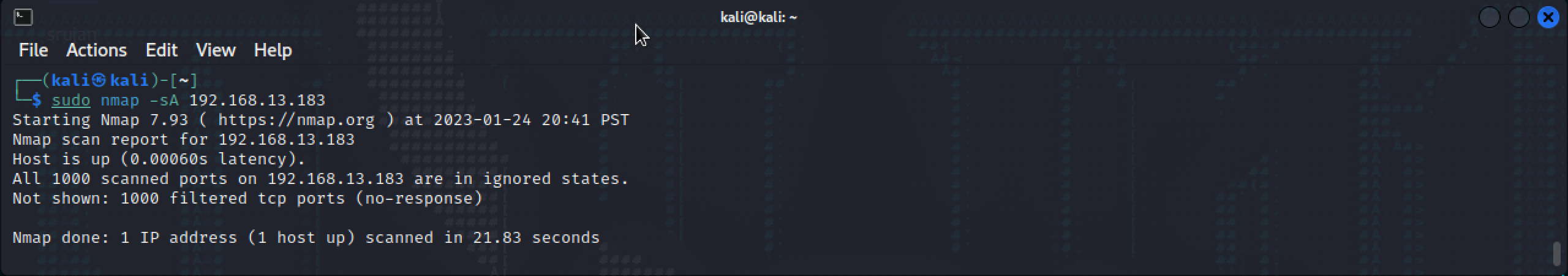
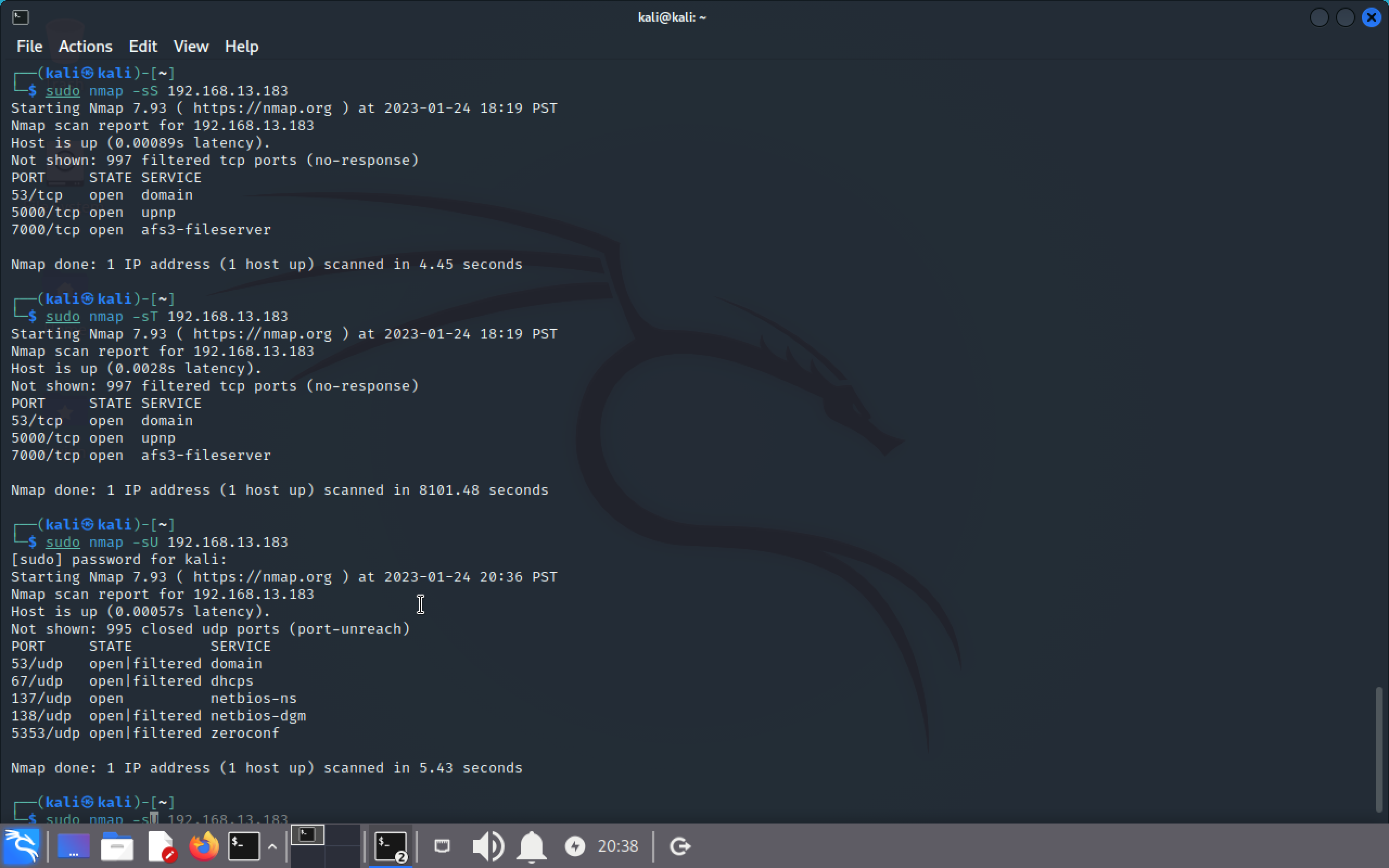
NMAP SCAN

EXERCISE-1

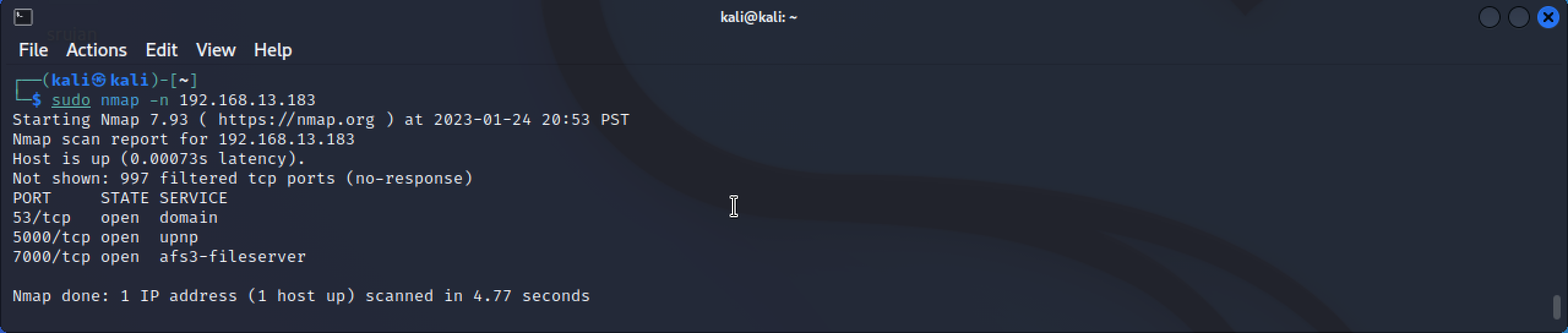
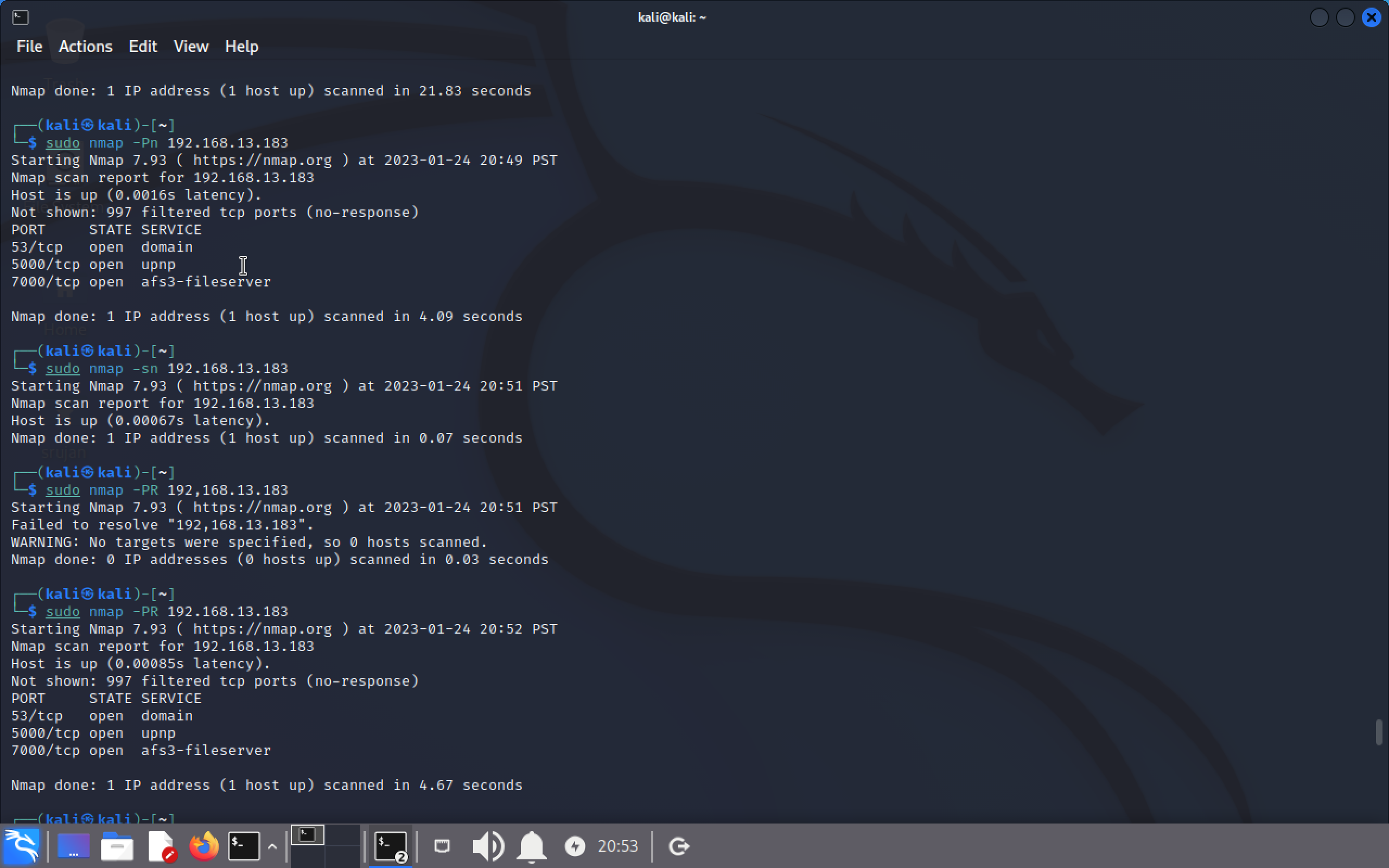
**Scanning Techniques**

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Command** |
| **-sS** | **TCP syn port scan** | **nmap -sS 192.168.13.183** |
| **-sT** | **TCP connect port scan** | **nmap -sT 192.168.13.183** |
| **–sU** | **UDP port scan** | **nmap –sU 192.168.13.183** |
| **–sA** | **TCP ack port scan** | **nmap –sA 192.168.13.183** |

**OUTPUT:**

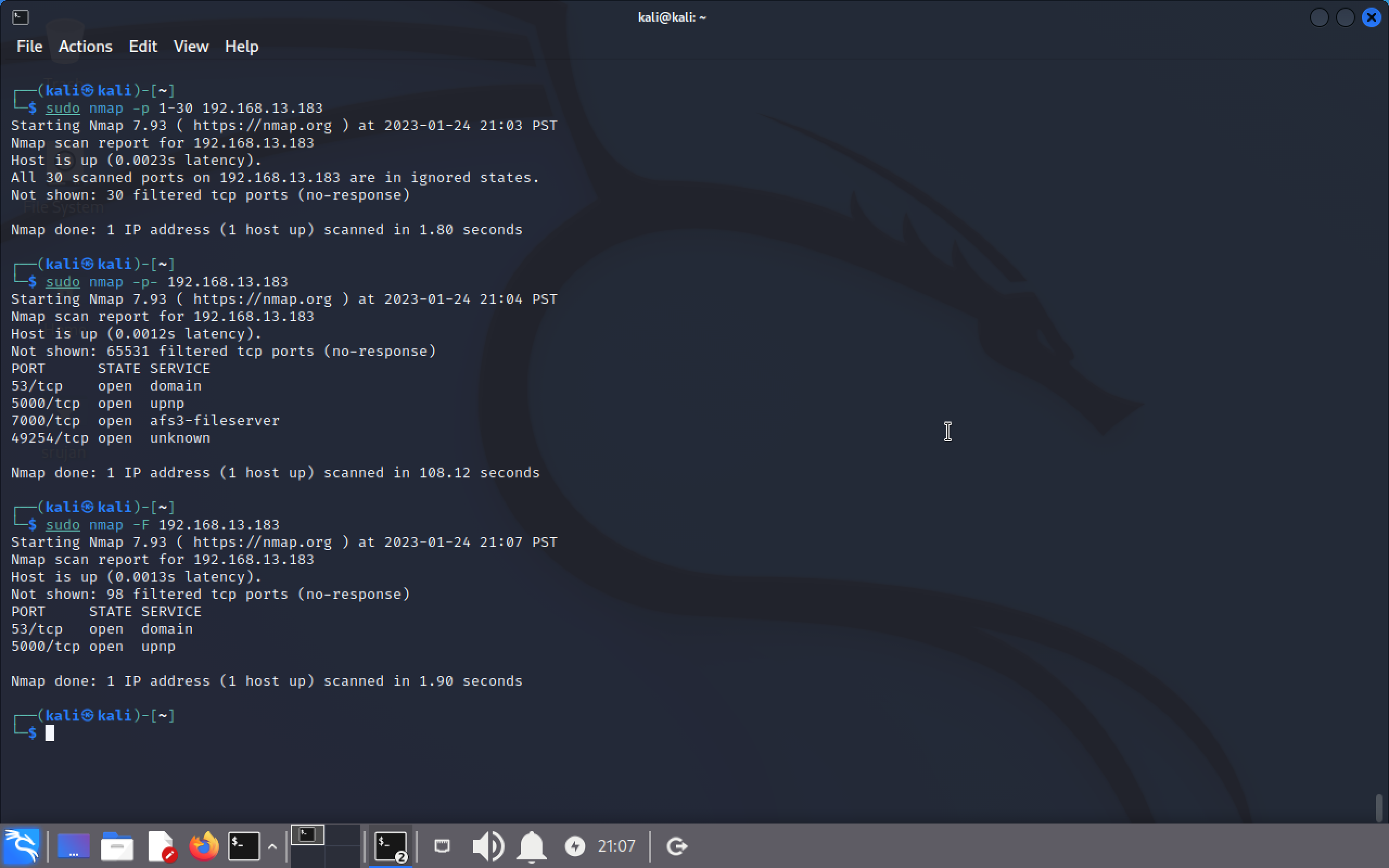
**Host Discovery**

|  |  |  |
| --- | --- | --- |
| -Pn | only port scan | nmap -Pn192.168.13.183 |
| -sn | only host discover | nmap -sn192.168.13.183 |
| -PR | arp discovery on a local network | nmap -PR192.168.13.183 |
| -n | disable DNS resolution | nmap -n 192.168.13.183 |

**OUTPUT:**

**Port Specification**

|  |  |  |
| --- | --- | --- |
| **Flag** | **Use** | **Command** |
| **-p** | **specify a port or port range** | **nmap -p 1-30 192.168.13.183** |
| **-p-** | **scan all ports** | **nmap -p- 192.168.13.183** |
| **F** | **fast port scan** | **nmap -F 192.168.13.183** |

**OUTPUT:**

***Service Version and OS Detection***

|  |  |  |
| --- | --- | --- |
| Flag | Use | Command |
| -sV | detect the version of services running | nmap -sV 192.168.13.183 |
| -A | aggressive scan | nmap -A 192.168.13.183 |
| -O | detect operating system of the target | nmap -O 192.168.13.183 |

OUTPUT: