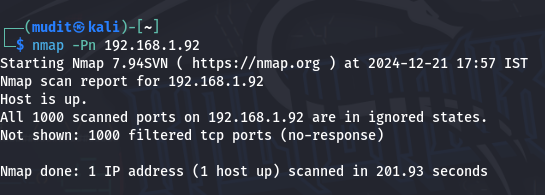
**Lab Practical 2:**

**Perform NMAP tool for scanning system vulnerability.**

**Commands:**

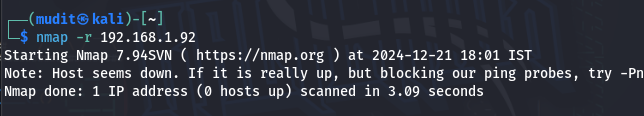
* -Pn: The command is used for Port Scanning and no discovery of Hosts.



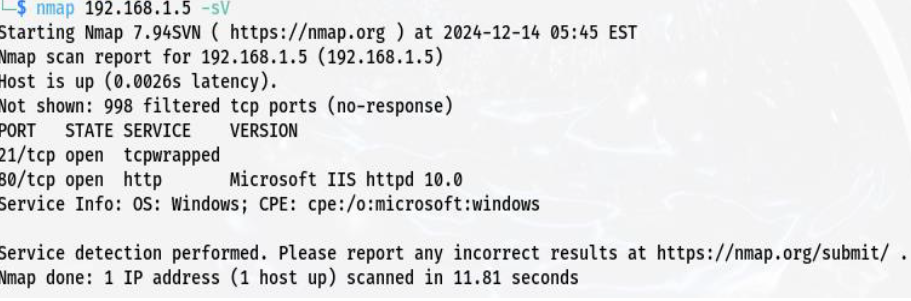
* -F: Fast scanning of ports for speeding up the process.



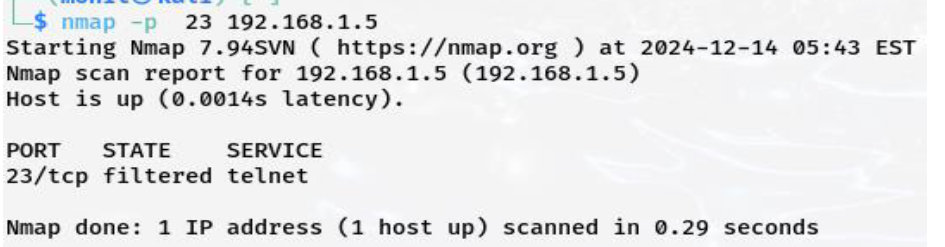
* -r: The command option is used for sequential scanning of the port.



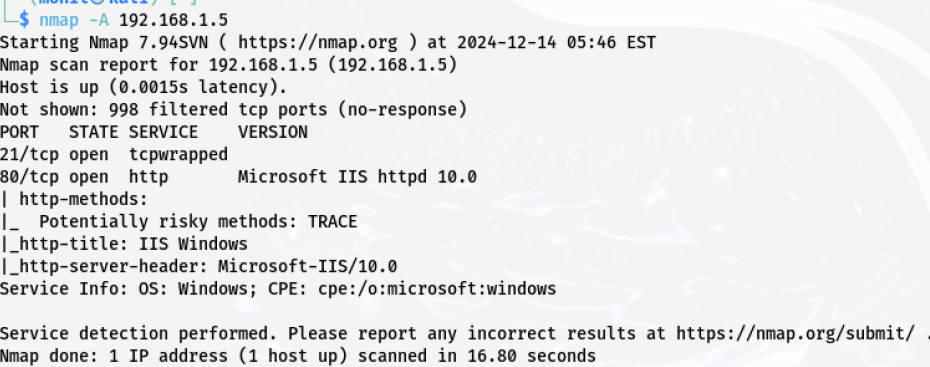
* -Sv: The command is used to identify and check for the version of service on that port.



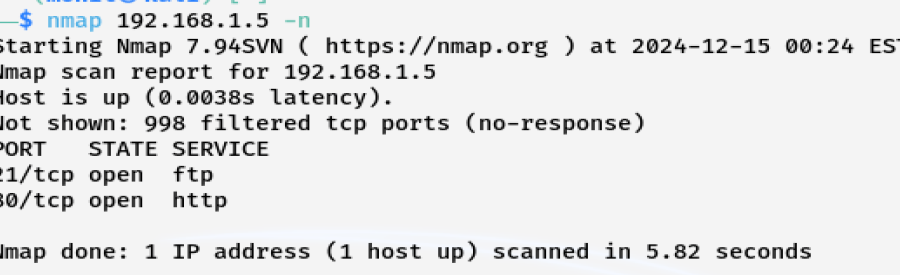
* -p: The command is used for scanning a specific port.



* -A: It enables OS detection, version detection, script tracing, traceroute.



* -n: No DNA resolution over the port.



* -T5: Very aggressive scanning on the port.

