Course Code : CSL604 **Course Name : System Security Lab**

Class : TE-CO **Batch : Computer Engineering**

Roll no : 18CO63 **Name : SHAIKH TAUSEEF MUSHTAQUE ALI**

Experiment : 07

Aim : Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.

Theory :

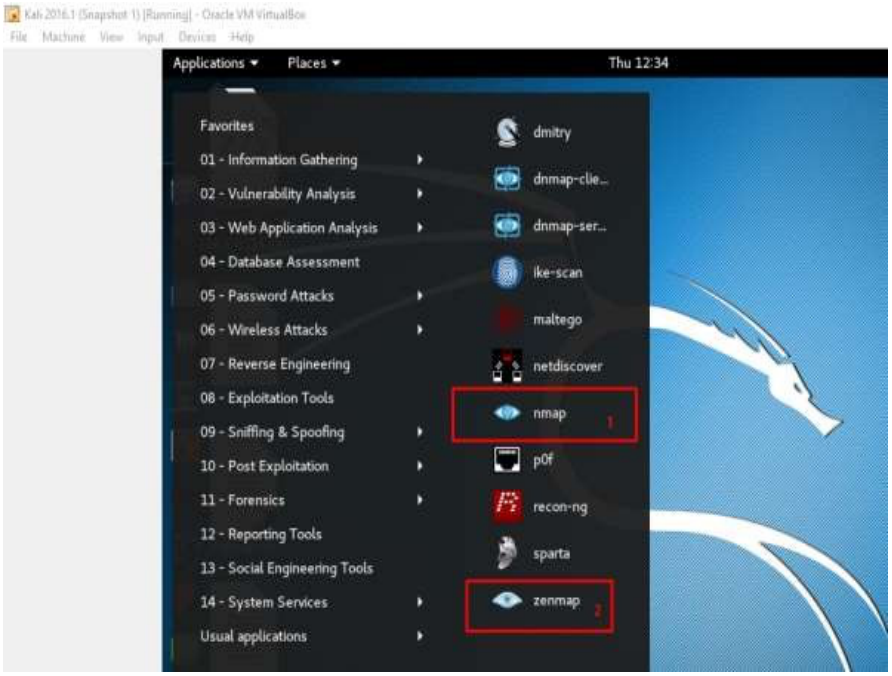
NMAPandZenMAP

NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

NMAP uses raw IP packets in novel ways to determine which hosts are available on the network, what services (application name and version) those hosts are offering, which operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, etc.

Now, let's go step by step and learn how to use NMAP and ZenMAP.



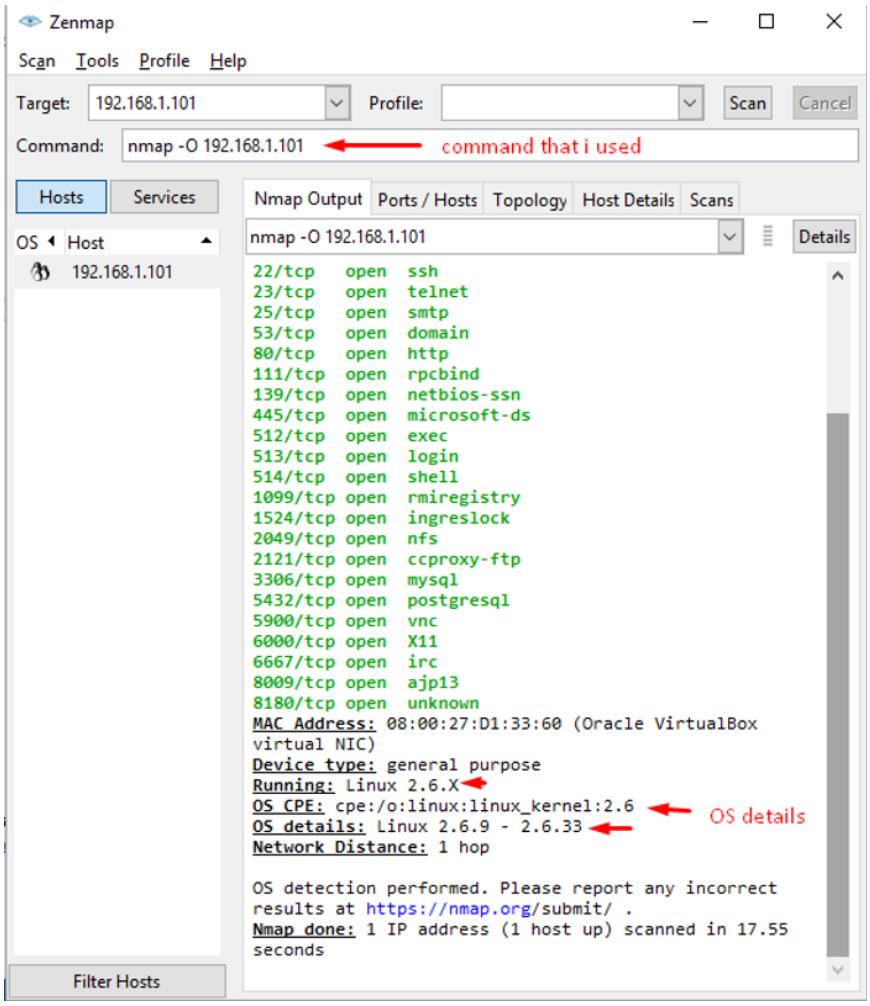
Step 1: To open, go to Applications -> 01-Information Gathering -> nmap or zenmap.

Step 2: The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable "-O". For more information, use this link: https://nmap.org/book/man-os-detection.html

The command that we will use is:

```
nmap –O 192.168.1.101
```

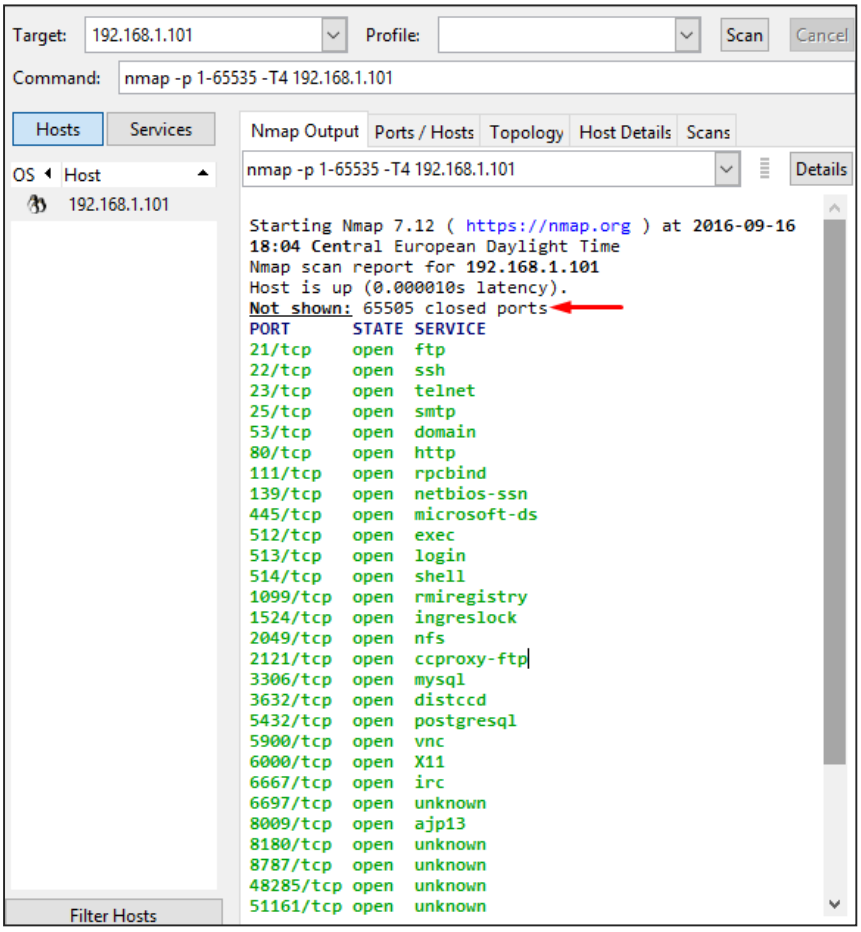
The following screenshot shows where you need to type the above command to see the Nmap output:



Step 3: Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP, use the following command:

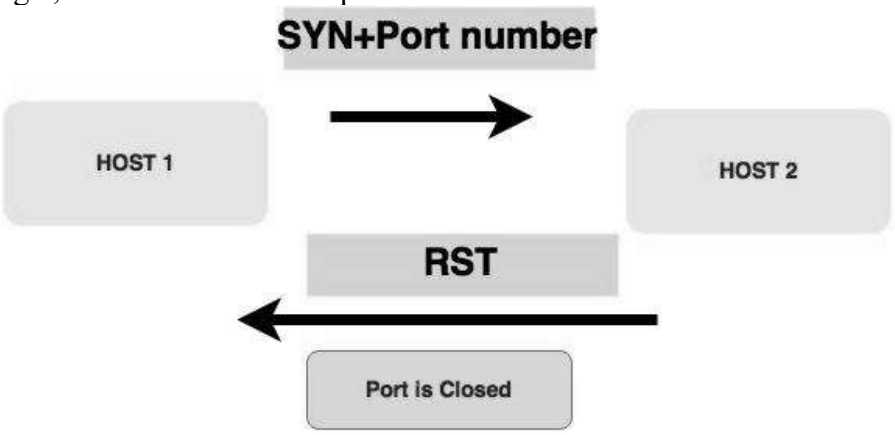
```
nmap –p 1–65535 –T4  192.168.1.101
```

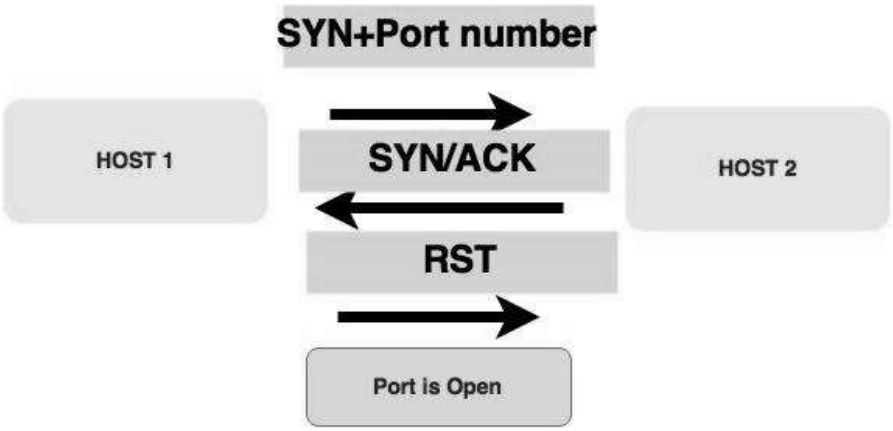
Where the parameter "–p" indicates all the TCP ports that have to be scanned. In this case, we are scanning all the ports and "-T4" is the speed of scanning at which NMAP has to run.
Following are the results. In green are all the TCP open ports and in red are all the closed ports. However, NMAP does not show as the list is too long.



StealthScan

Stealth scan or SYN is also known as **half-open scan**, as it doesn't complete the TCP three-way handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it is assumed the port isn't active or is closed.

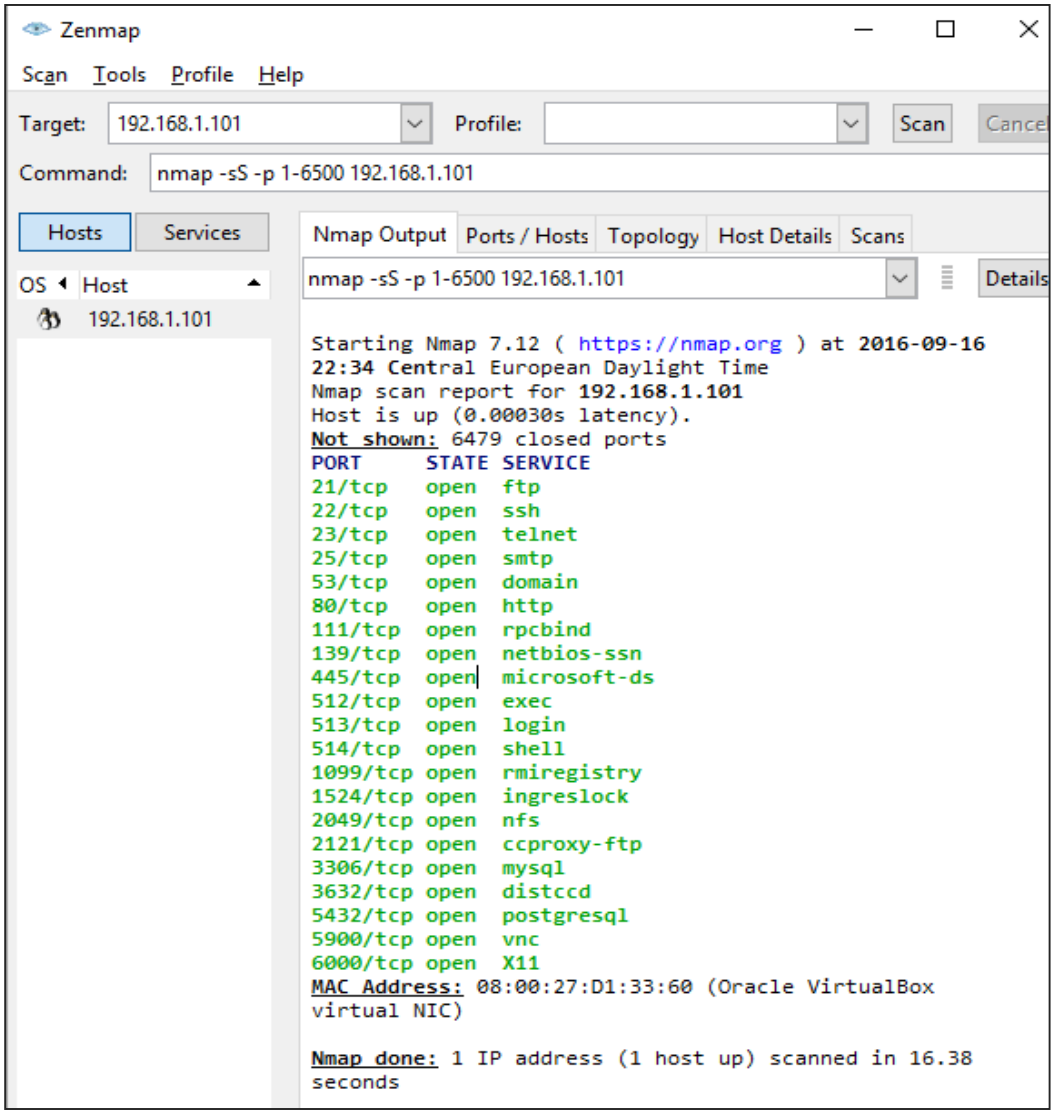




Now to see the SYN scan in practice, use the parameter **–sS** in NMAP. Following is the full command –

```
nmap –sS –T4 192.168.1.101
```

The following screenshot shows how to use this command:



Conclusion:

Used different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port
scan, xmas scan etc. by downloading nmap.