Nmap Port Scanning

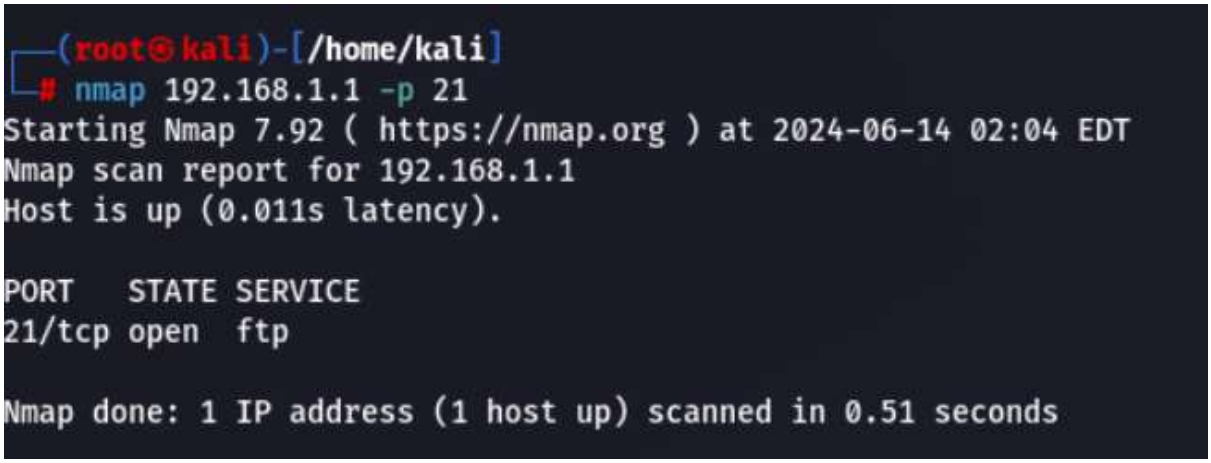
Nmap port scanning is a fundamental feature of Nmap used to identify open ports and services running on a target host or network. Port scanning helps network administrators, security professionals, and ethical hackers discover the various entry points into a system, assess the security posture of a network, and identify potential vulnerabilities.

Port scanning works by sending packets to specific ports on a target and analyzing the responses to determine the state of each port. Ports can be in various states such as open, closed, or filtered, indicating whether a service is listening, no service is present, or the port is being blocked by a firewall, respectively.

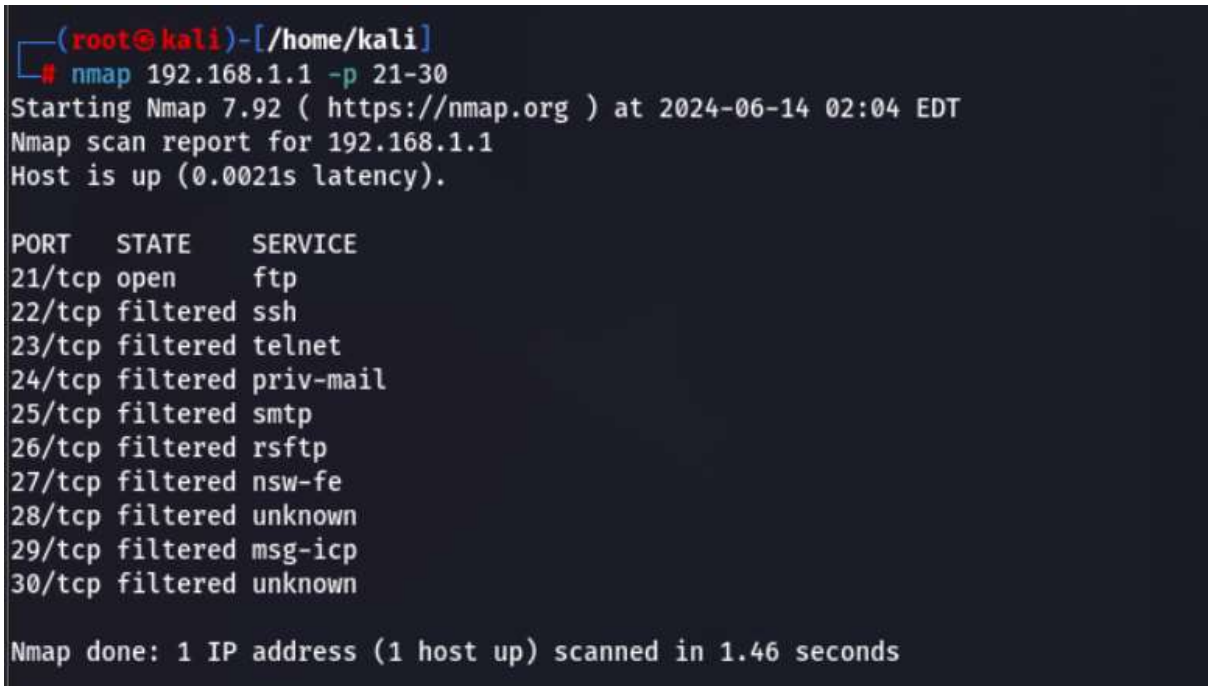
Port scanning with Nmap can be customized further with options to specify port ranges, set timing and performance parameters, and employ advanced techniques like version detection (-sV) and script scanning (-sC) to gather more detailed information about running services and potential vulnerabilities. This comprehensive approach makes Nmap an invaluable tool for network security assessments and management.

Examples: -

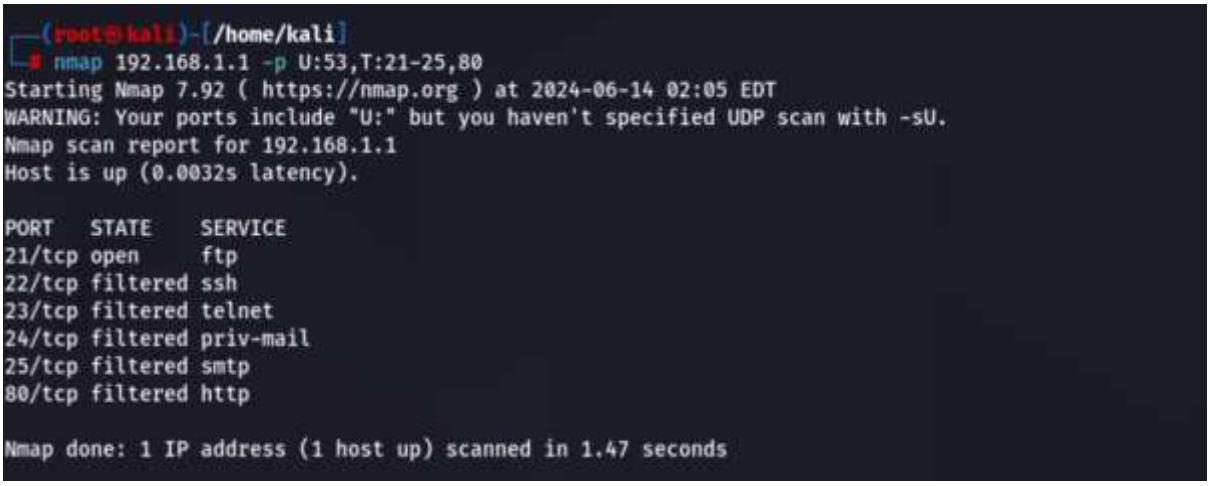
1. This command will scan port scan for defined port x.



2. This command will scan ports scan for defined range of port x.

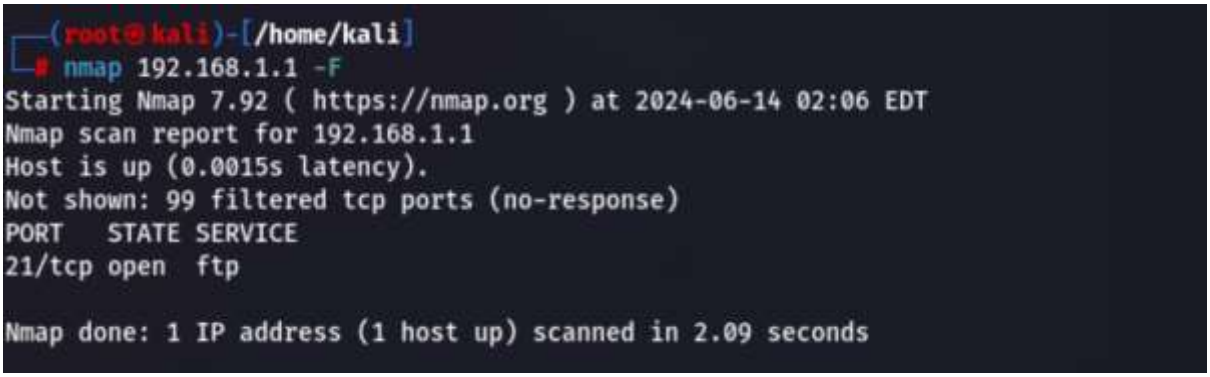


3. This command is for port scan for multiple TCP and UDP ports.



4. This will scan for all the available 65535 ports. You can't be able to see the result below as I have stop the scan as it is going to scan all the ports which is very time consuming.

5. This will do a fast port scan for 100 ports.



6. Here port scanning is done from service name.