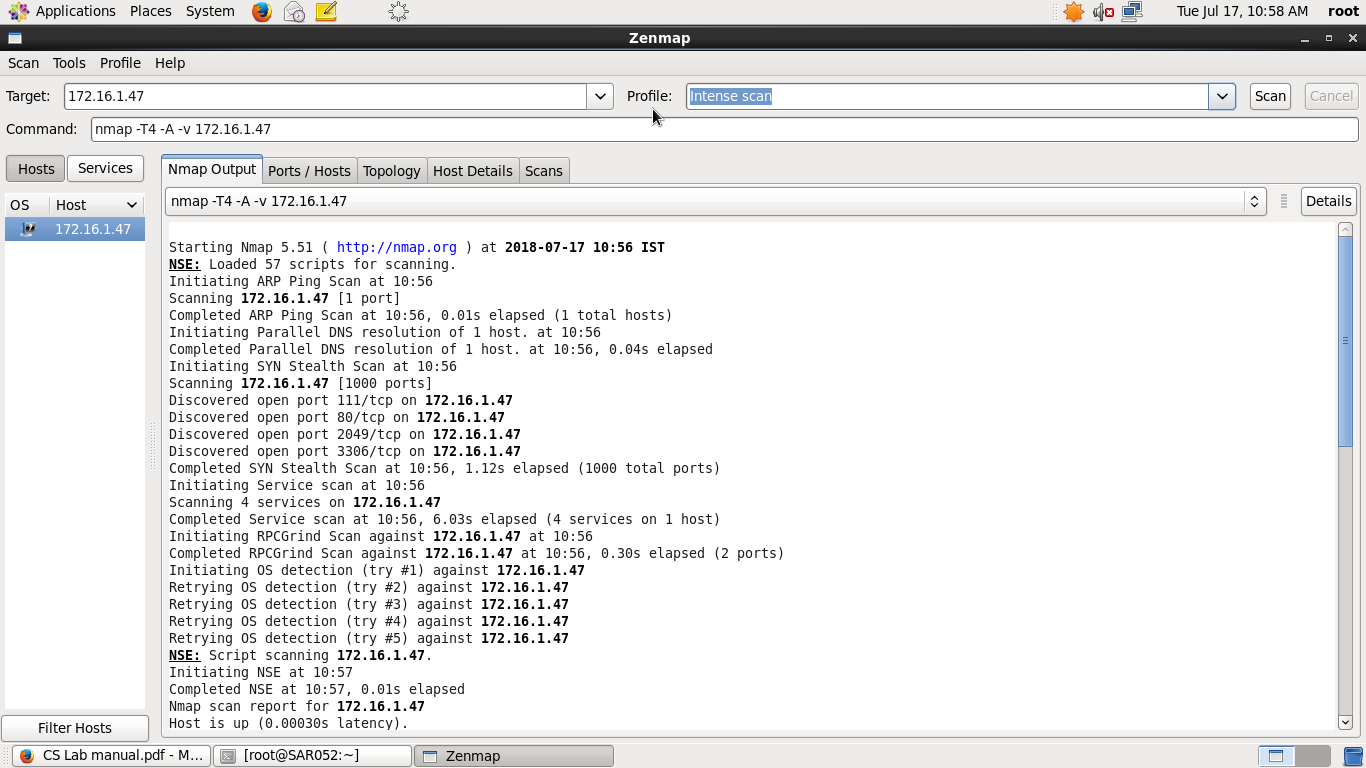
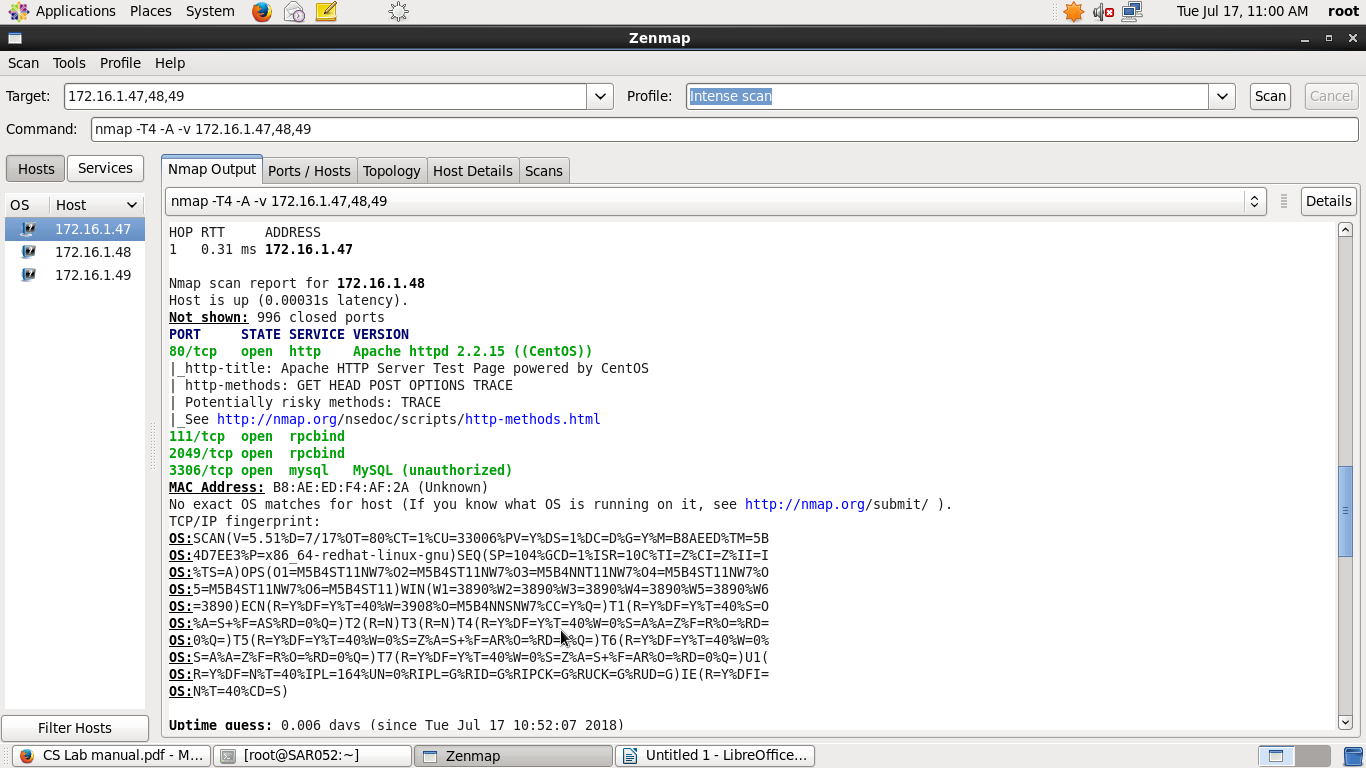
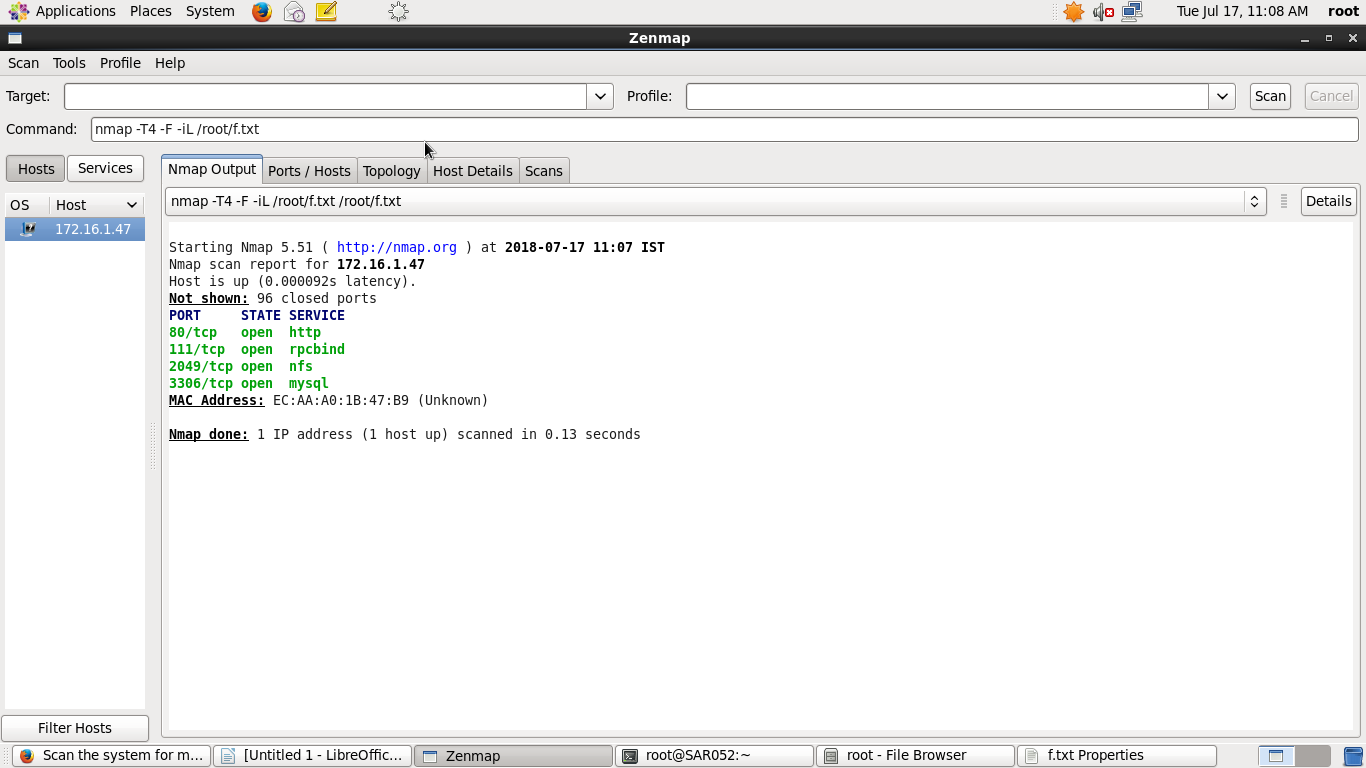
1.Scan a system using Hostname and IP address.



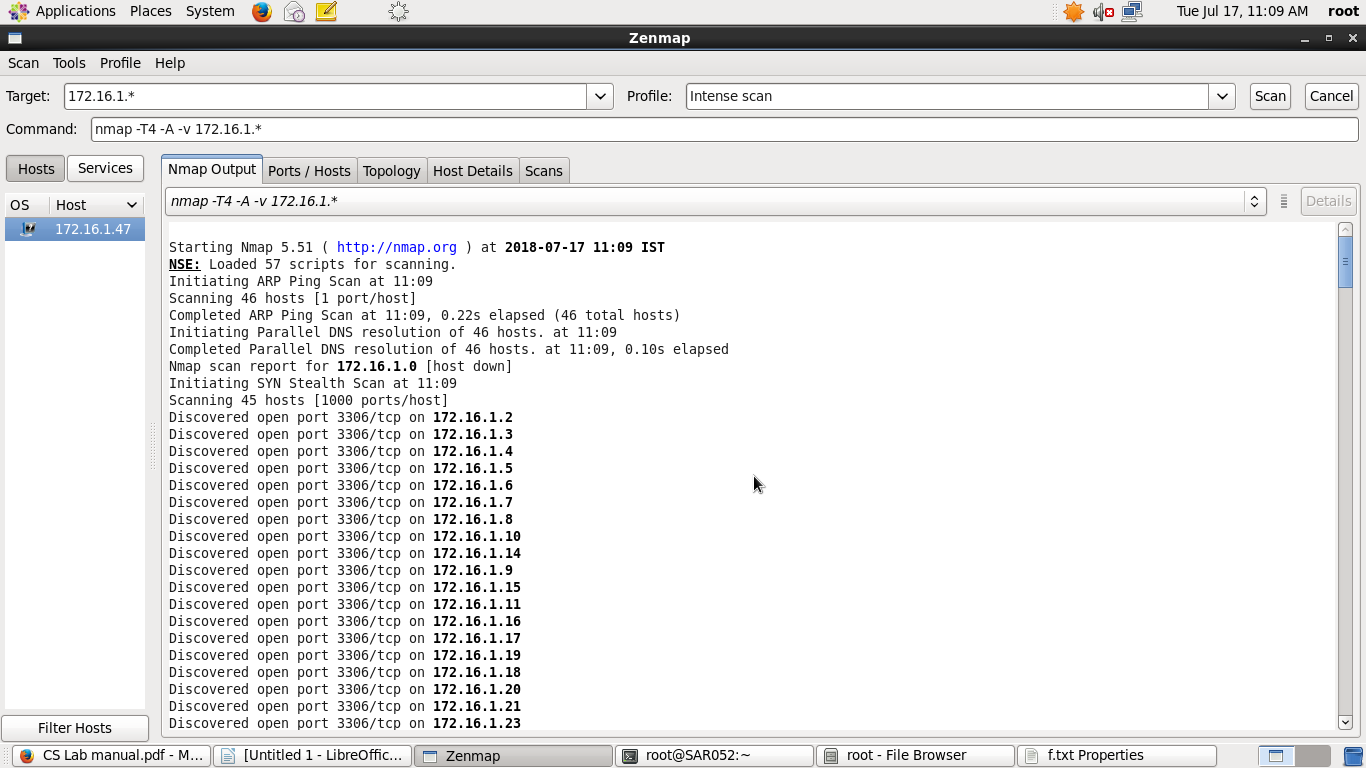
2.Scan the system for multiple host.



3.Scan the system for multiple host using file.

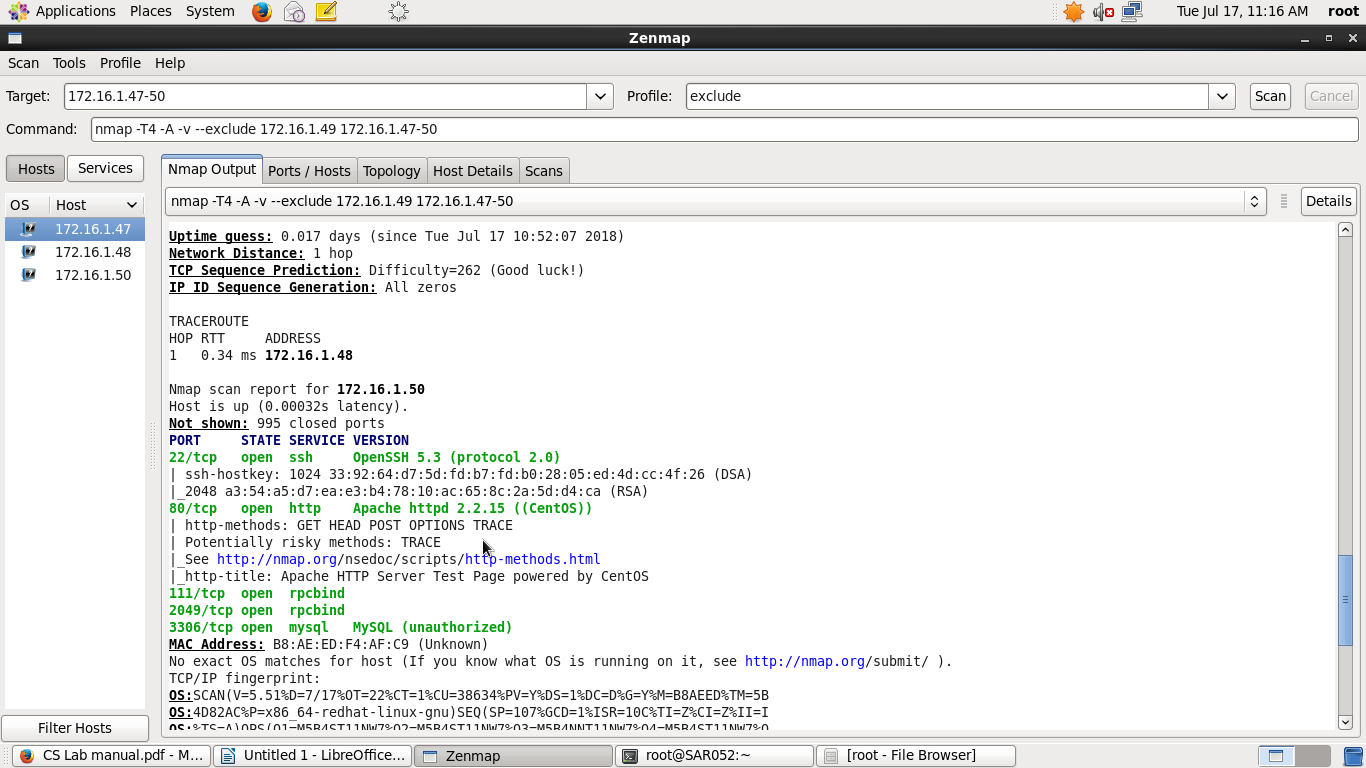


4.Scan the system using whole subnet mask.

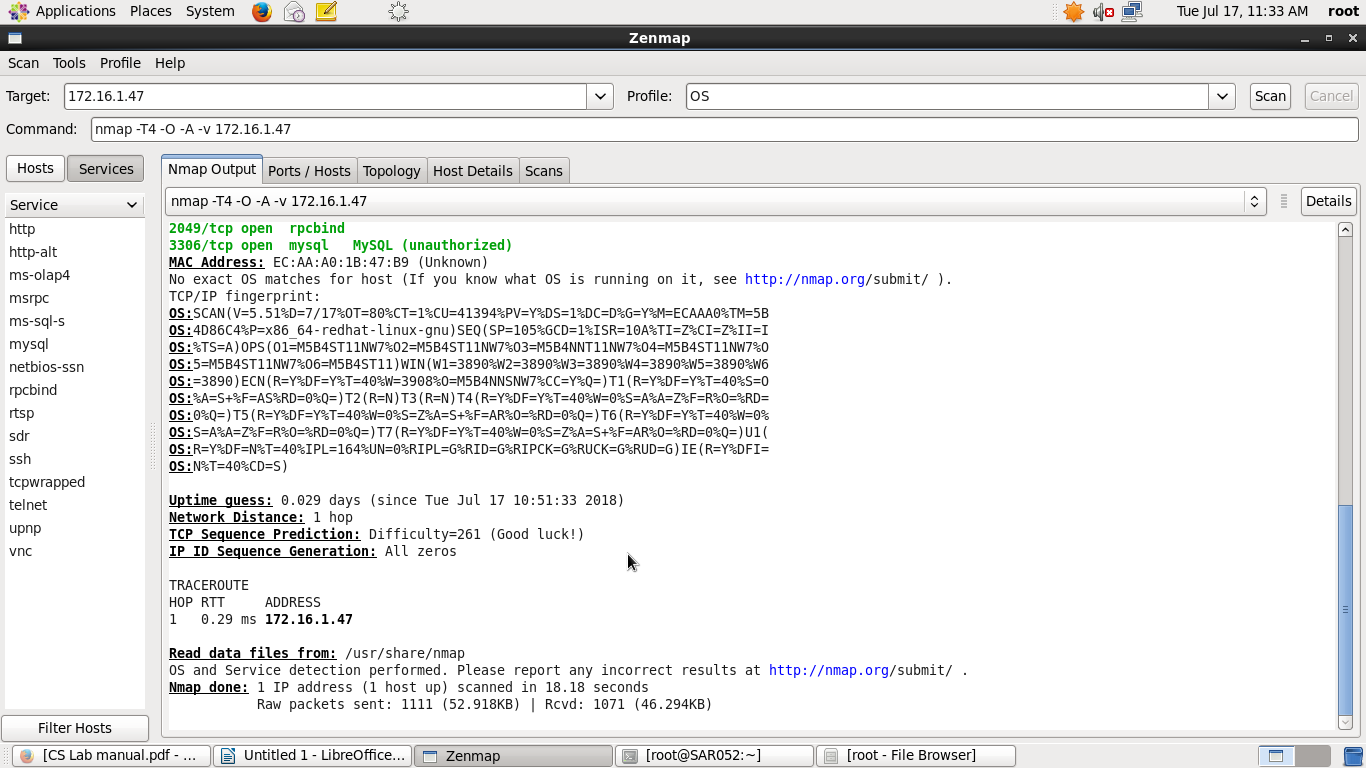


5.Scan the system for multiple system using last octet of IP address.

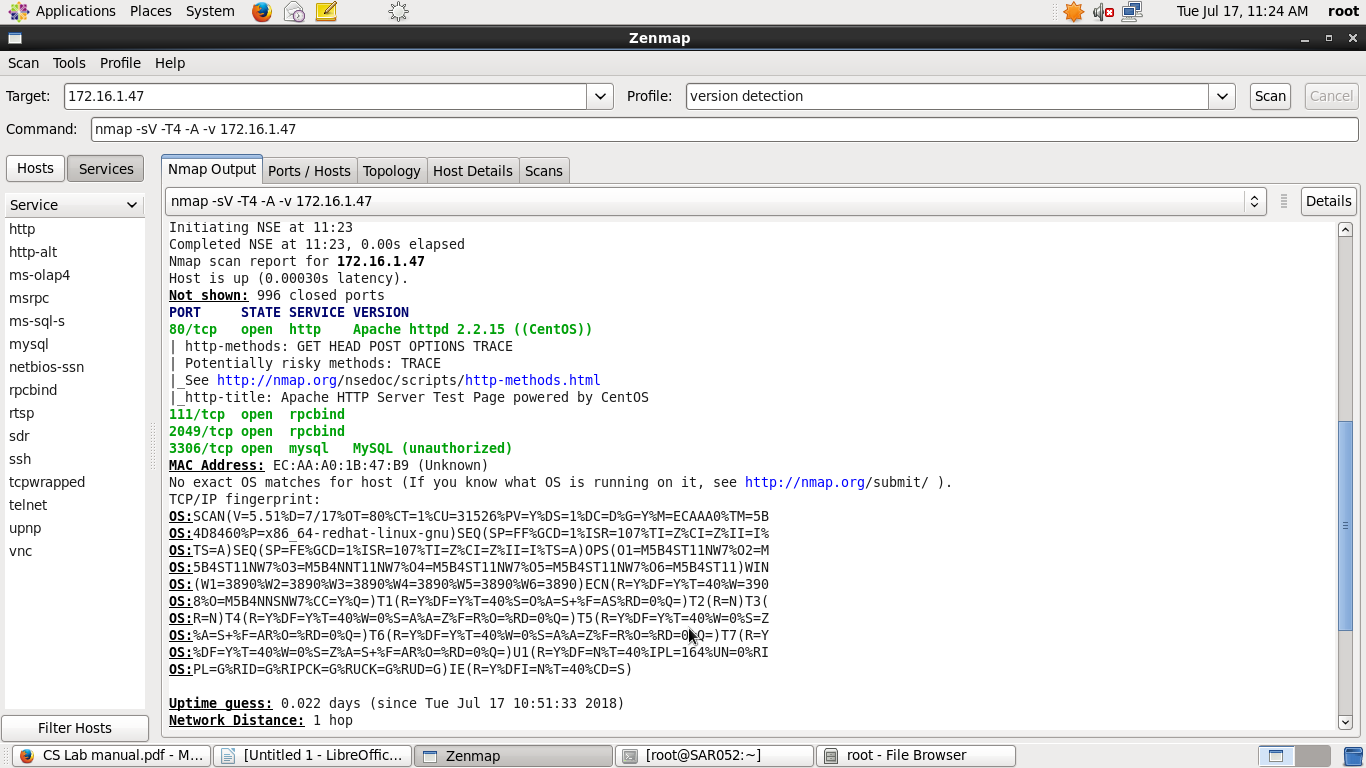
6.Scan IP address rang and excluding particular user



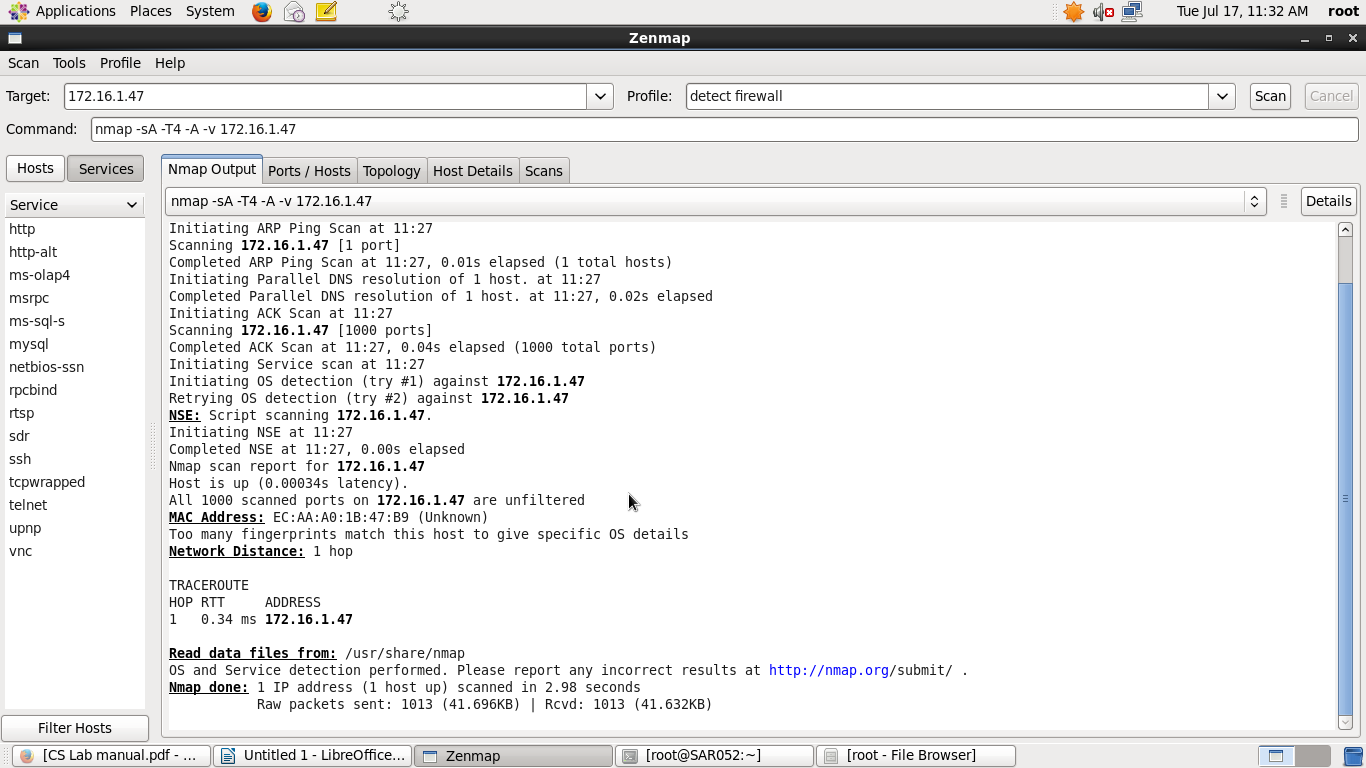
7.Show OS detail and trace route.



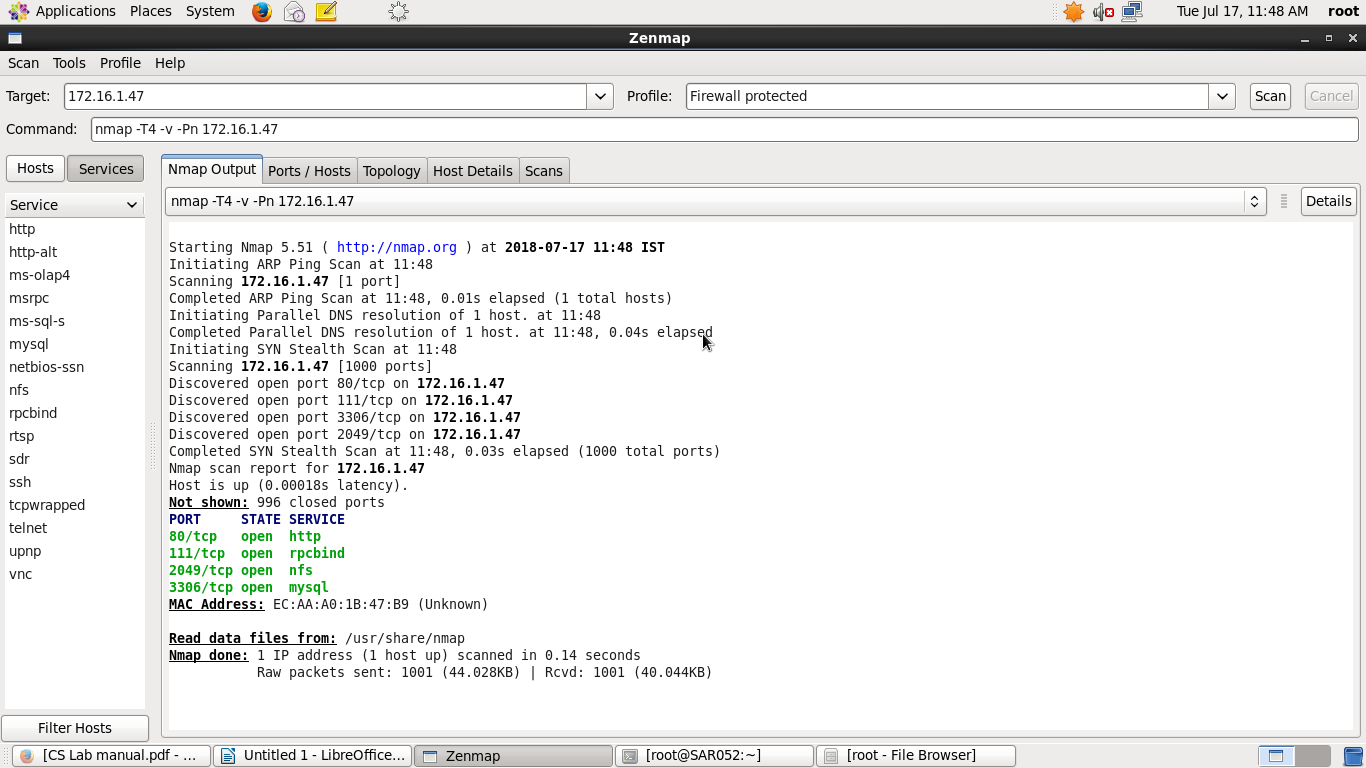
8.Enable version detection using NMAP.



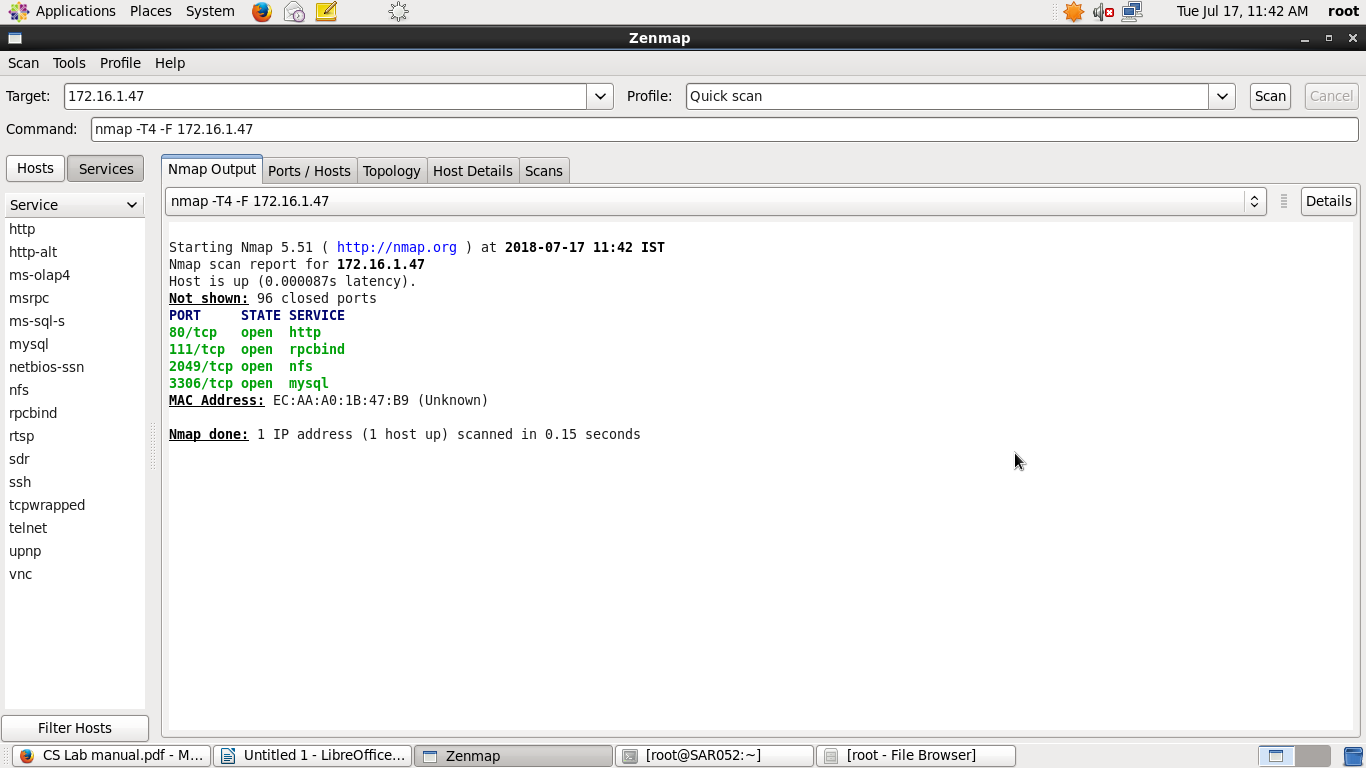
9.Scan a host to detect firewall.



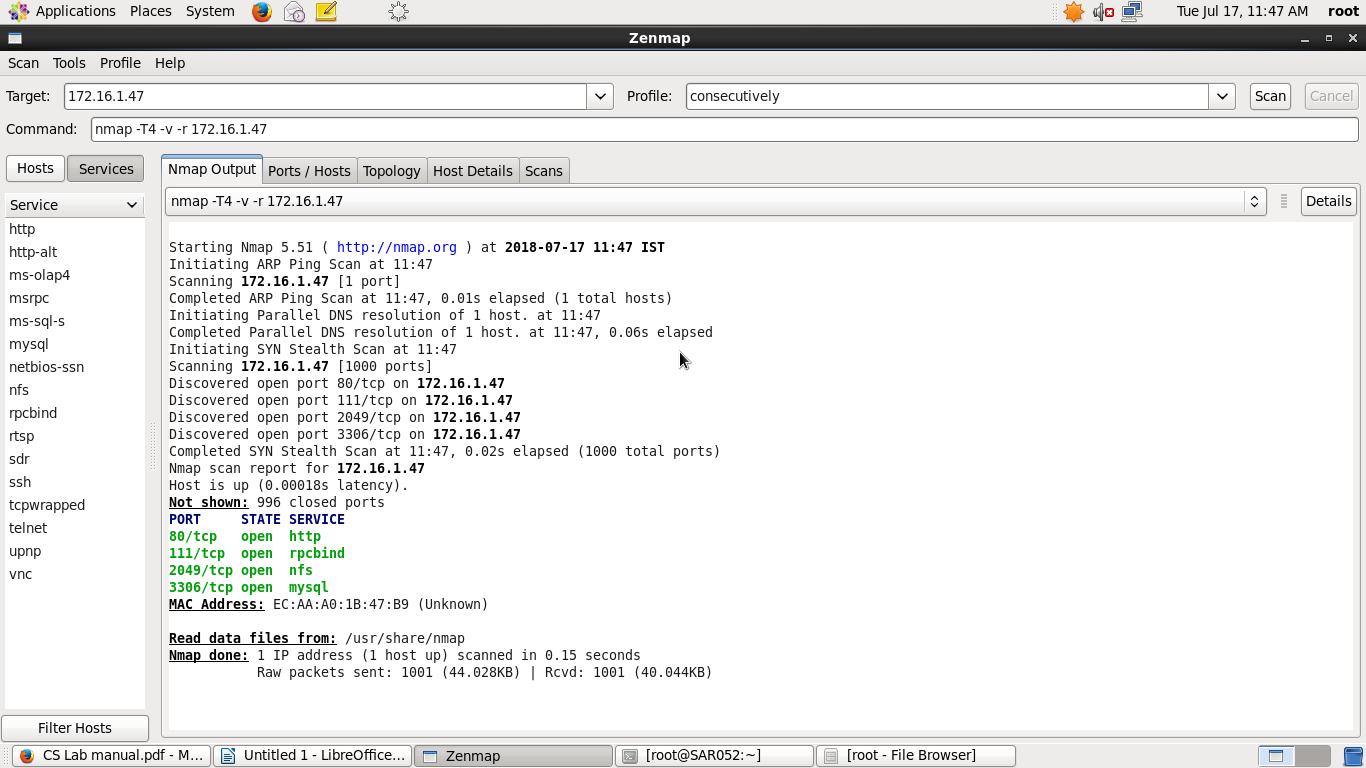
10.Scan a host to check whether its protected by a firewall or not.



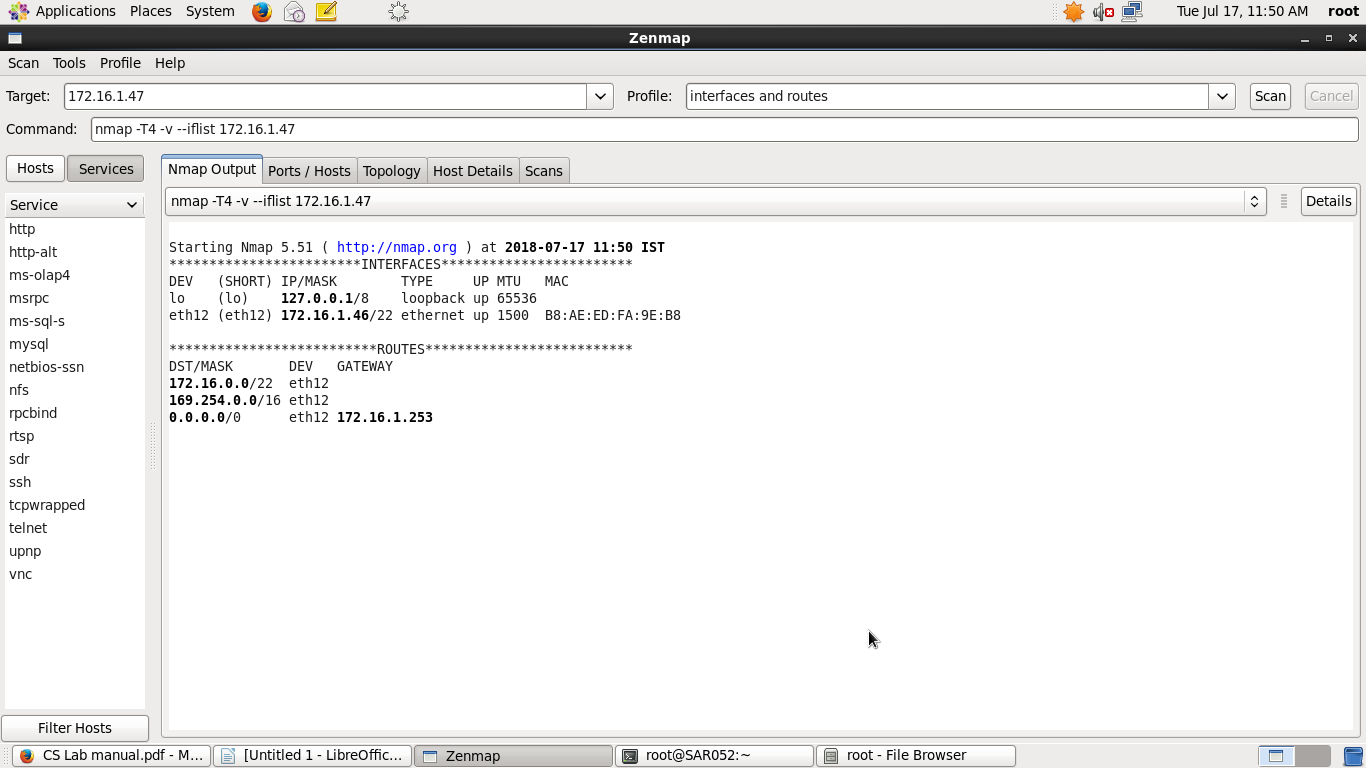
11.Perform fast scan using ZENMAP.



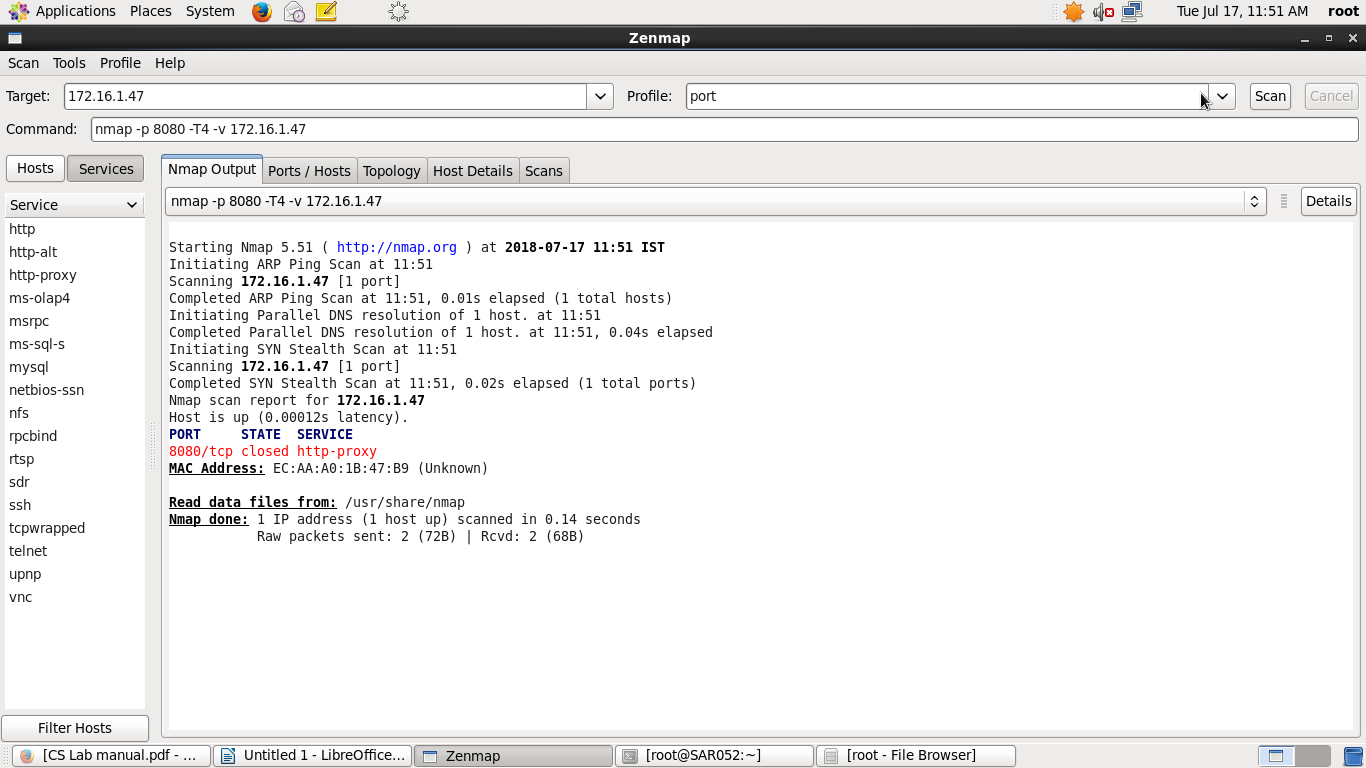
12.Scan port consecutively.



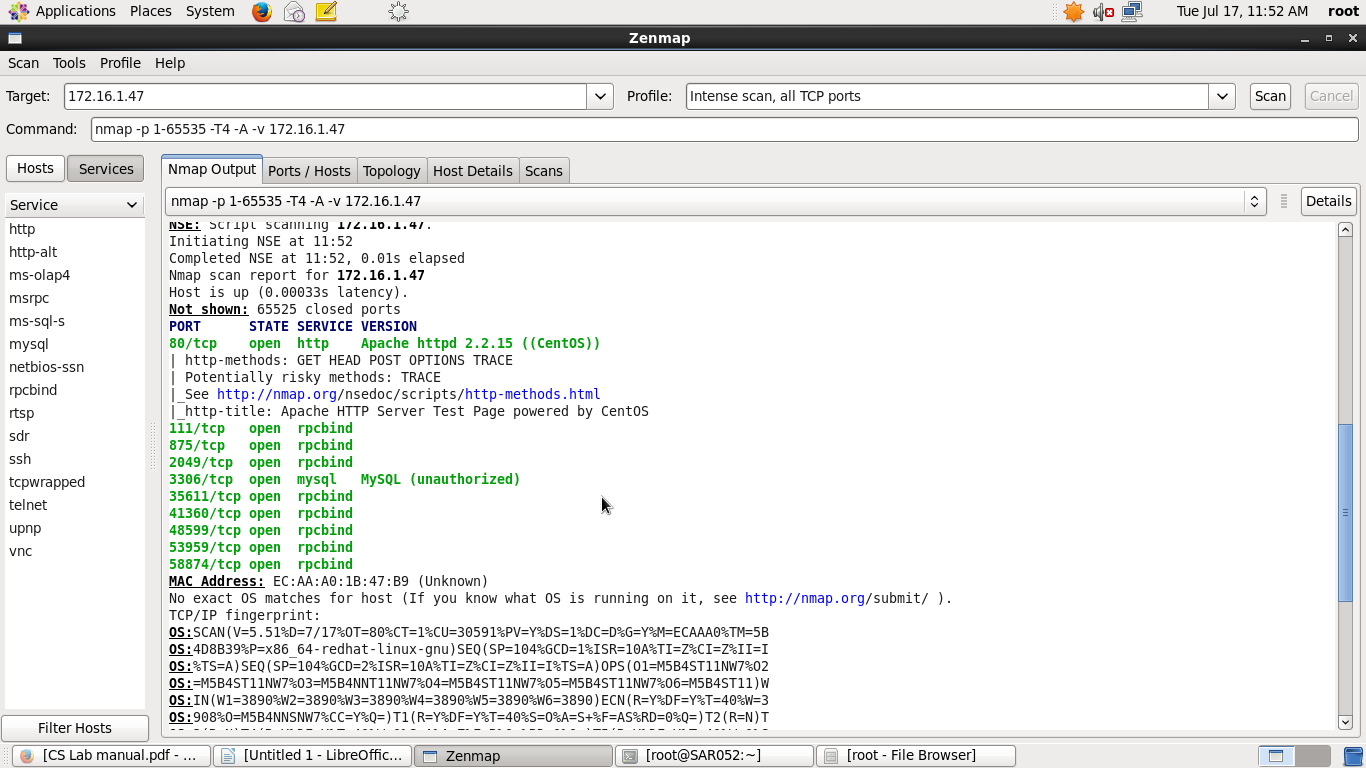
13.Print hosts interfaces and routes.



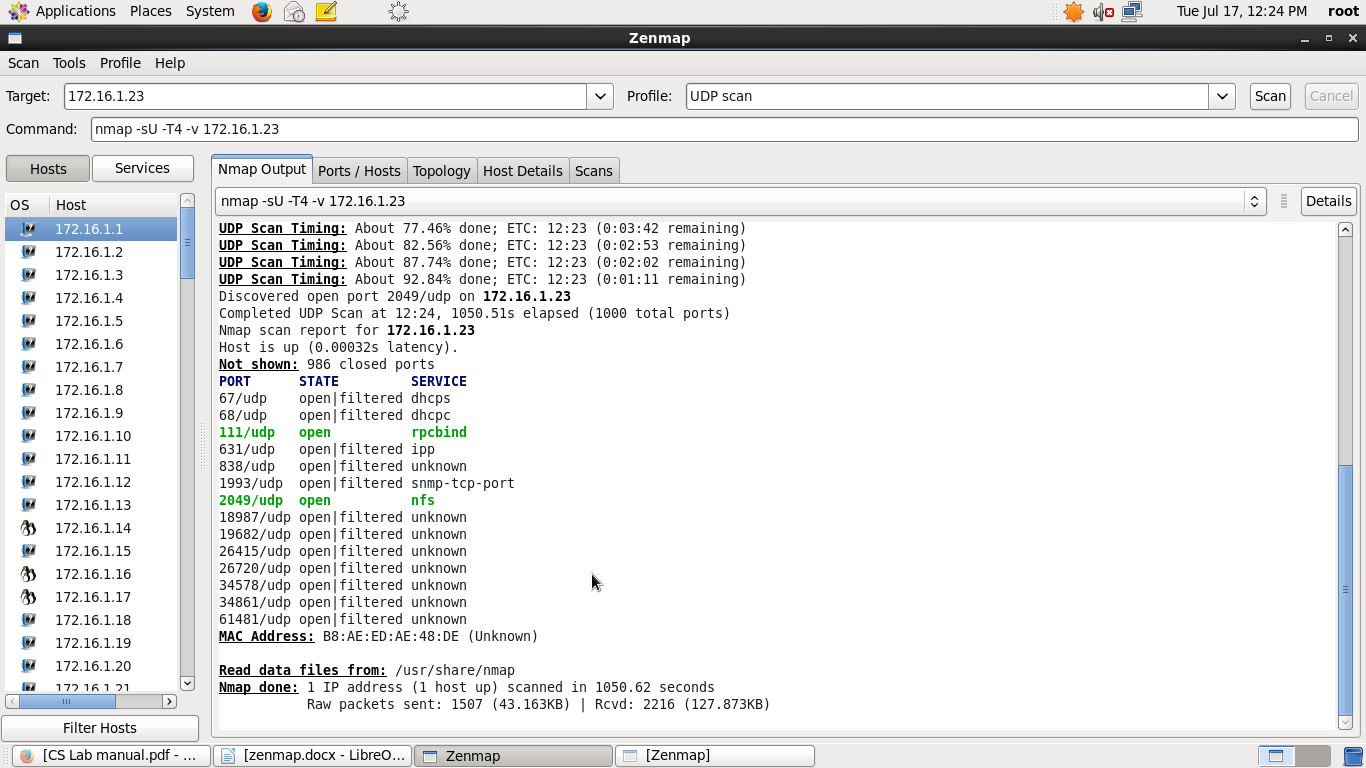
14.Scan for a specific port.



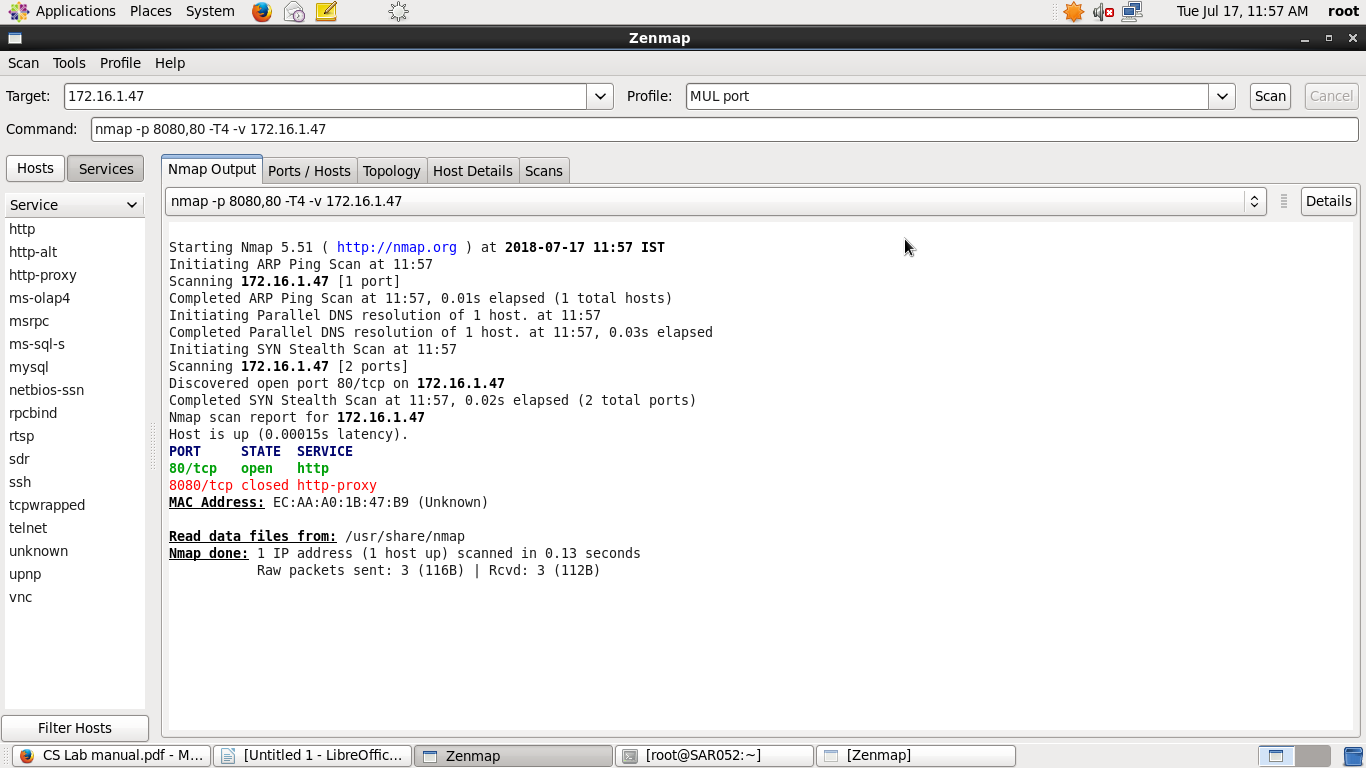
15.Scan for TCP port.



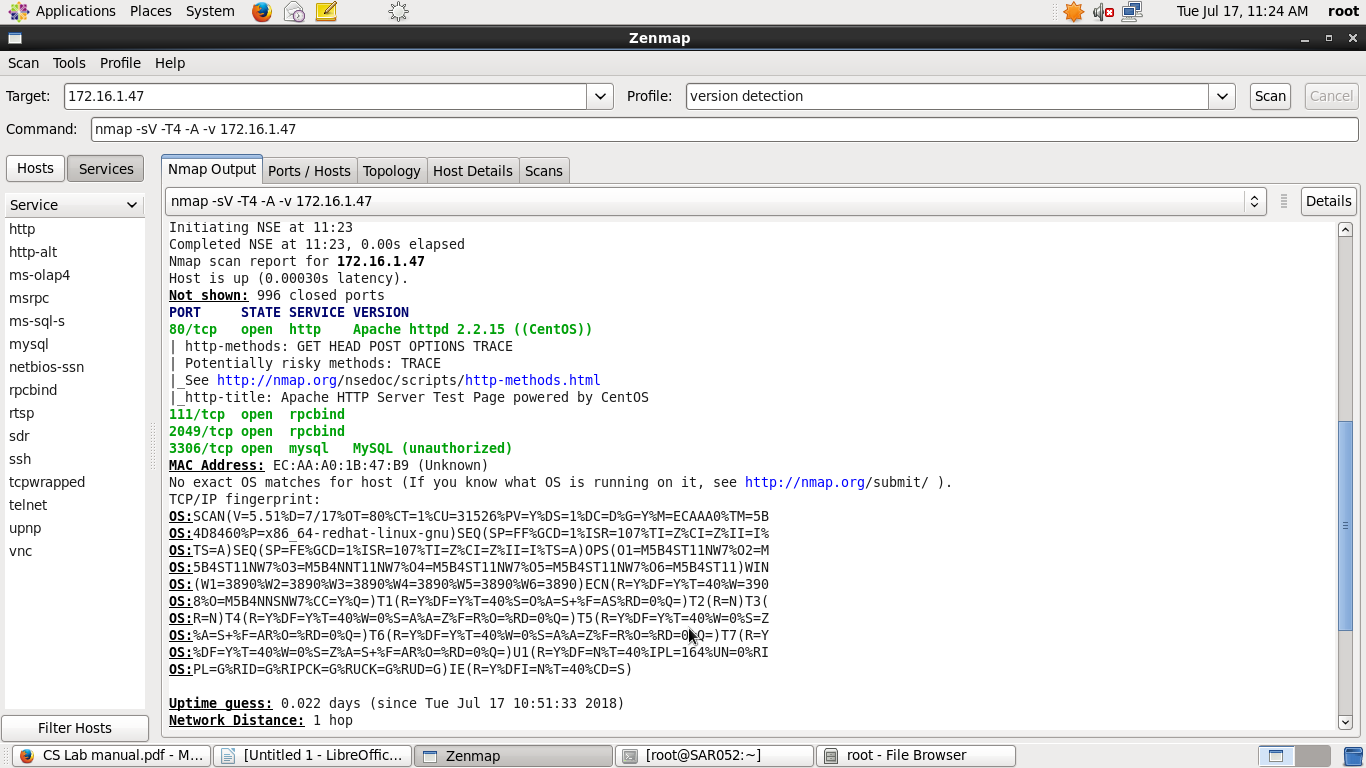
16.Scan for UDP port.



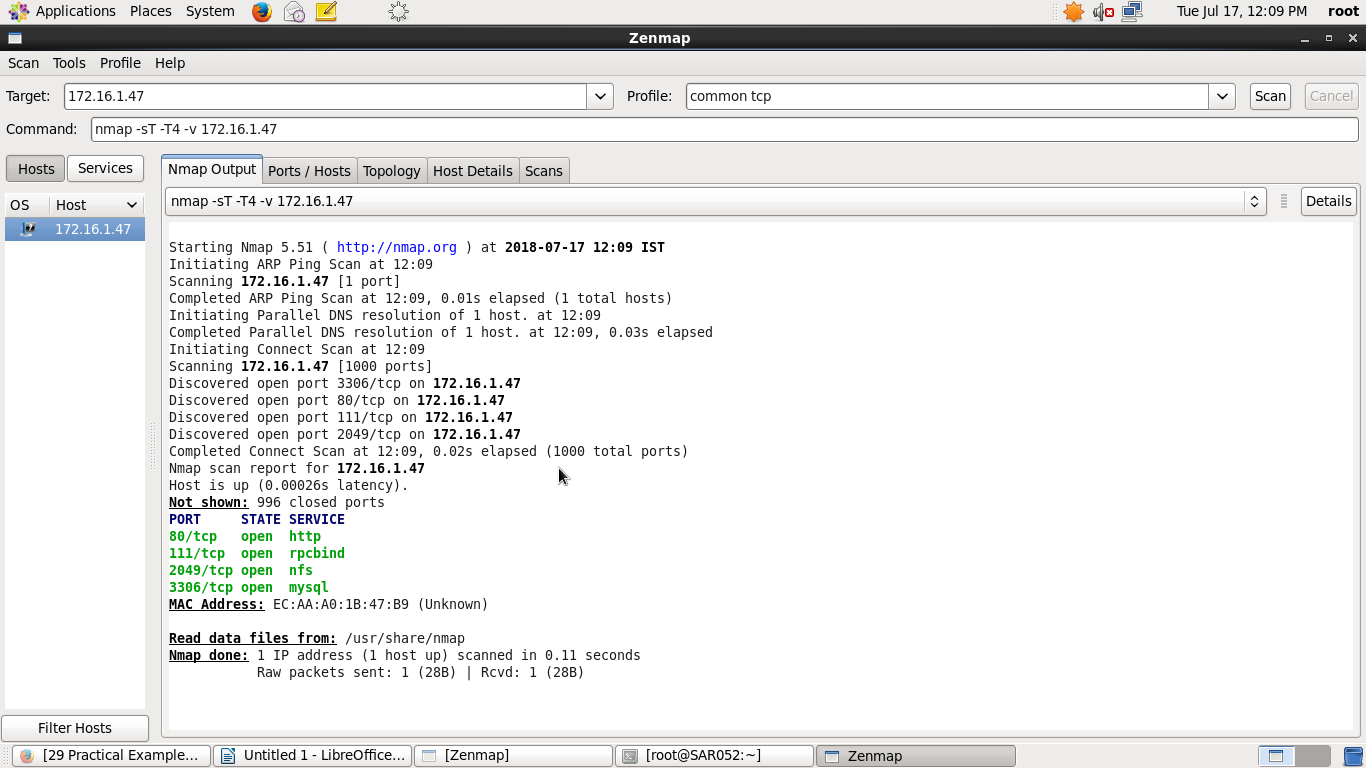
17.Scan for multiple port.



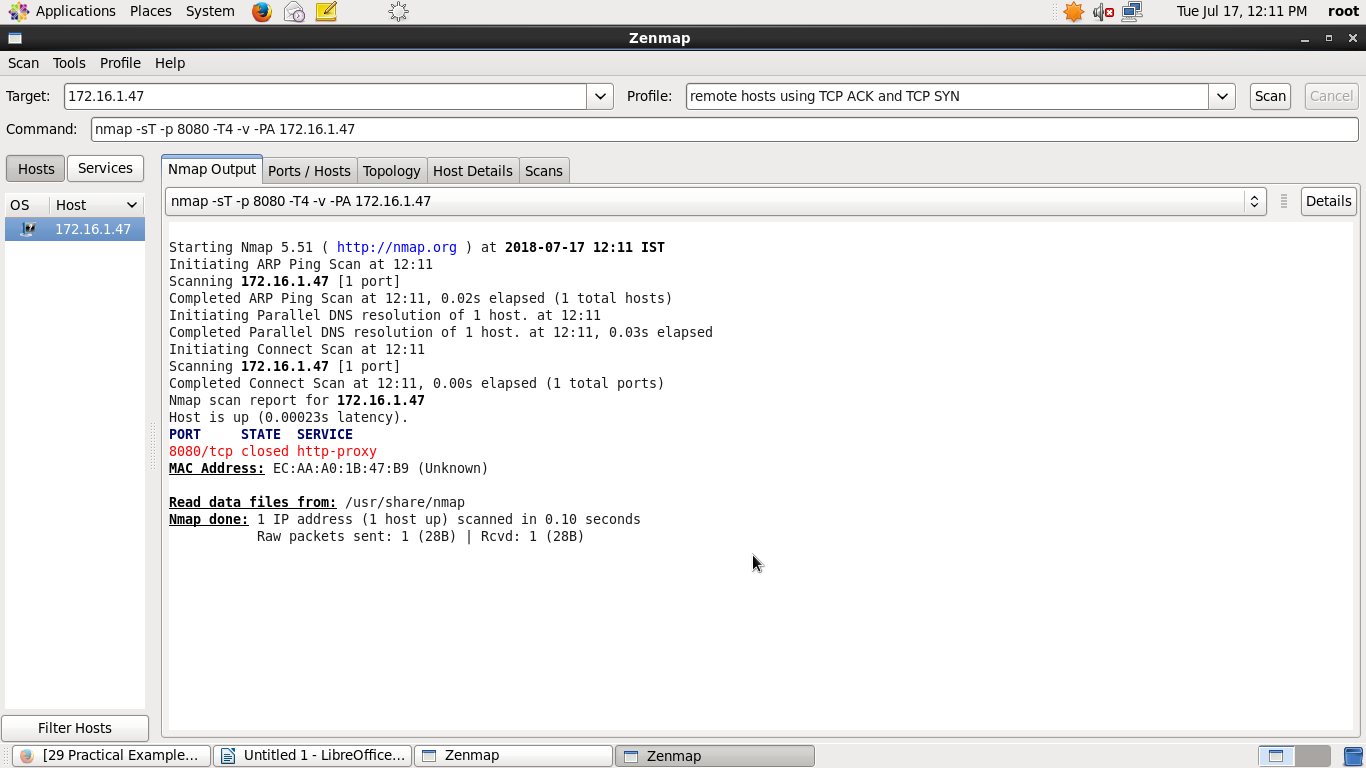
18.Find host services version no.



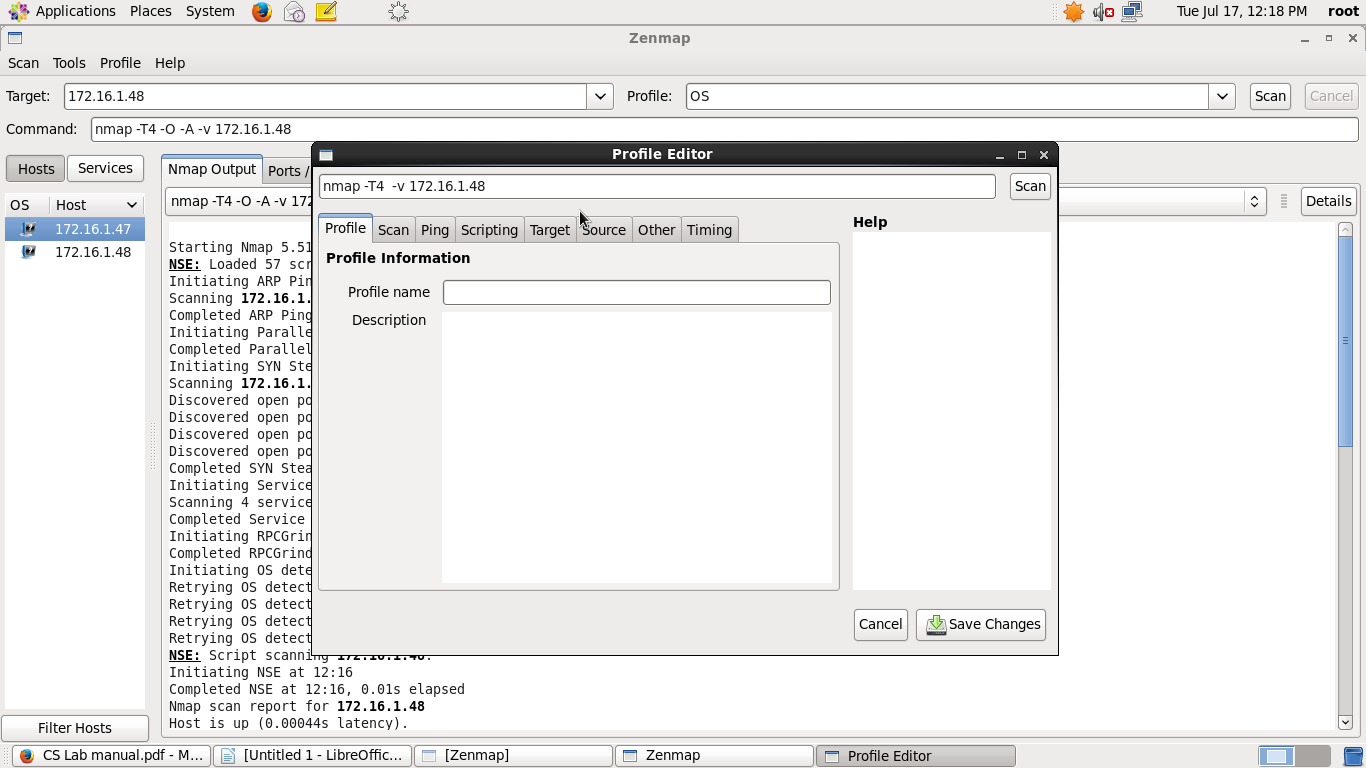
19.Perform can to find most commonly used ports using TCP syn.



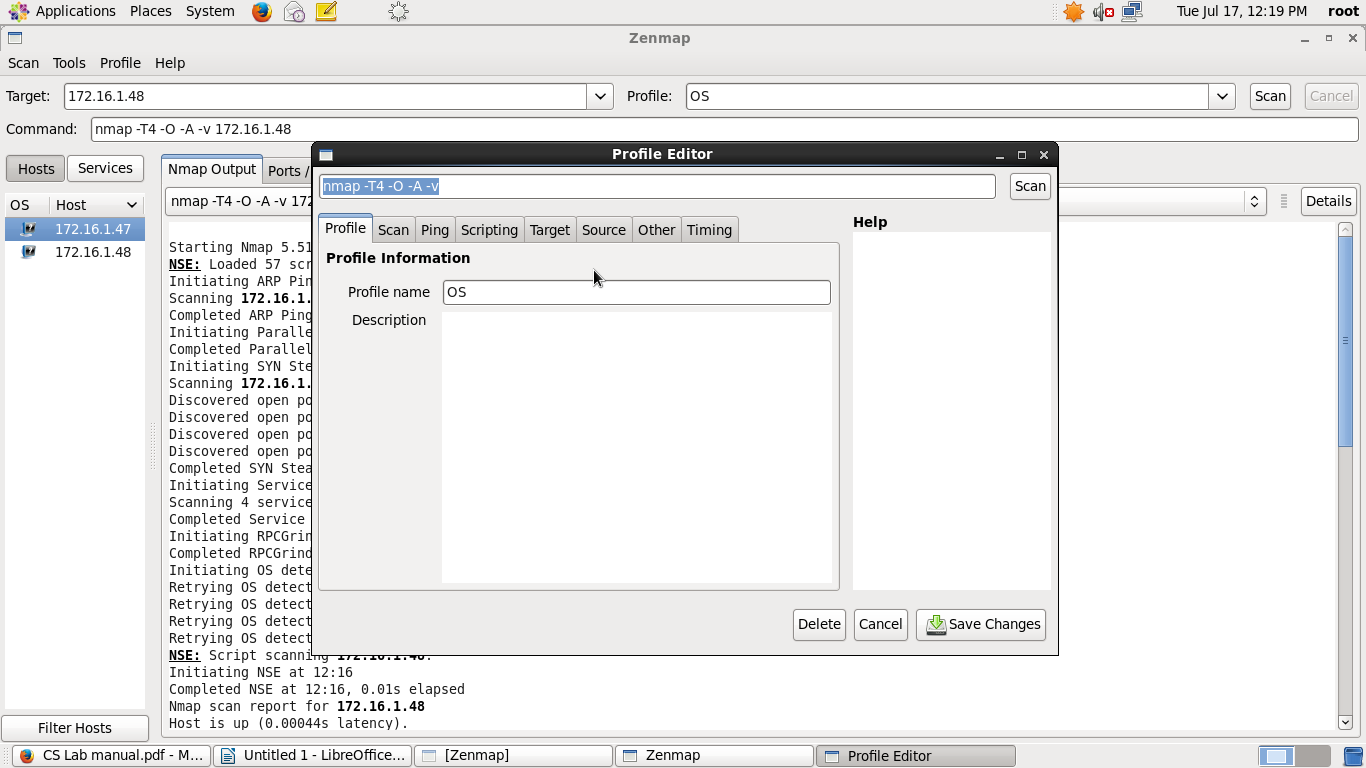
20.Scan remote hosts using TCP ACK and TCP SYN.



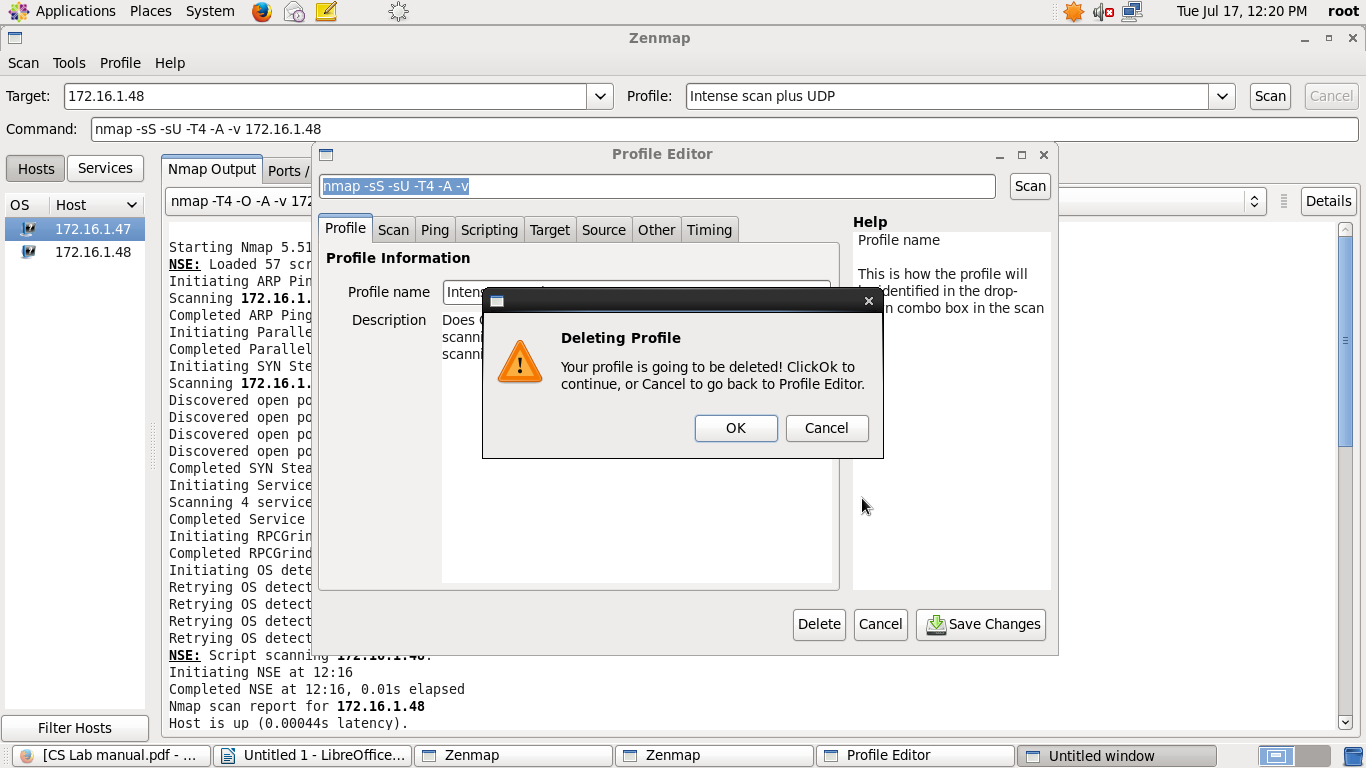
2.Create different profiles and scan target using that profile.



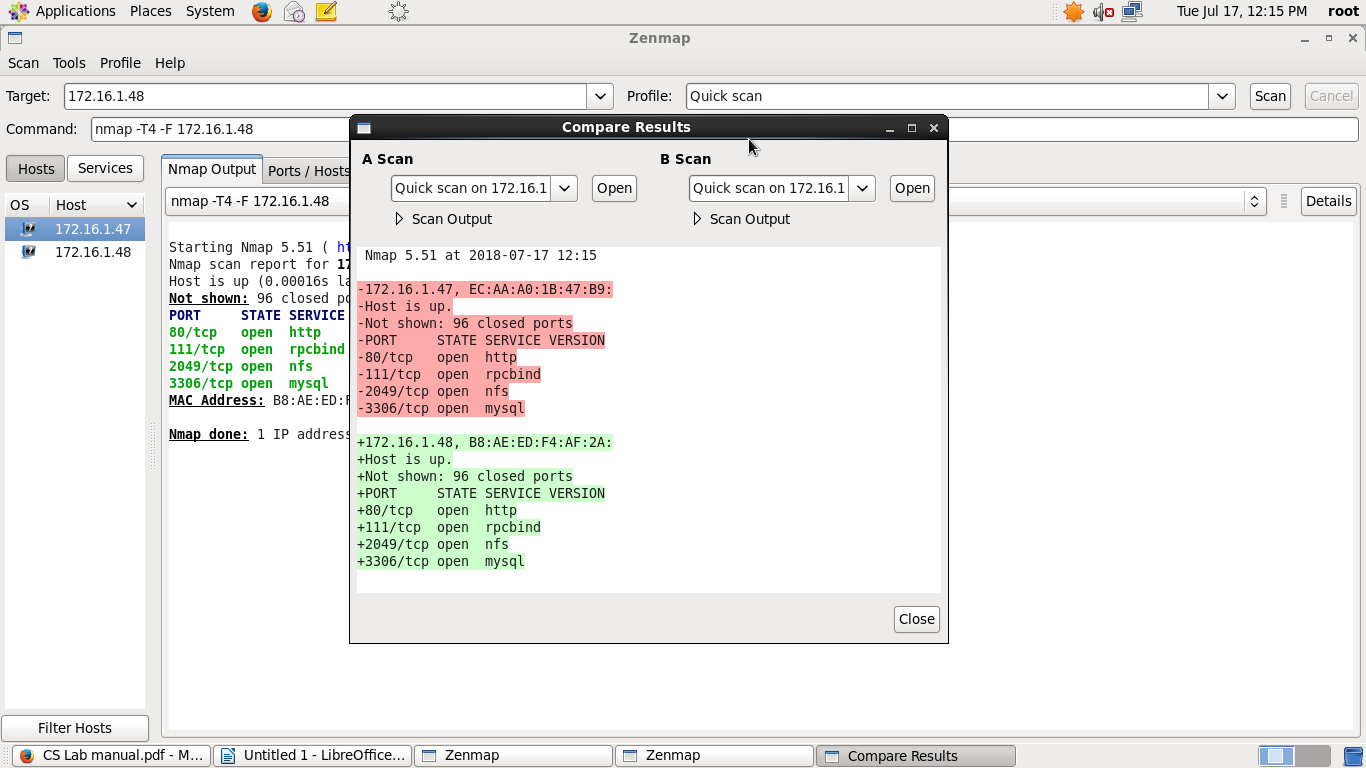
3.Edit existing profiles and perform scan.



4.Delete all the profiles created by user.



5.Compare results for 2 different hosts.



6.Compare results for same host with different options.

