**EXPERIMENT-2**

**NMAP SCAN**

**AIM:**

To install and perform Nmap scan (note :- you may use ip address or website name).

**PROCEDURE:**

* Open Nmap from Kali Linux (Goto Applications->select Information Gathering->select Nmap).
* Perform different types of scan (Tcp, Udp, Ack, Syn, Fin, Null, Xmas, Rpc, Idle)- scan types.
* To perform host discovery.

|  |  |  |
| --- | --- | --- |
| -Pn | only port scan | nmap -Pn192.168.1.1 |
| -sn | only host discover | nmap -sn192.168.1.1 |
| -PR | arp discovery on a local network | nmap -PR192.168.1.1 |
| -n | disable DNS resolution | nmap -n 192.168.1.1 |

* Port specification.

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Example** |
| **-p** | **specify a port or port range** | **nmap -p 1-30 192.168.1.1** |
| **-p-** | **scan all ports** | **nmap -p- 192.168.1.1** |
| **F** | **fast port scan** | **nmap -F 192.168.1.1** |

* Service version and OS Detection.

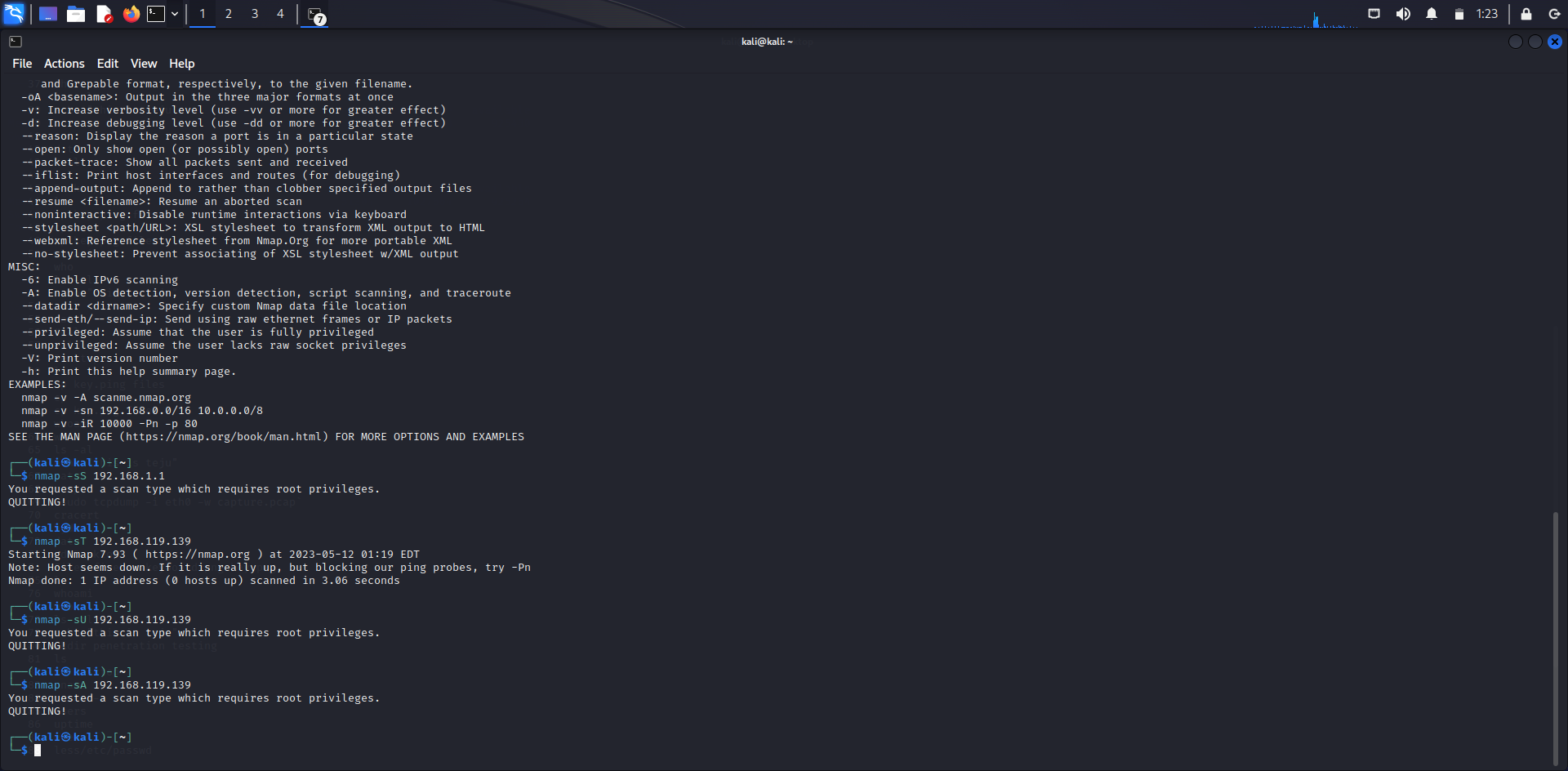
|  |  |  |
| --- | --- | --- |
| Flag | Use | Example |
| -sV | detect the version of services running | nmap -sV 192.168.1.1 |
| -A | aggressive scan | nmap -A 192.168.1.1 |
| -O | detect operating system of the target | nmap -O 192.168.1.1 |

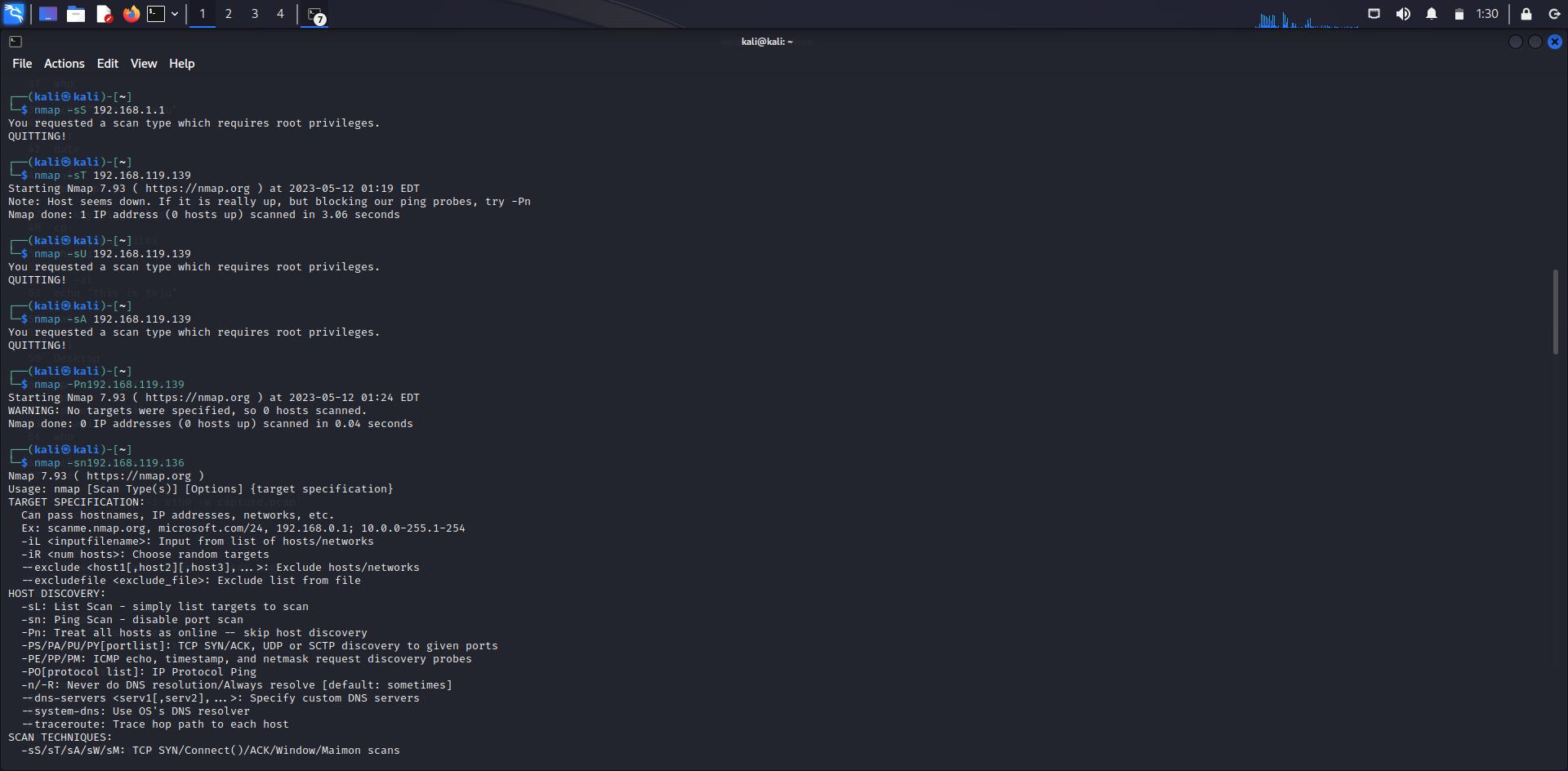
* Timing and performance.

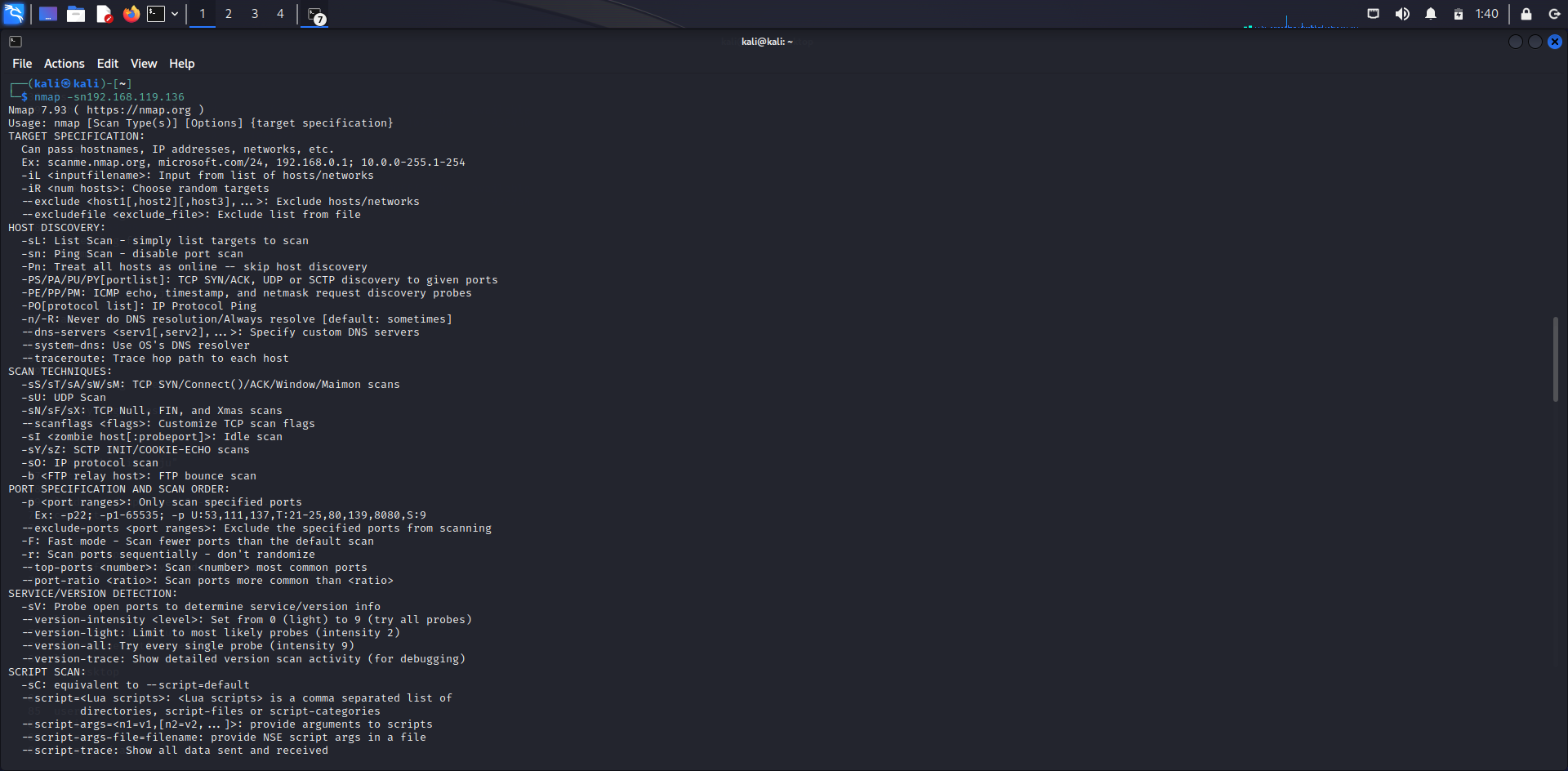
|  |  |  |
| --- | --- | --- |
| Flag | Use | Example |
| -T0 | paranoid IDS evasion | nmap -T0 192.168.1.1 |
| -T1 | sneaky IDS evasion | nmap -T1 192.168.1.1 |
| -T2 | polite IDS evasion | nmap -T2 192.168.1.1 |
| -T3 | normal IDS evasion | nmap -T3 192.168.1.1 |
| -T4 | aggressive speed scan | nmap -T4 192.168.1.1 |
| -T5 | insane speed scan | nmap -T5 192.168.1.1 |

**OUTPUT:**

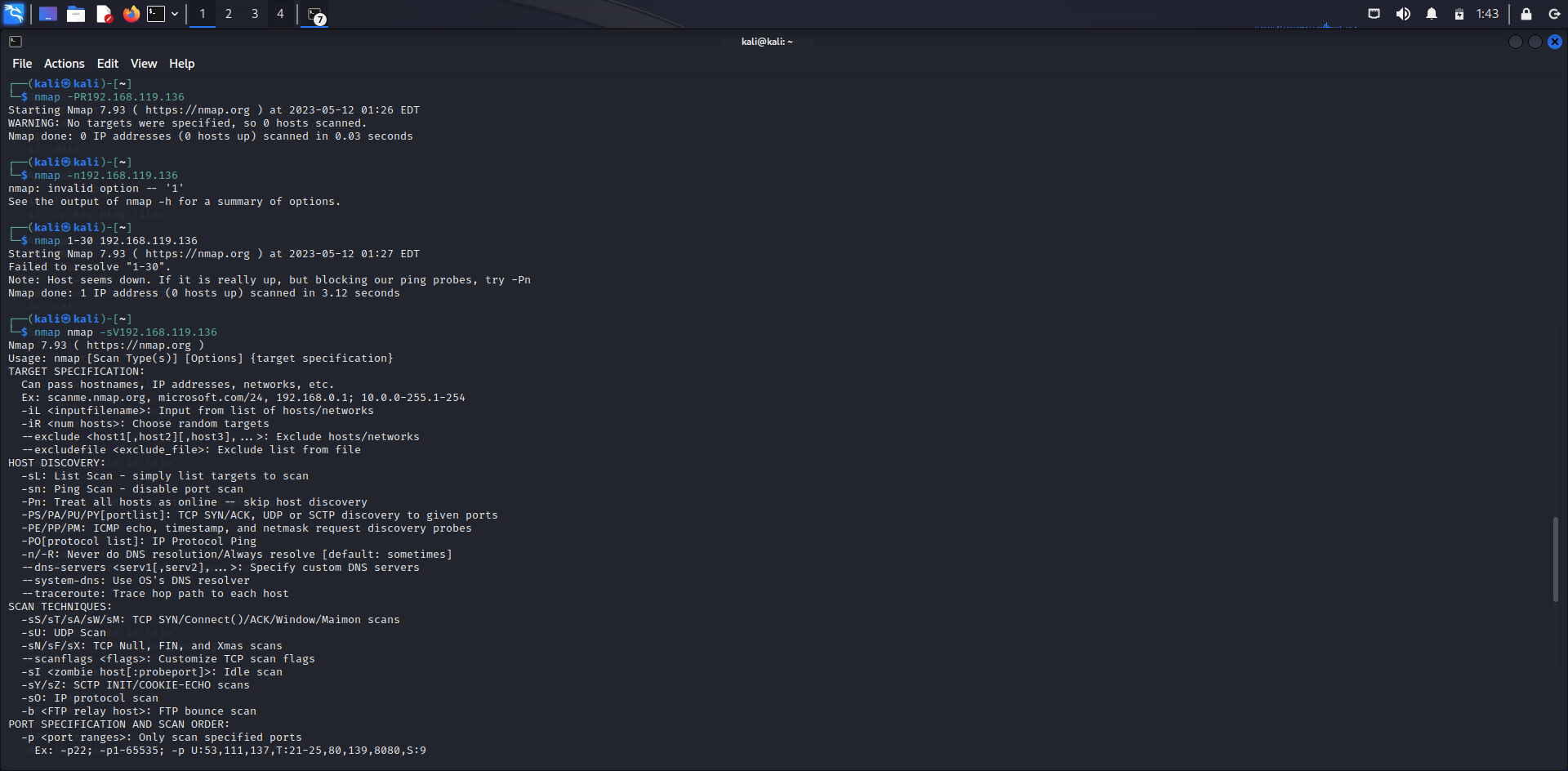
****

****

****

****

****

****

****

****

**RESULT:**

Installation and performing the Nmap has successfully done.