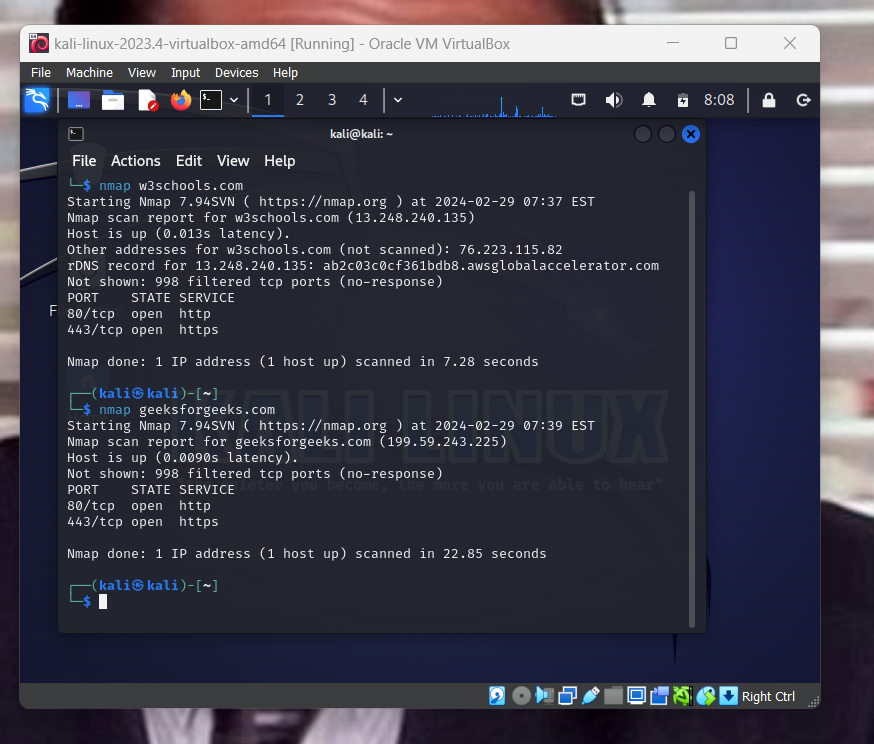
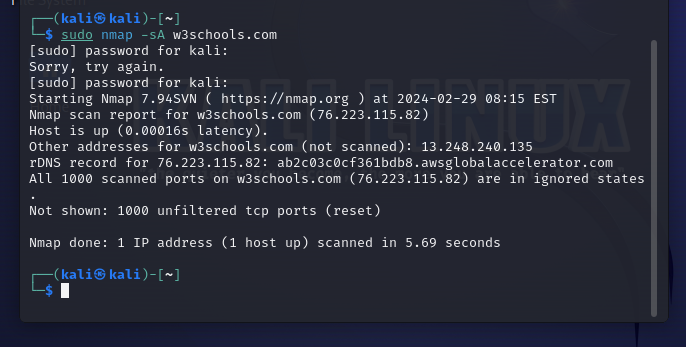
1. **Basic usage for nmap**

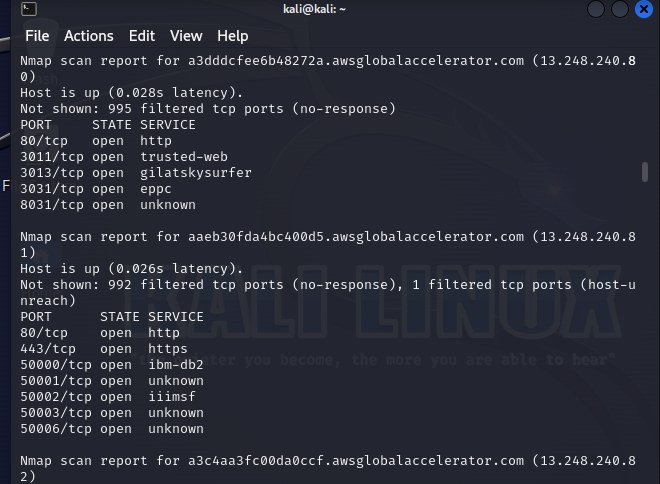
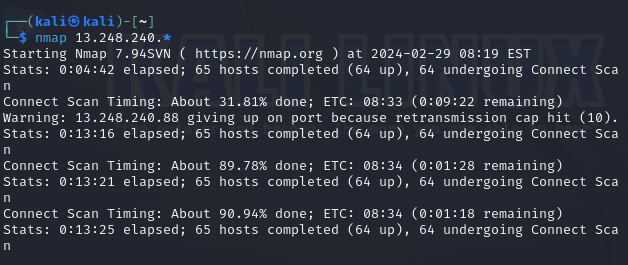


1. **Use nmap -sA to get remote firewall settings**

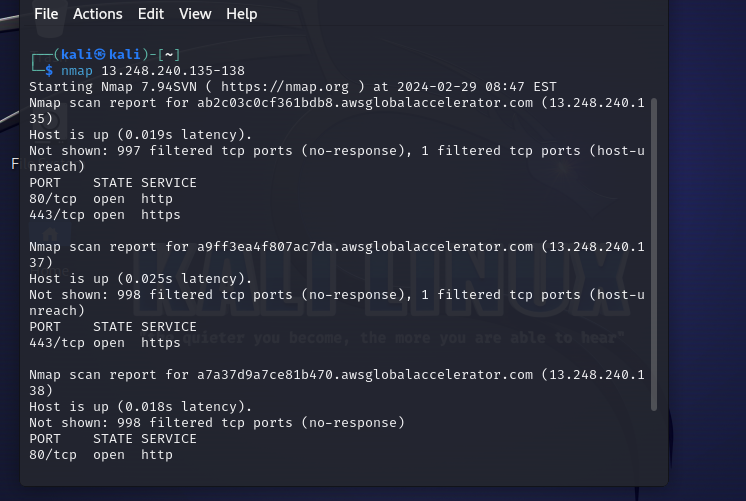


1. **Use \* to scan the whole subnet:**

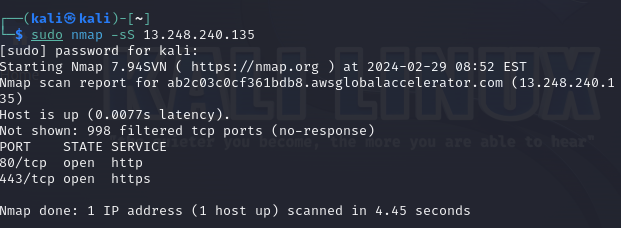
**This commands scans for all the hosts in a given subnet.**



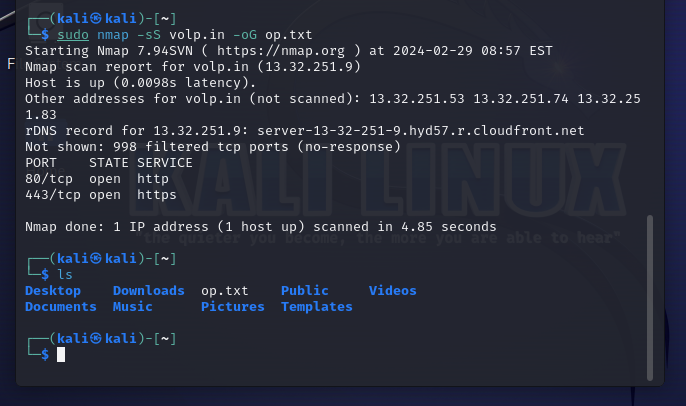
1. **Use ‘-’ to scan for a range of IP addresses. Eg - *nmap 192.68.1.1-5* will scan for 5 addresses**



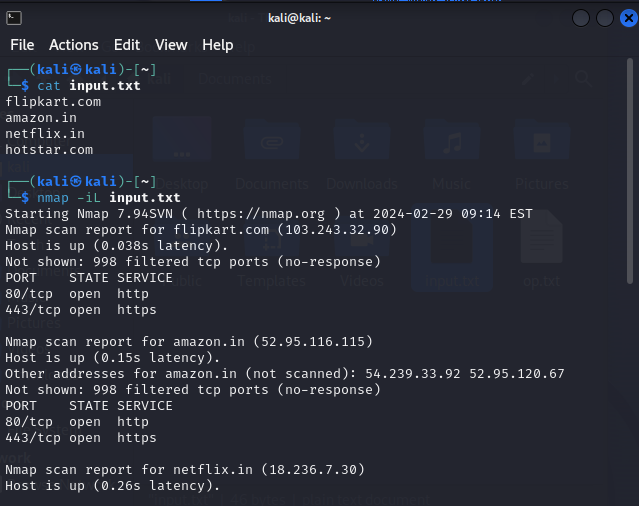
1. **Use option -sS for stealthily scanning all TCP SYN requests. Eg *nmap -sS <Domain Name>***



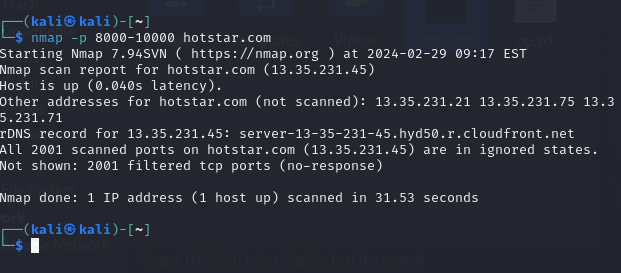
1. **Use the option -oG to write the output of nmap to a file**



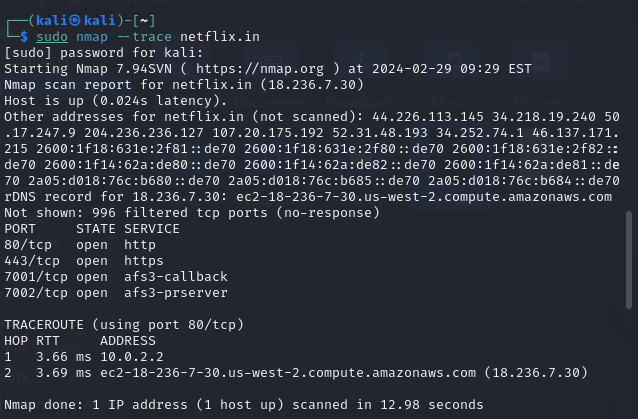
1. **Use the option -iL to give input via a text file**



1. **Use -p for scanning specific ports or range of ports**



1. **Trace the route to the target with - -trace option**



1. **Use the option -O to find out the target’s OS**

