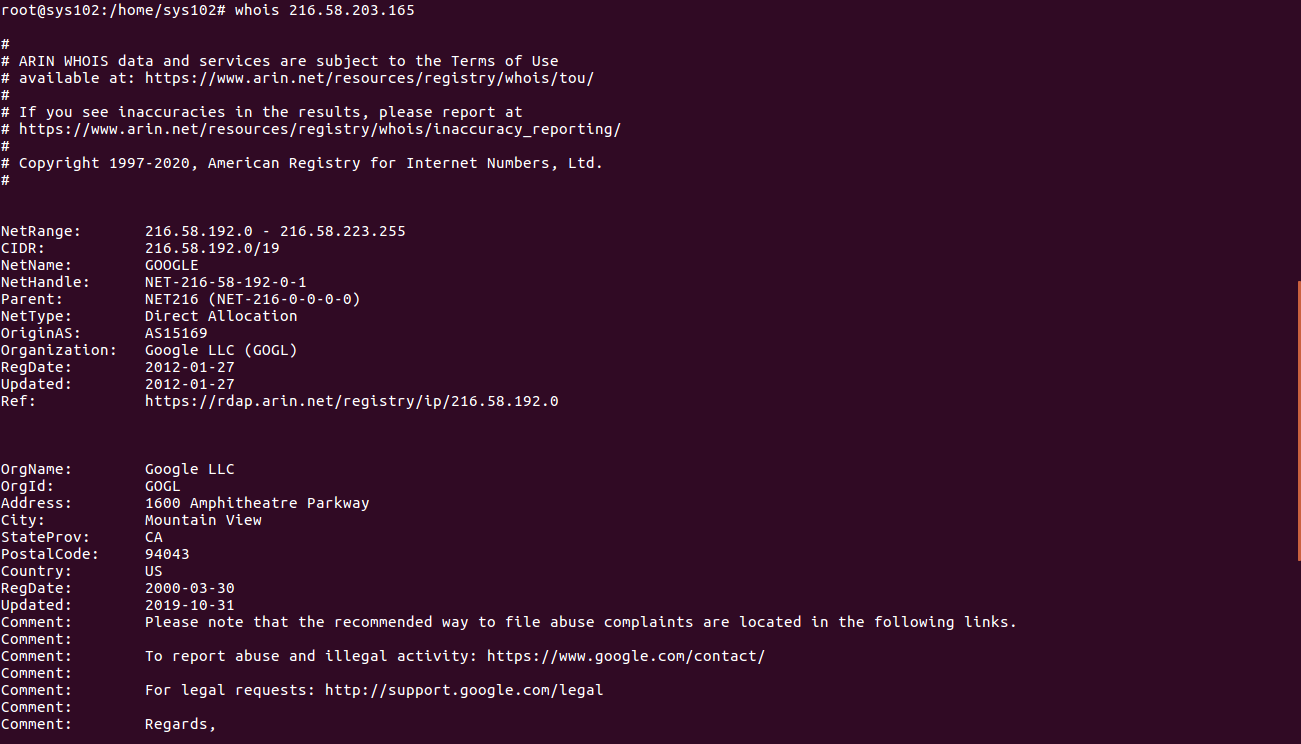
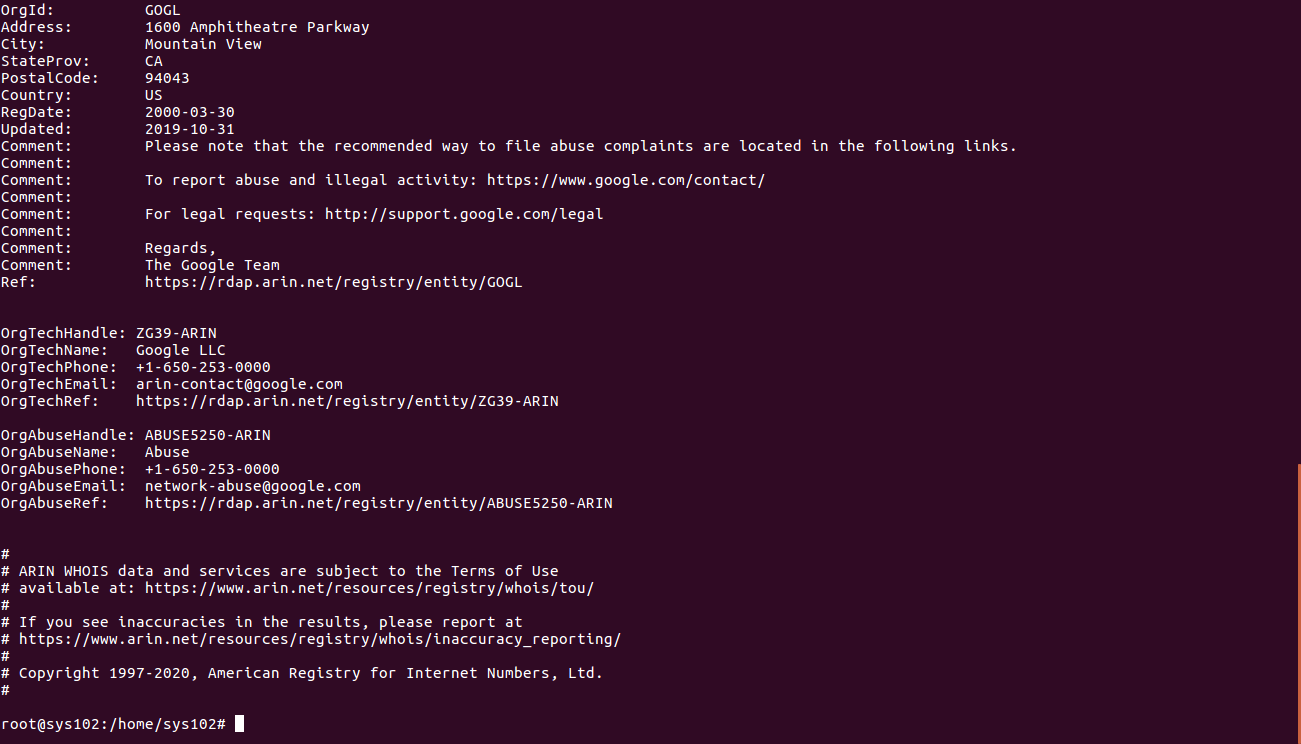
EXPERIMENT - 2

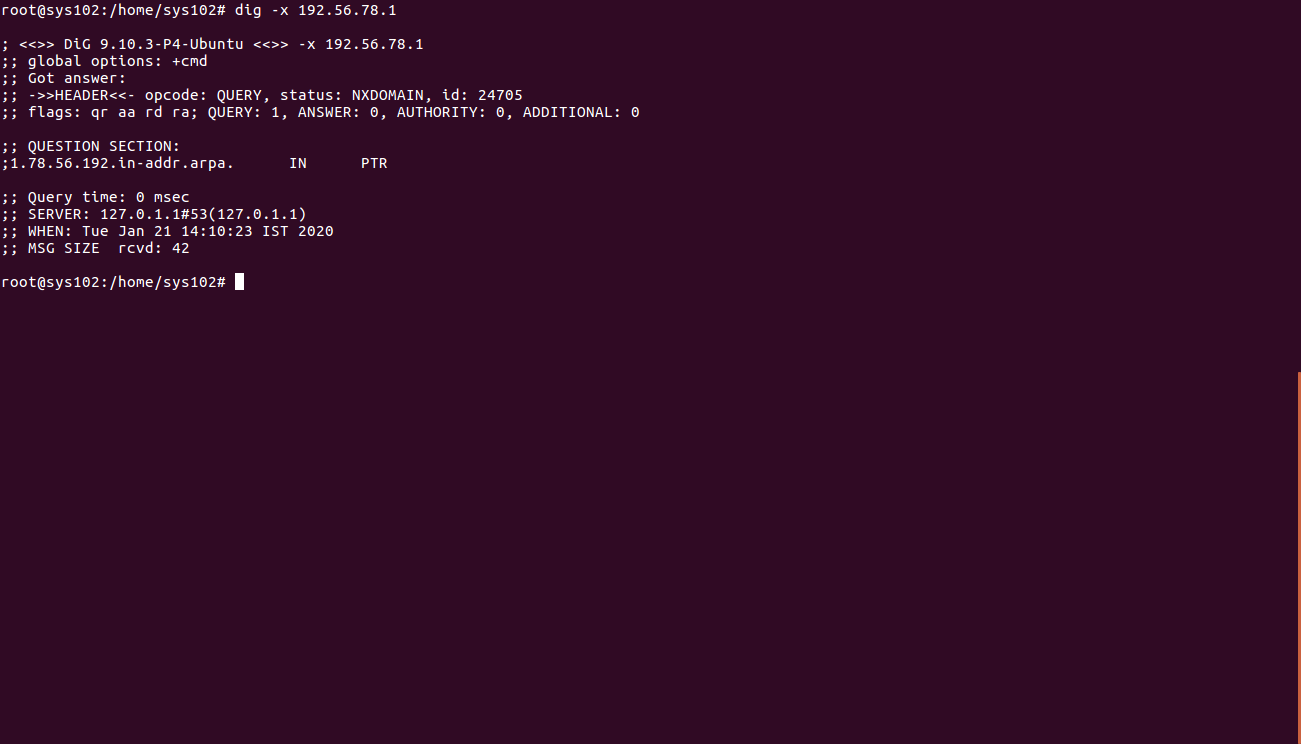
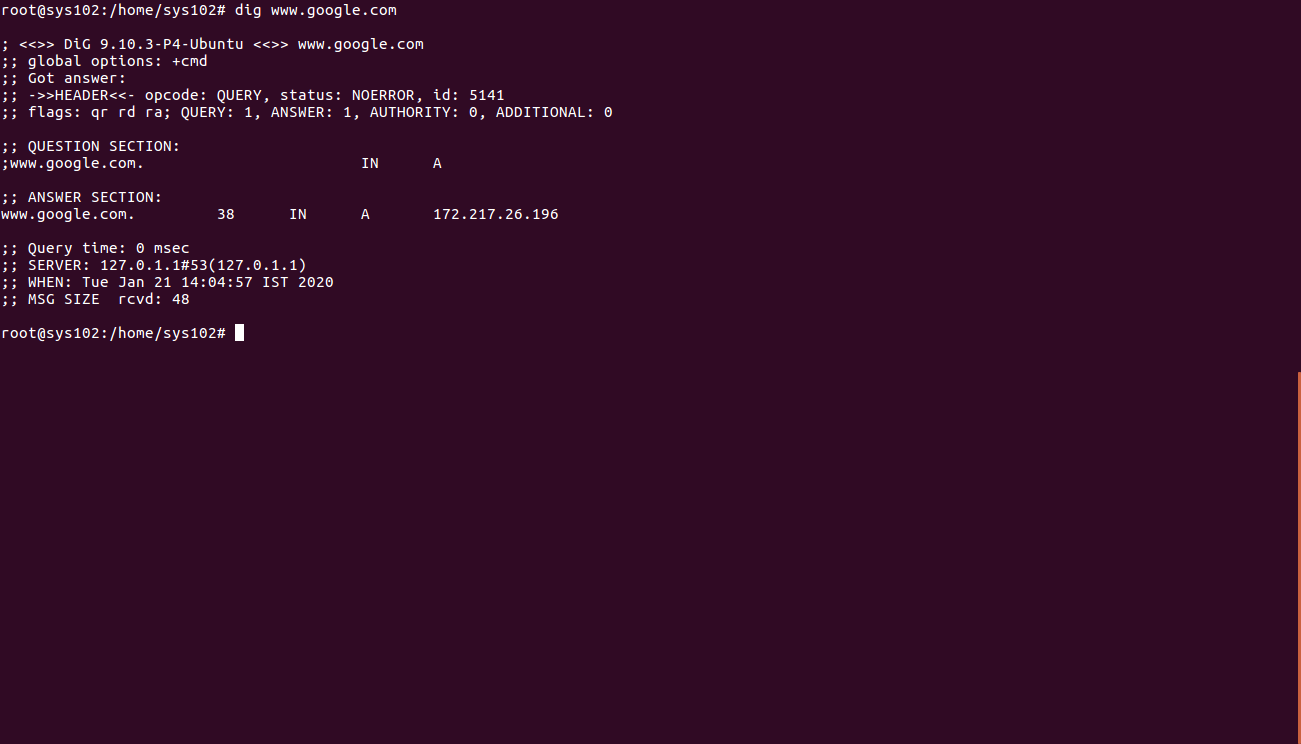
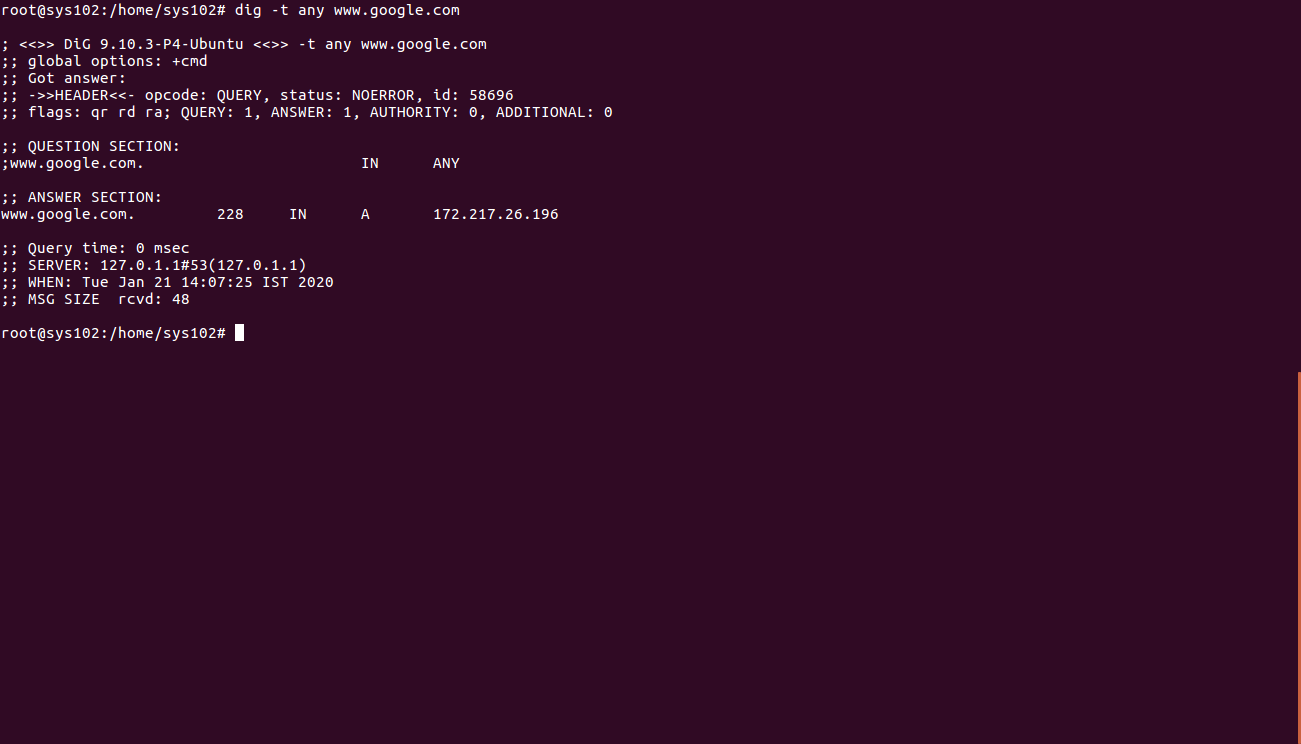
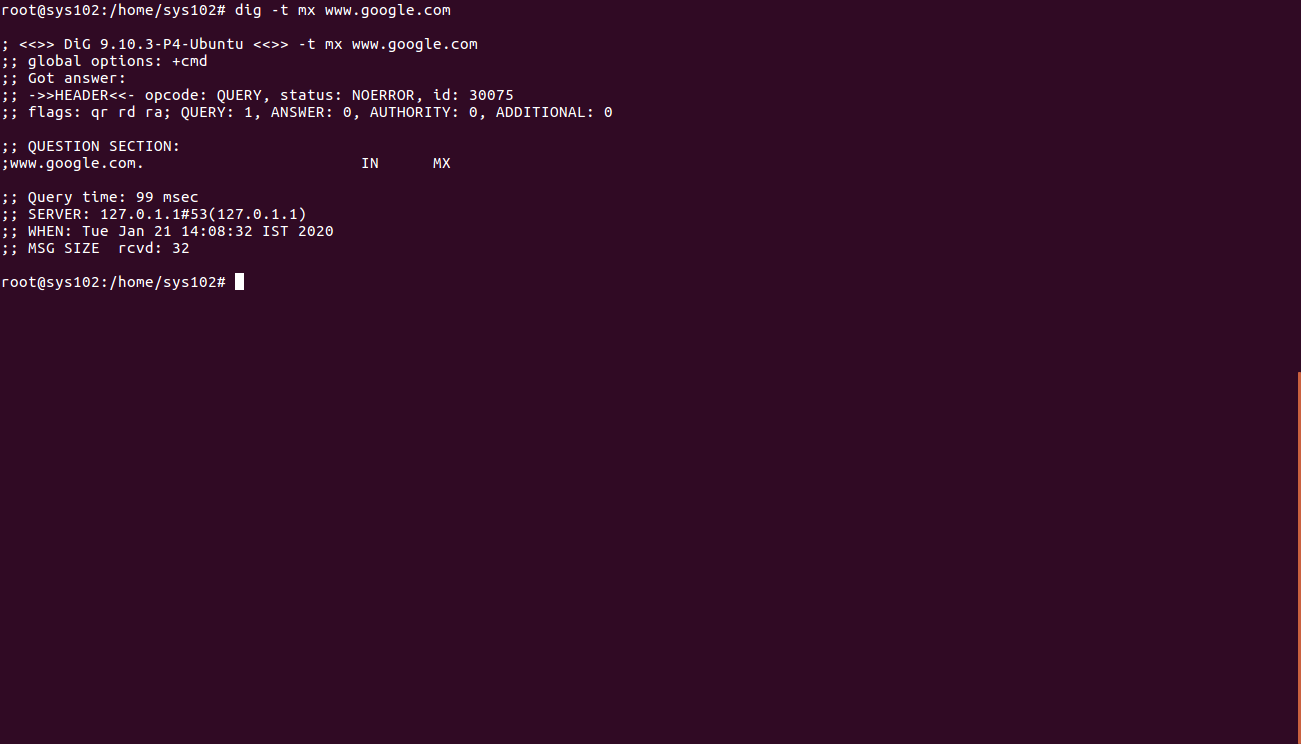
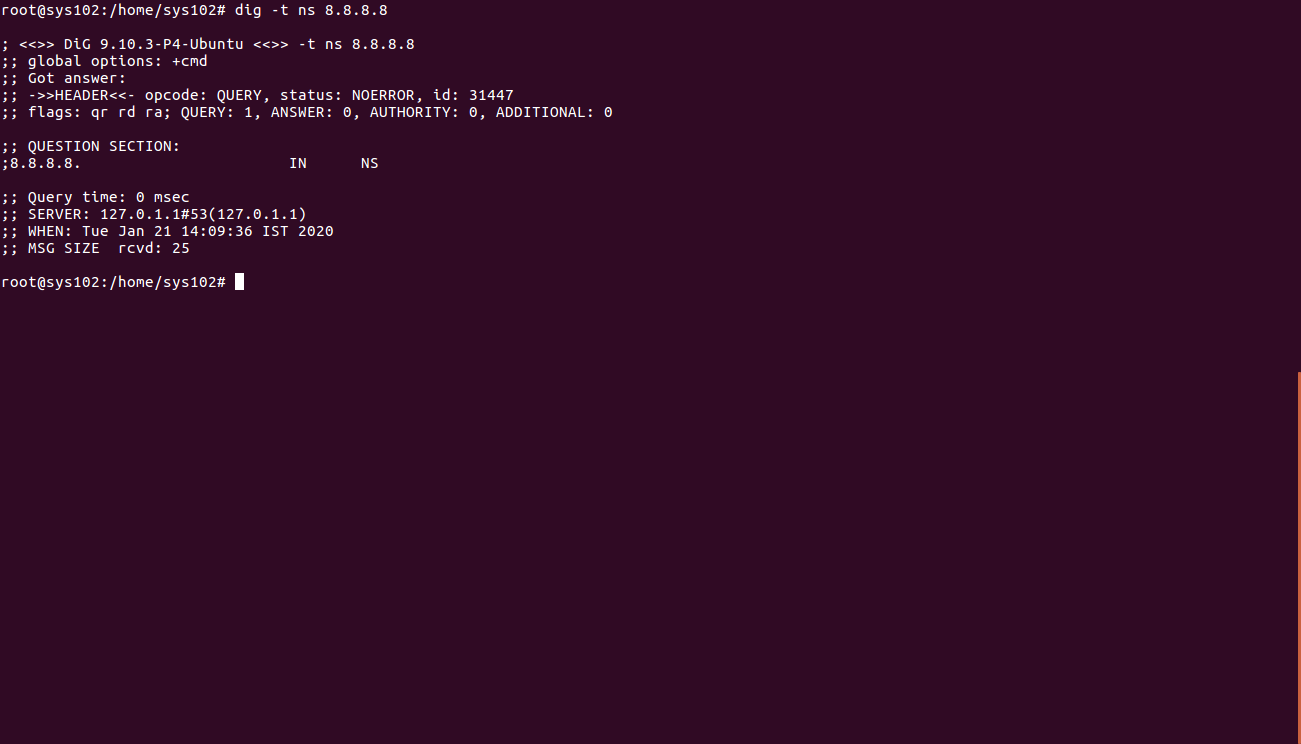
AIM : Study of network reconnaissance tools.

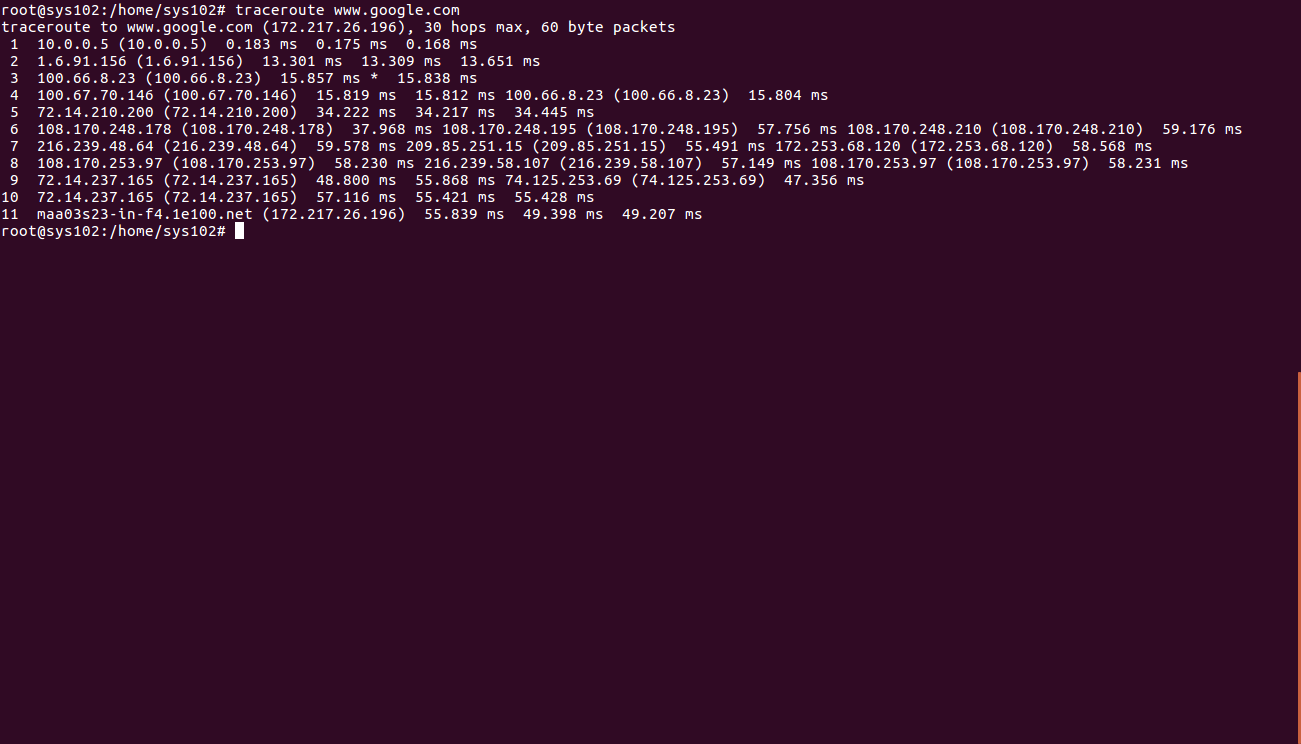
COMMANDS :

* Whois

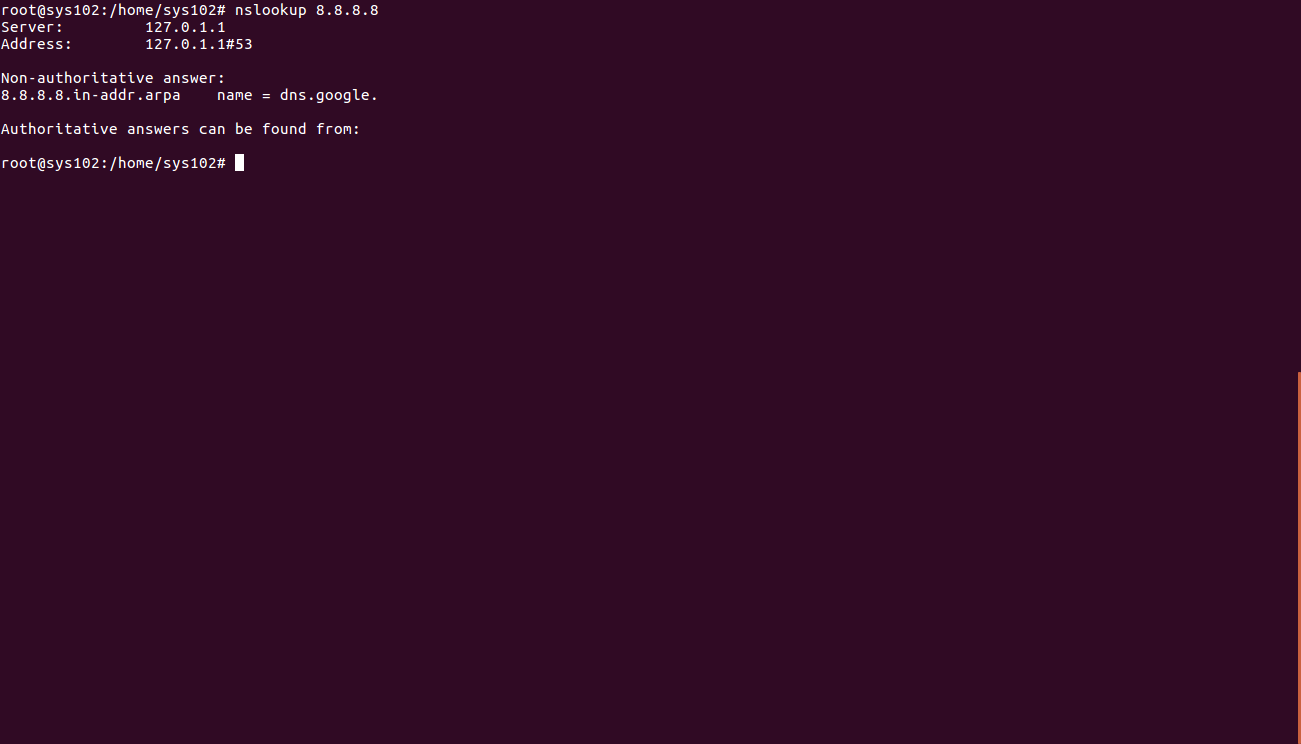




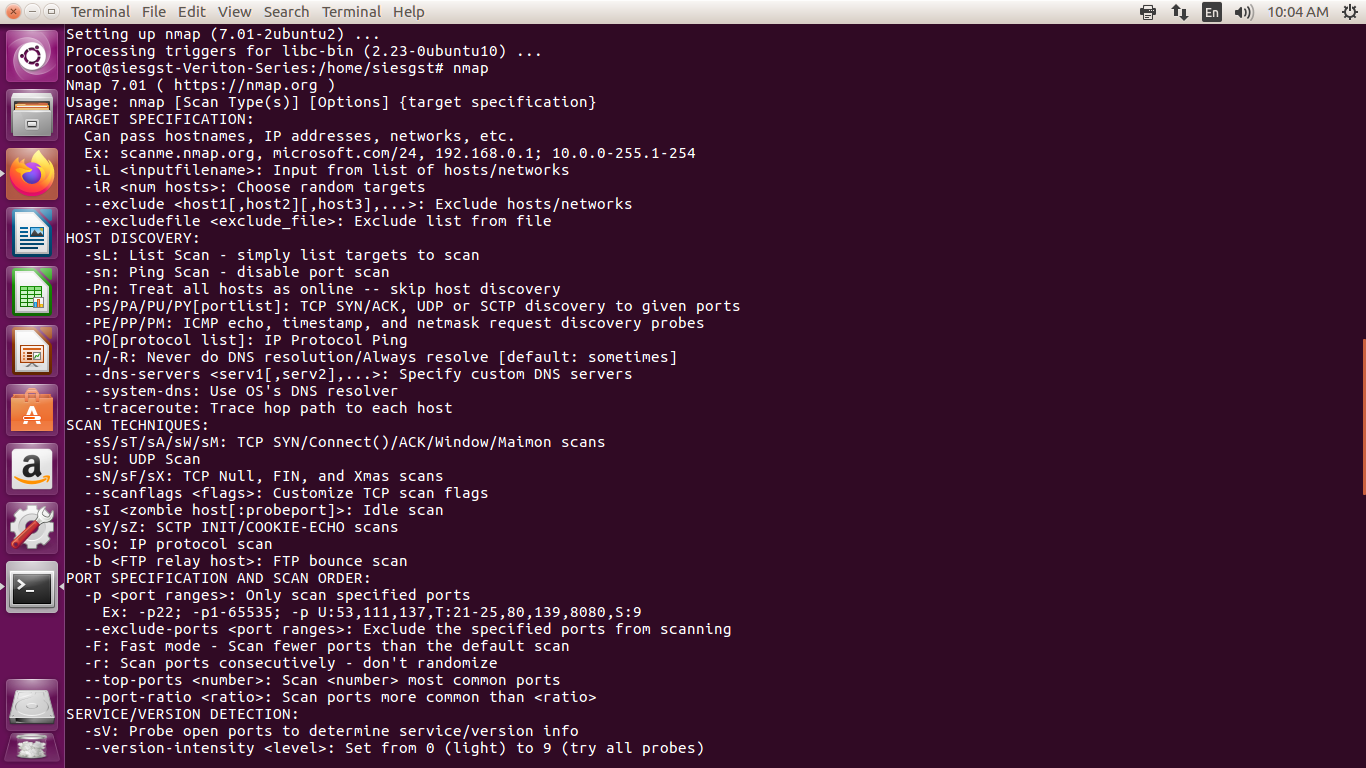
* Dig
* Traceroute

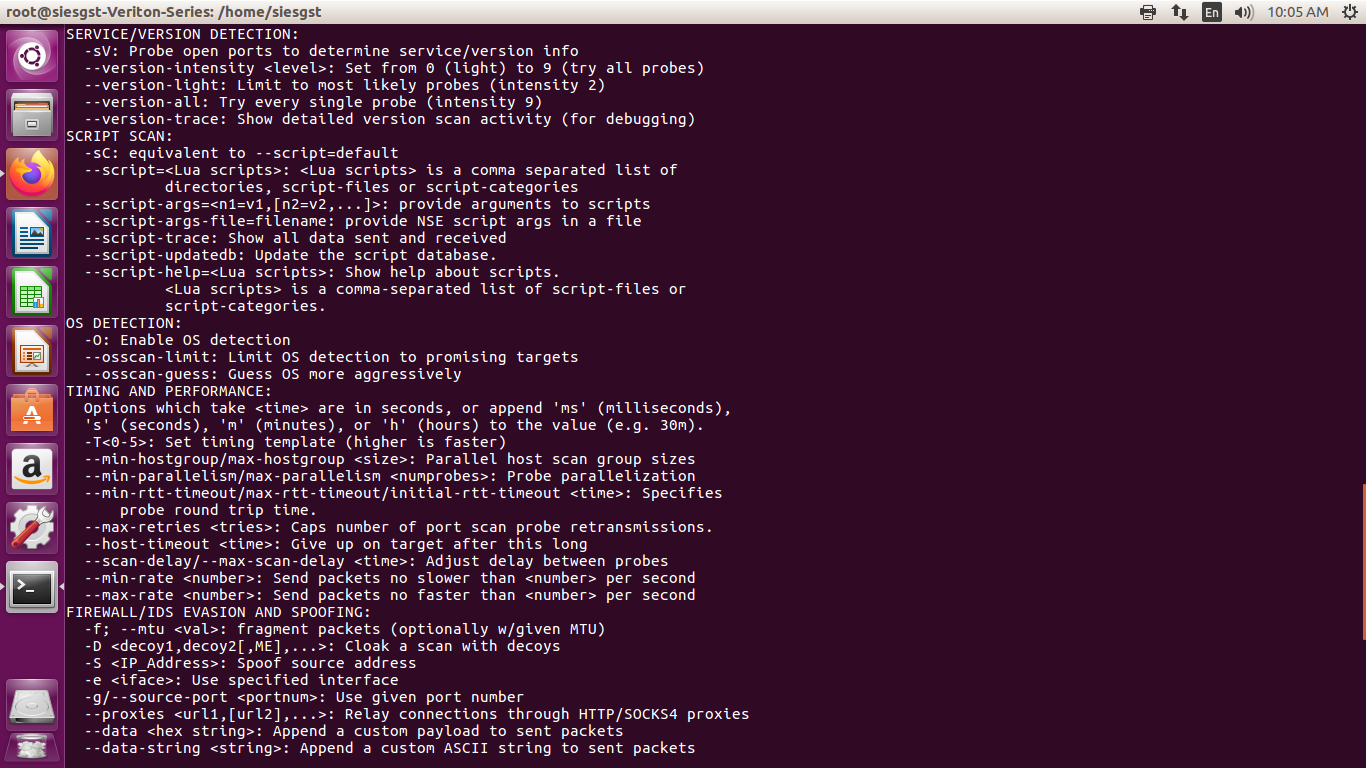


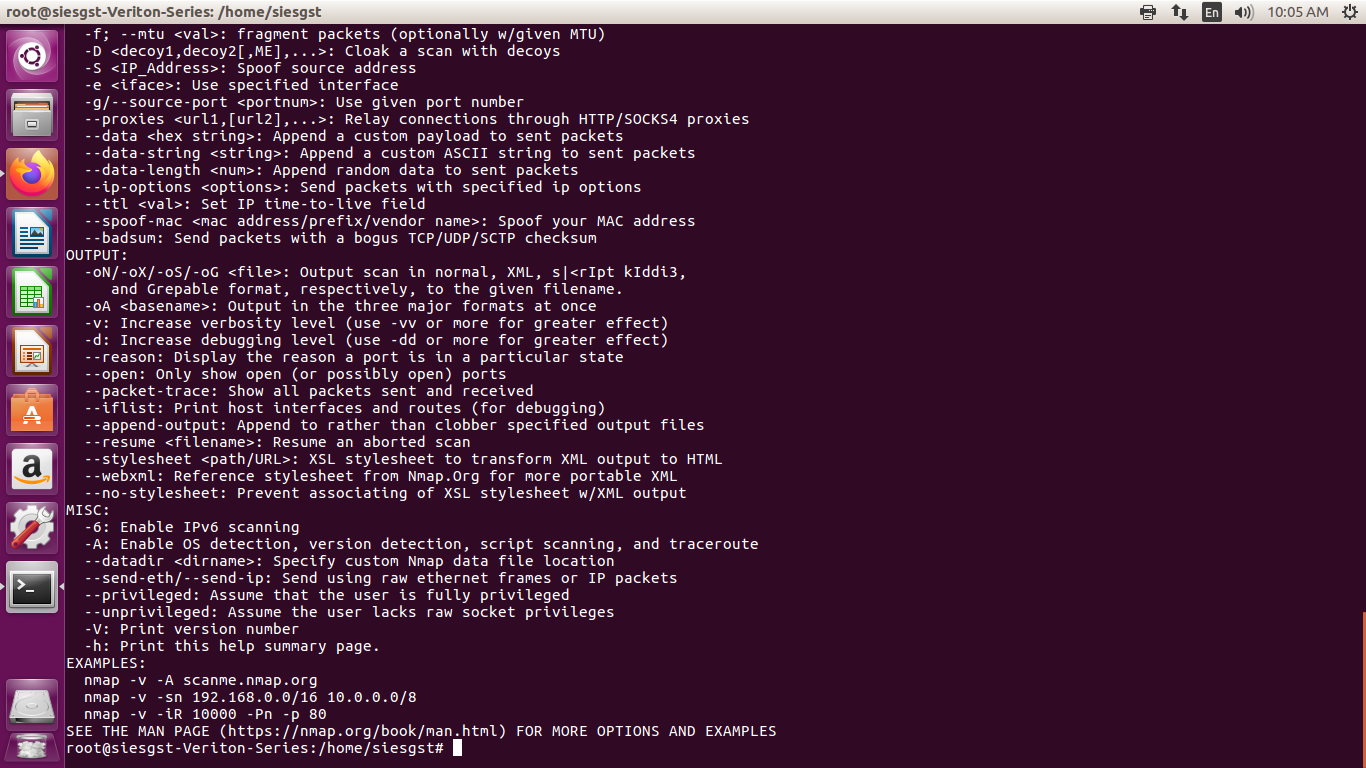
* Nslookup



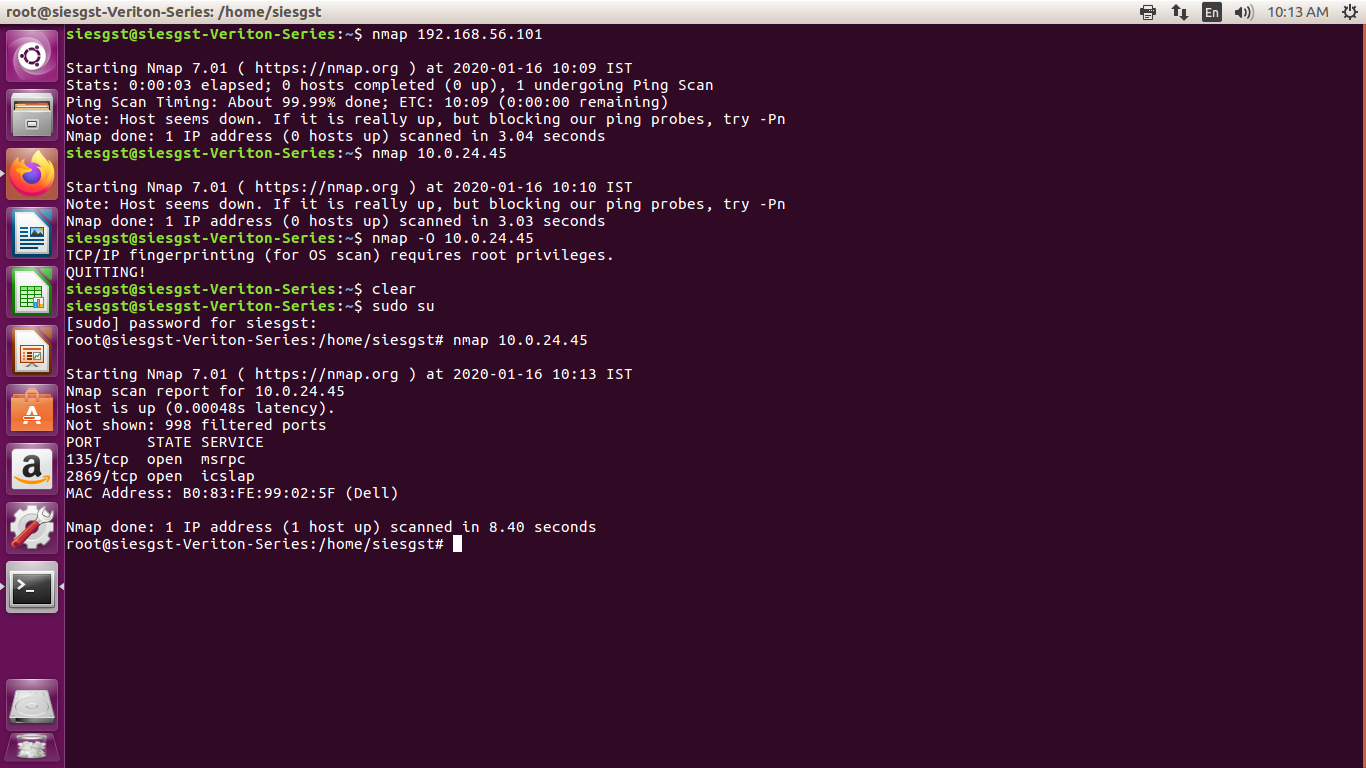
* Nmap



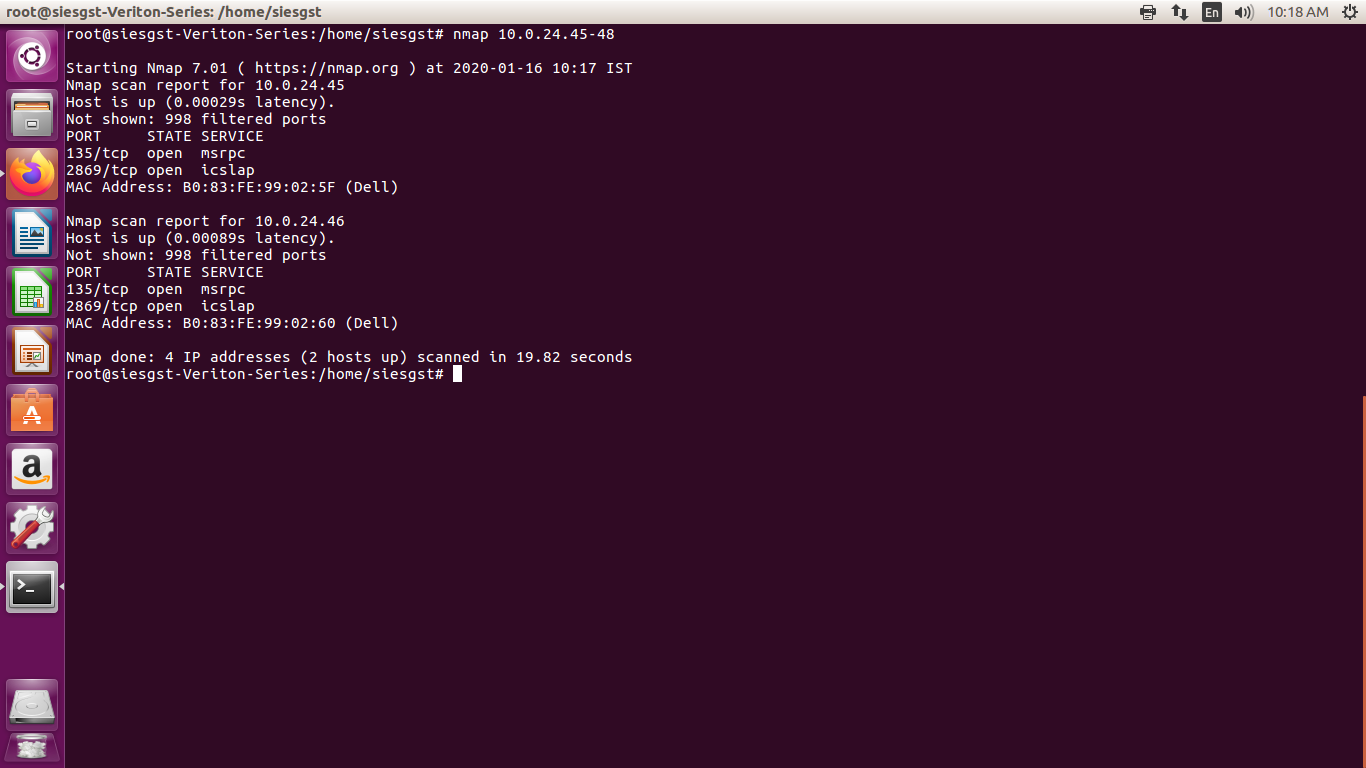




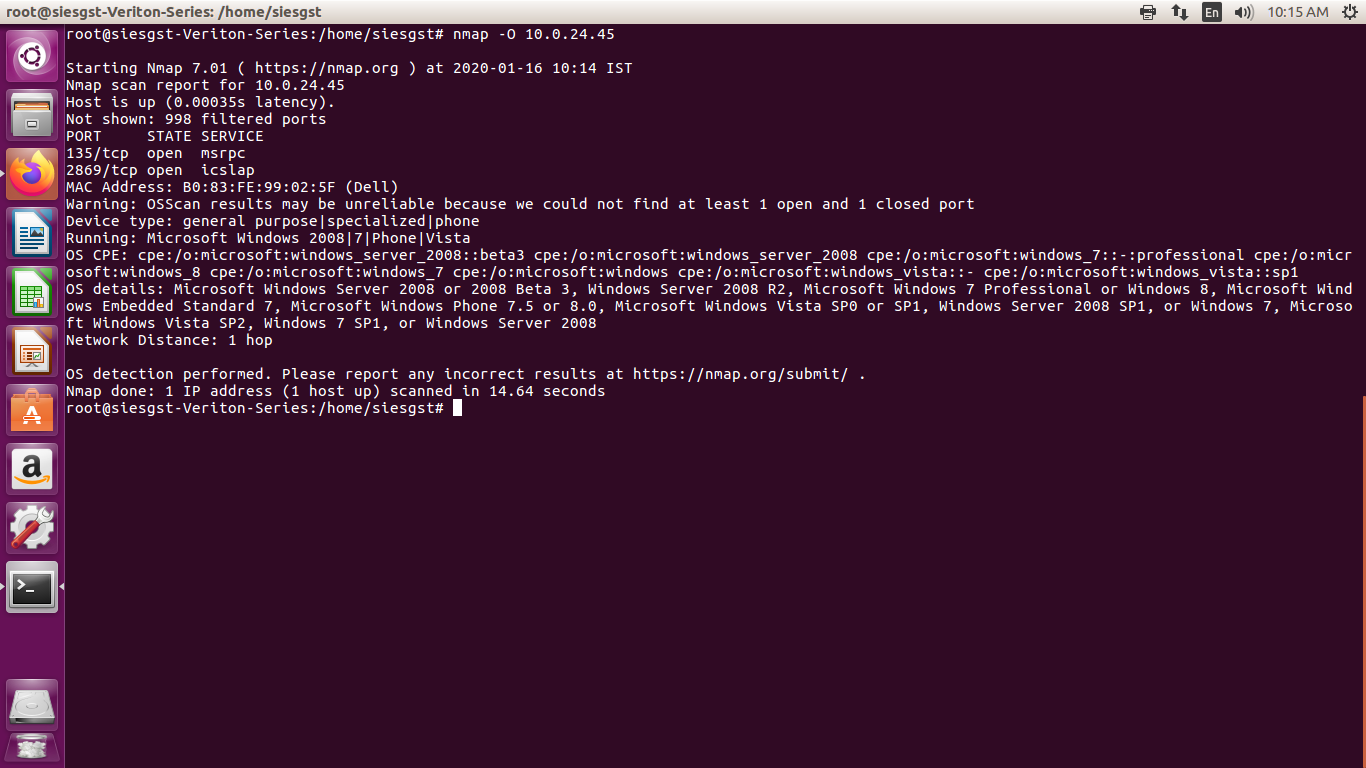
* nmap<ip\_address> :



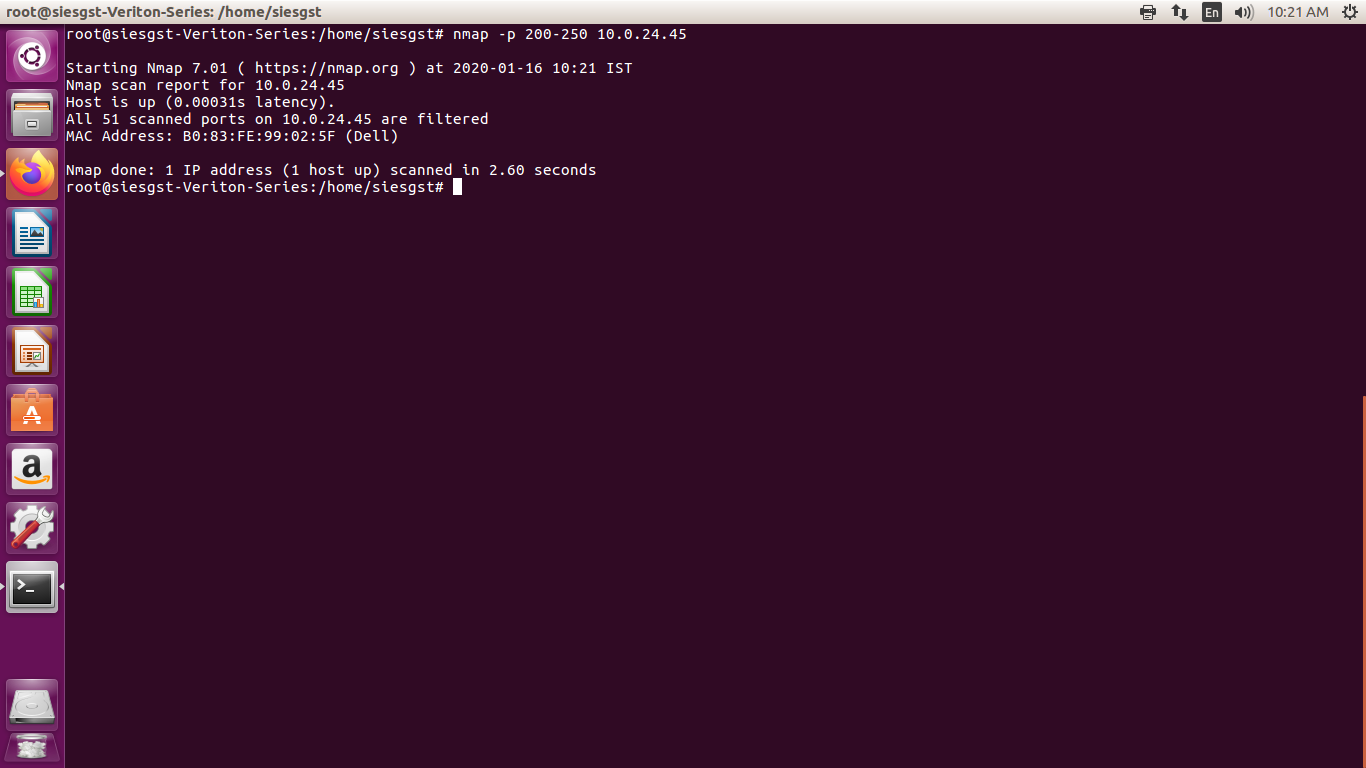
* nmap<ipaddr-(next 4/5 nos. to give range)> :



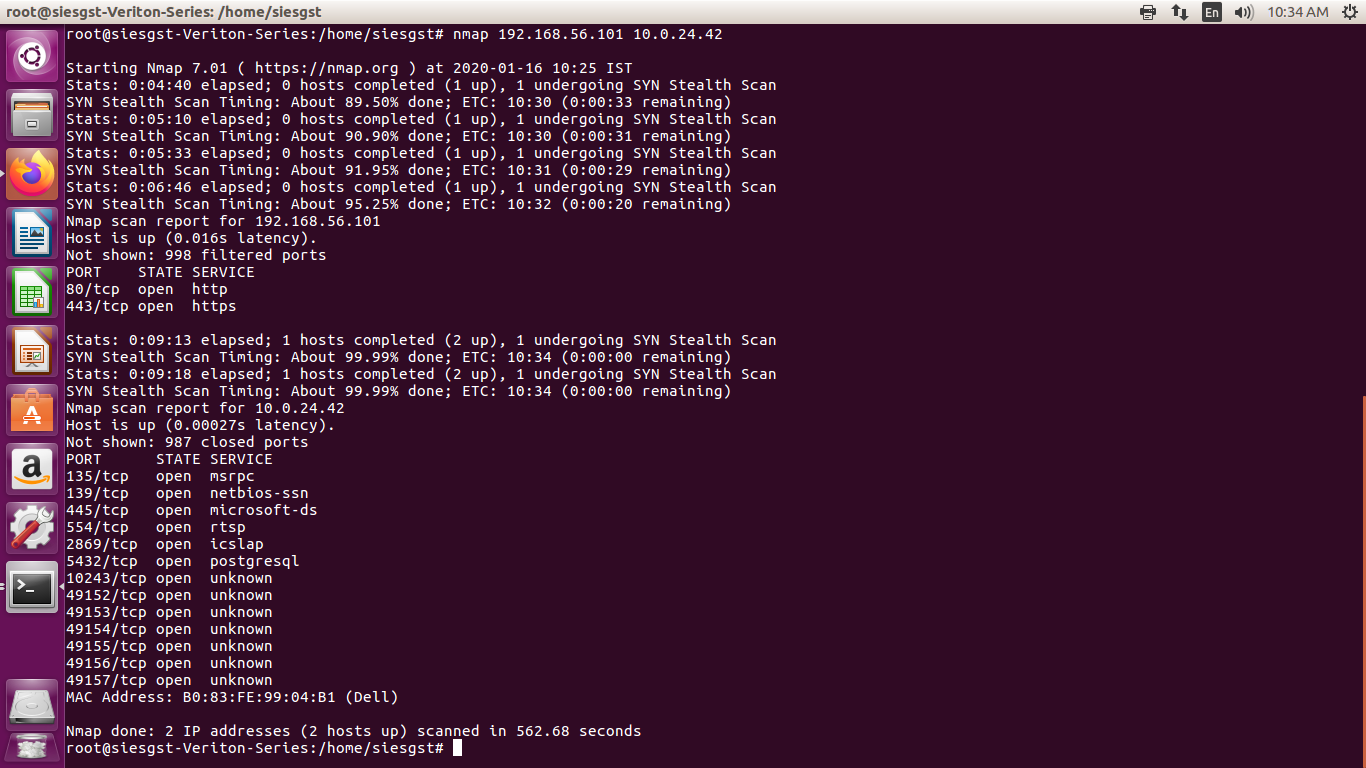
* nmap -O<ipaddr> :



* nmap -p<range><ipaddr> :



* nmap <ipaddr1><ipaddr2> :



* nmap -p<portname> :

