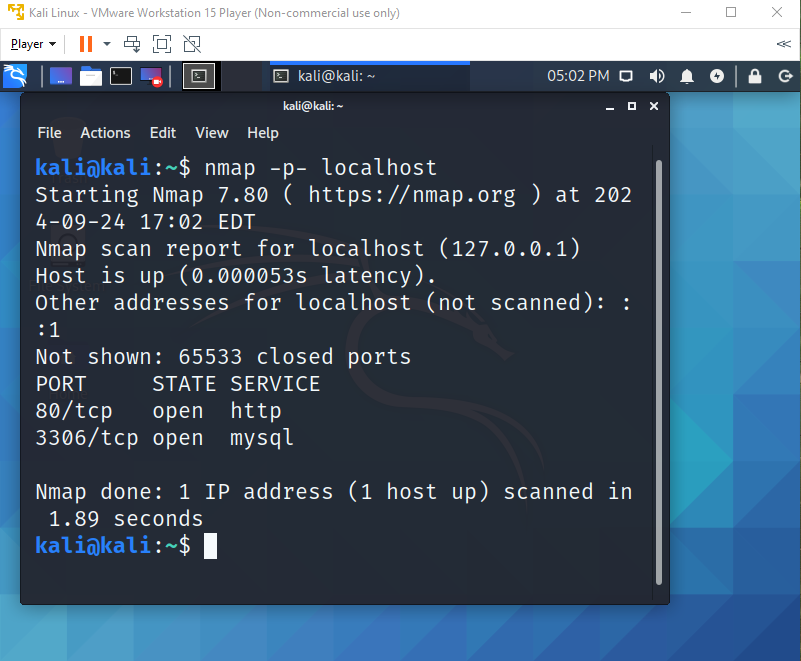
Scan 1000 common ports of your own system;

**nmap localhost**



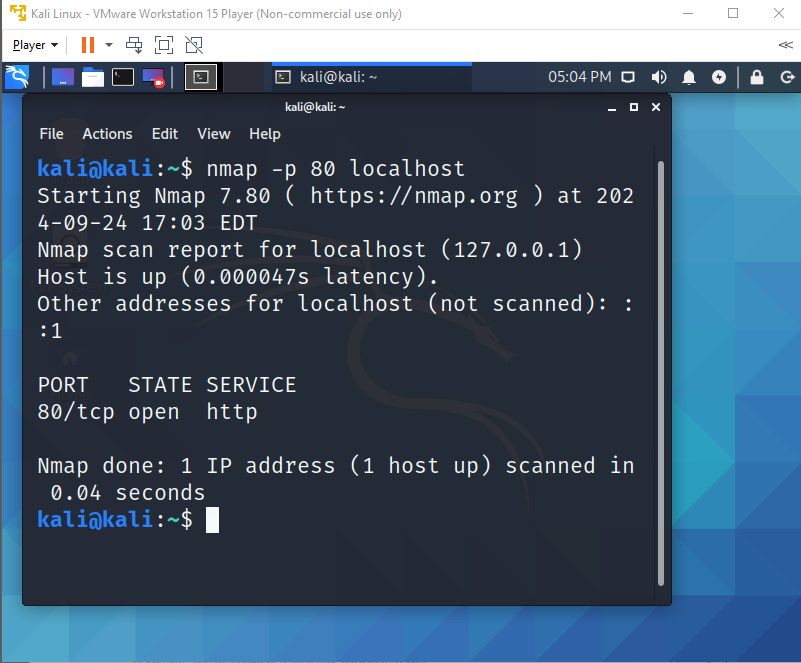
Scan ALL Ports

**nmap -p- localhost**



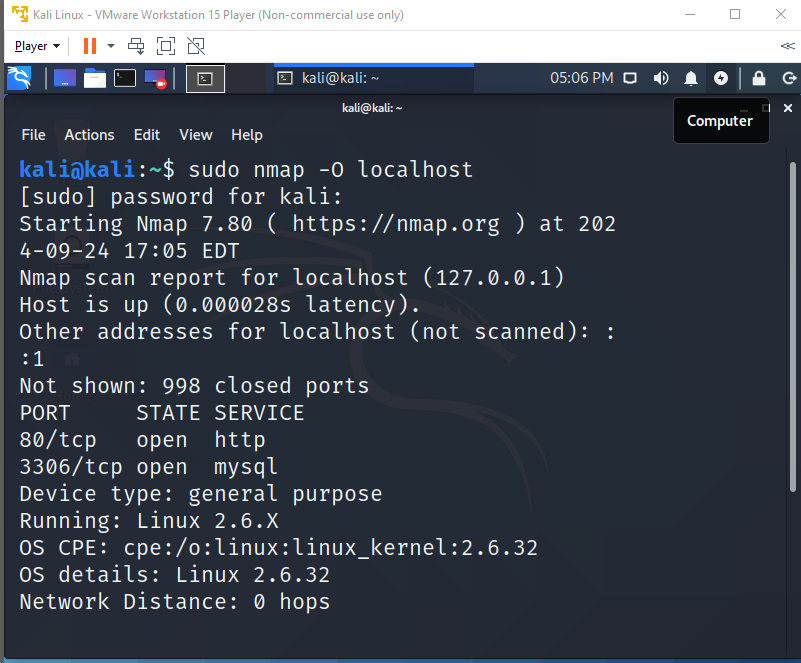
Scan Port 80

**nmap -p 80 localhost**



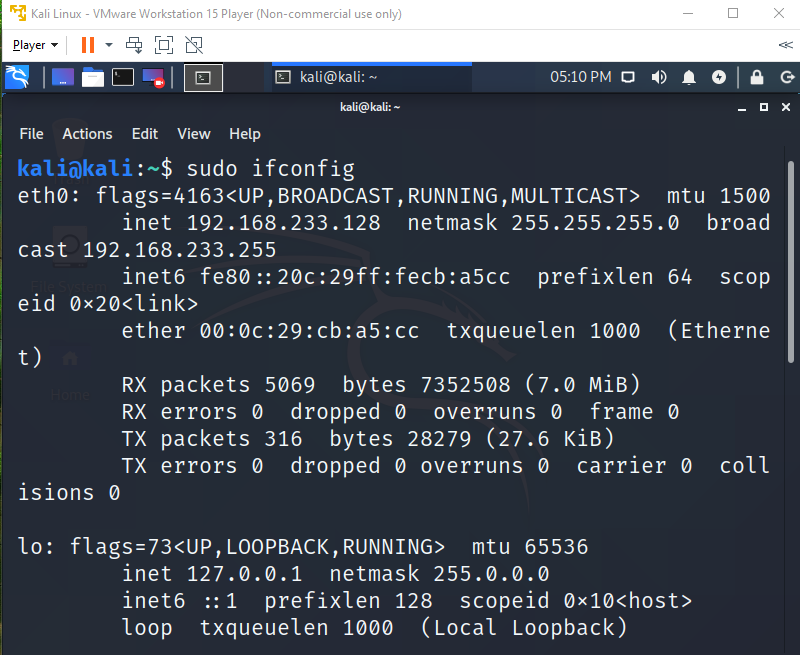
Fingerprint the Operating System

sudo nmap -O localhost (sudo for elevated privileges)



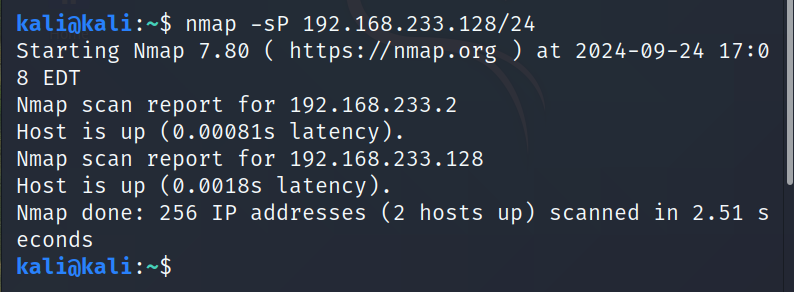
Continue fingerprint; find out the IP Address of the Ethernet Card that the VMWare machine is using.  
Issue the following command: ***ifconfig***

sudo ifconfig

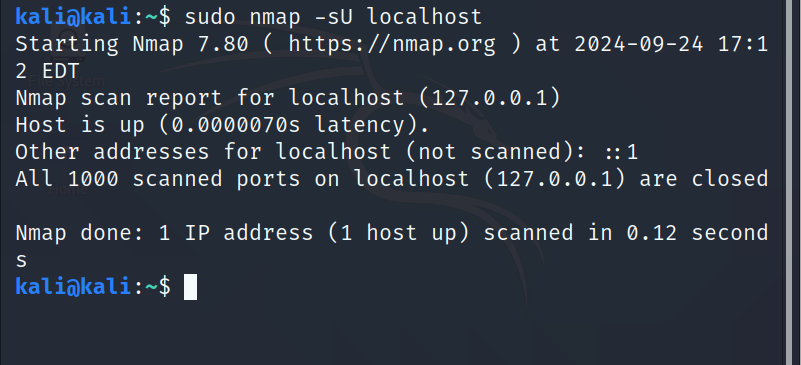


Discover all the IP Address within the subnet **nmap -sP [the IP Address \*192.168.233.128/24\*]** (/24 is its’ mask 255.255.255.0)

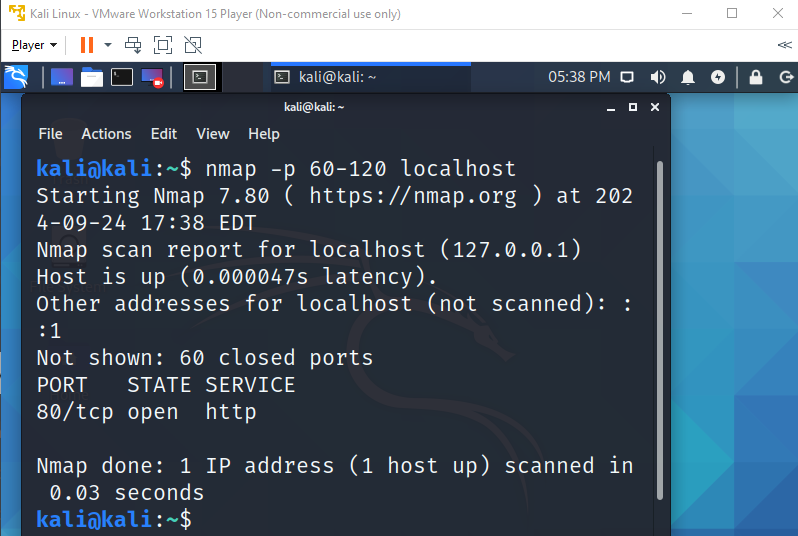
\*sP is for ping sweep or ping scan to discover all the IP address within the subnet



\*Will display all the host which are running



Scan port range 60-120



Scan for telnet port (24), scan only a single port

