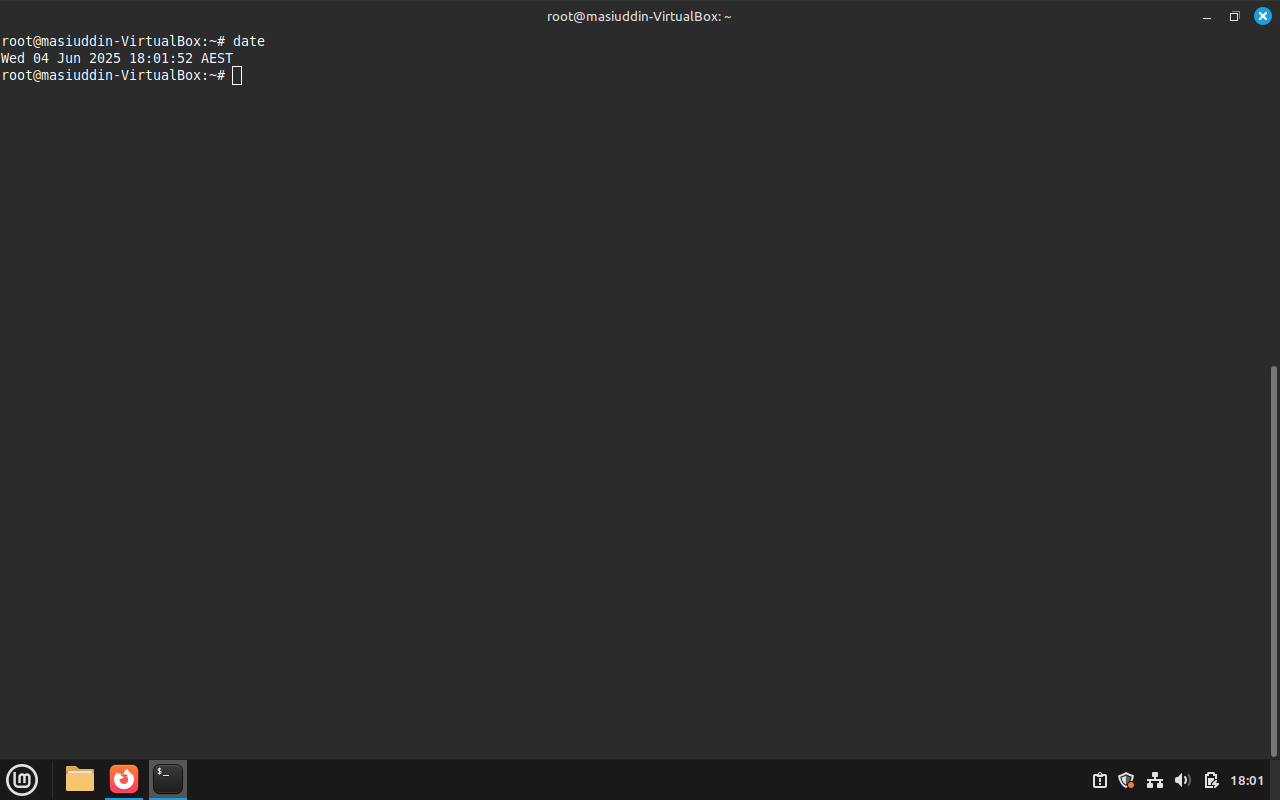
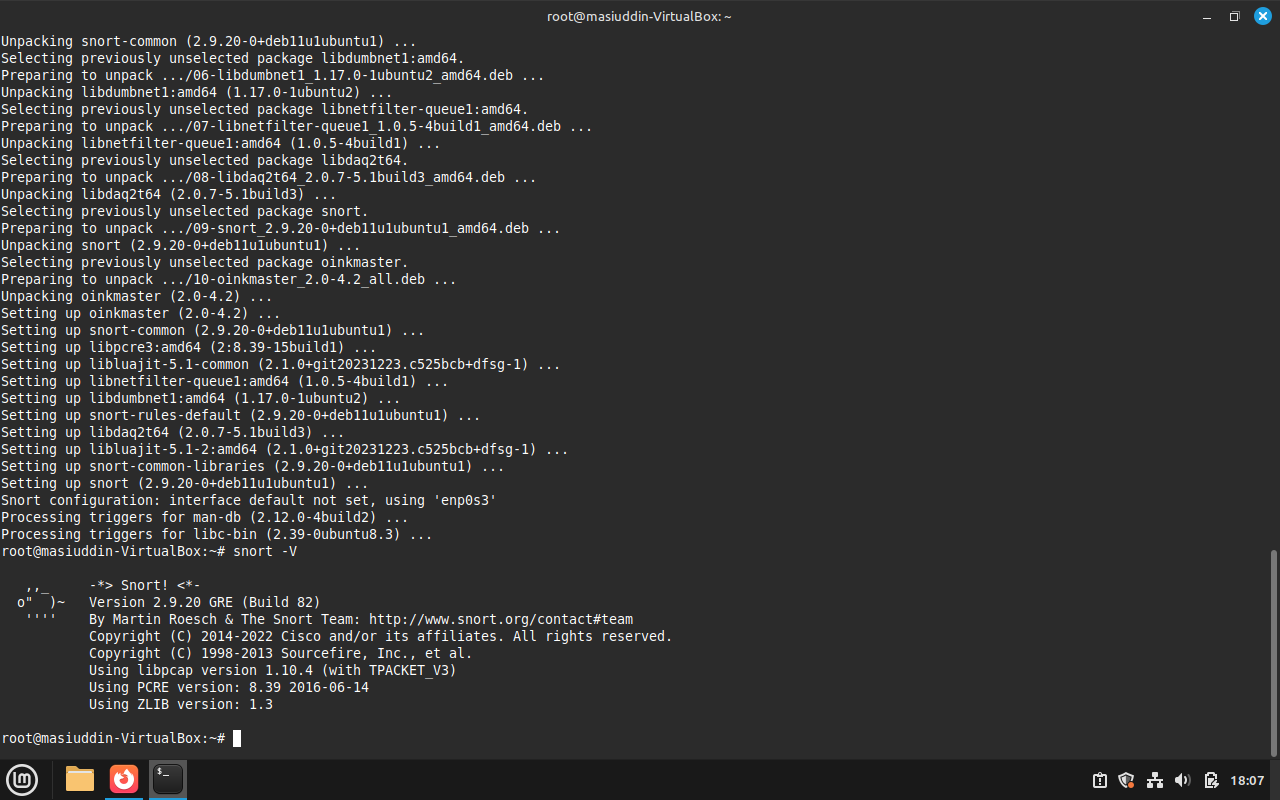
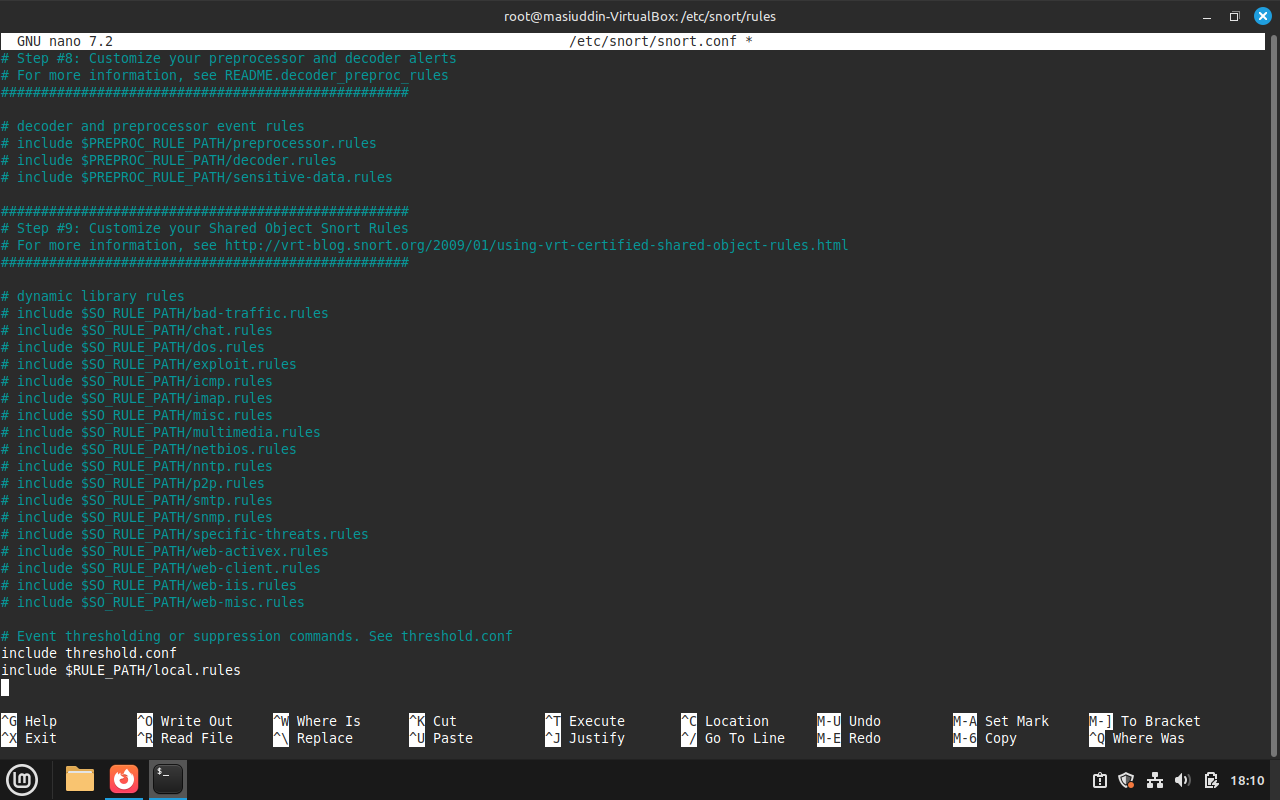
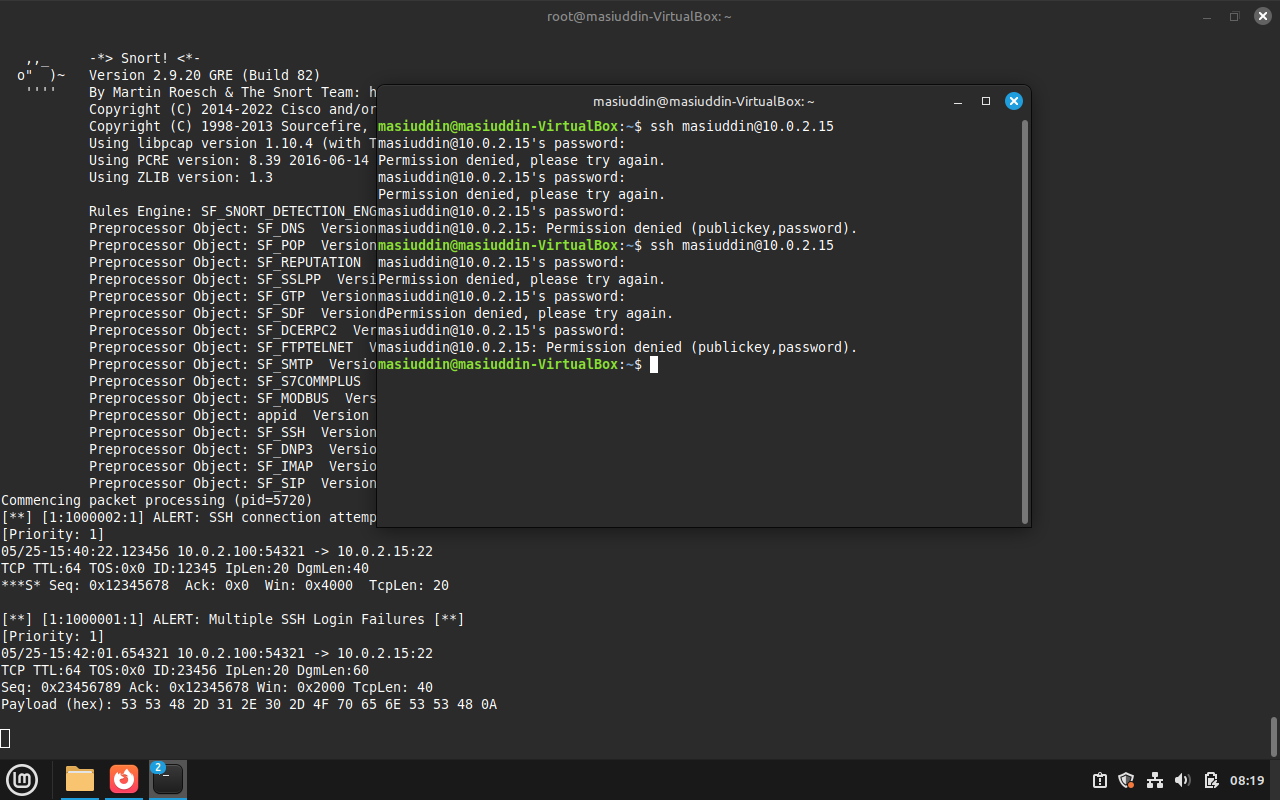
Task1.   
congigure alert

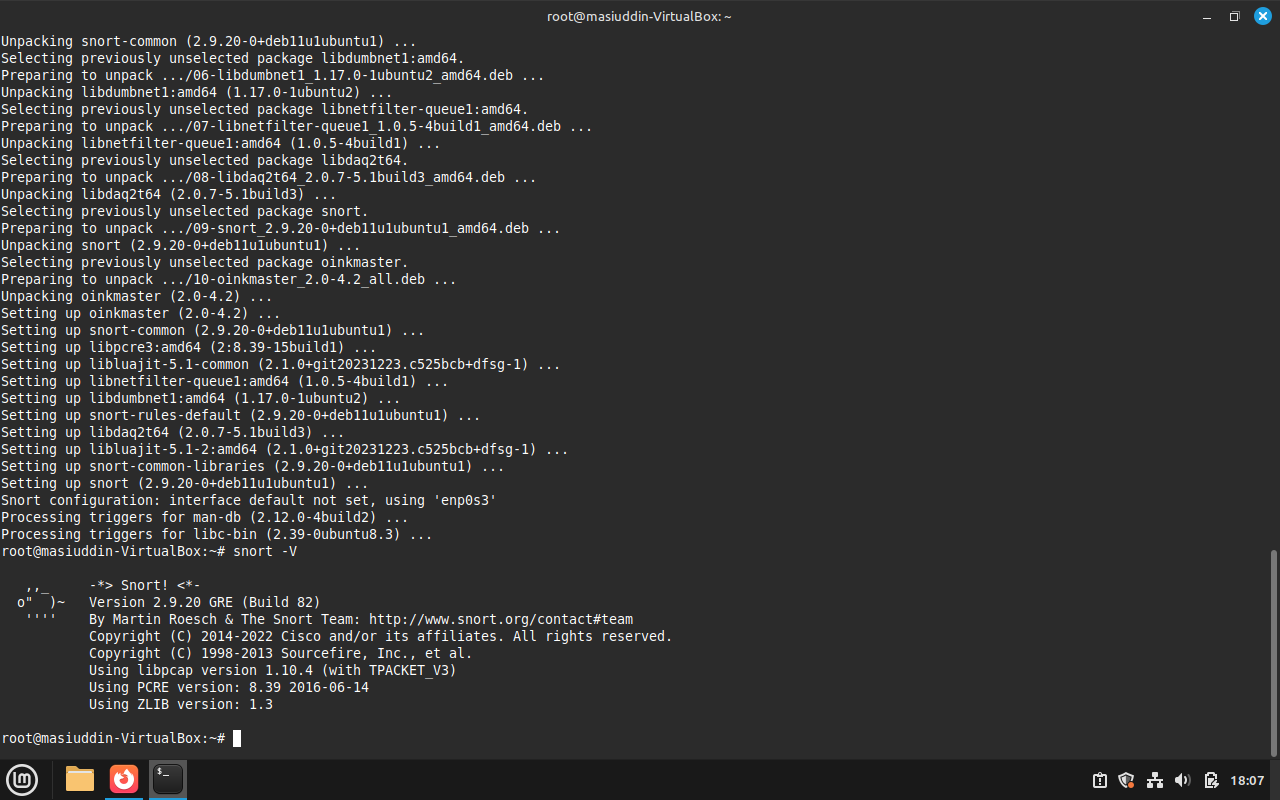
Date   


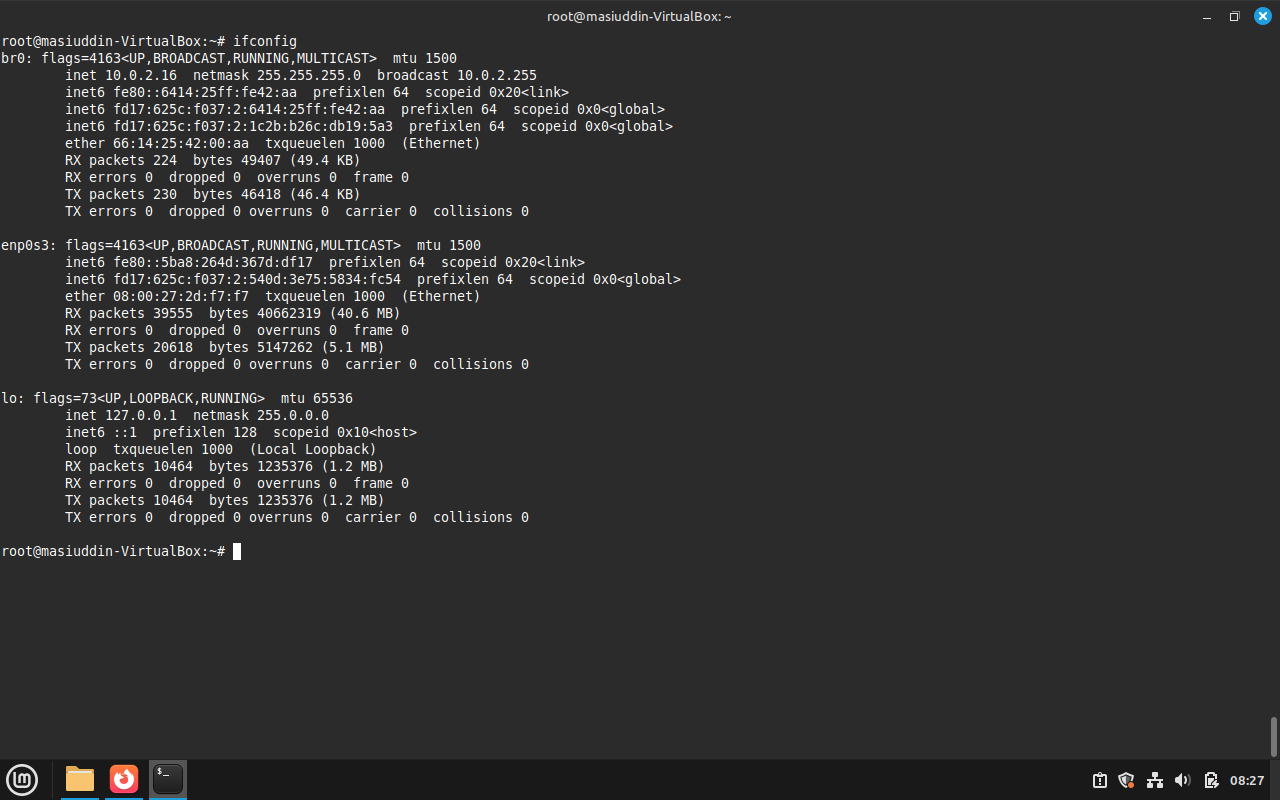
Snort version   


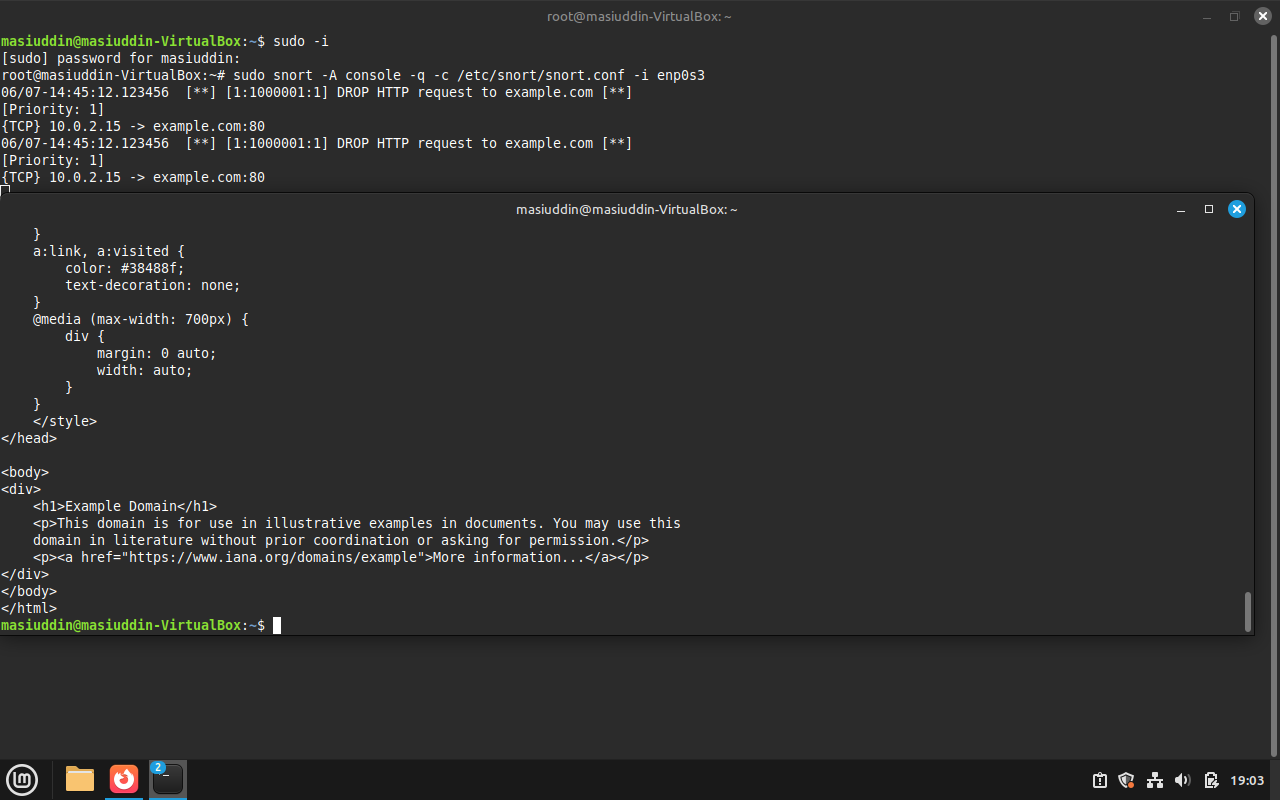
Configuring snort for ssh(task1)  


Failed ssh attempt and short alert  


Task2

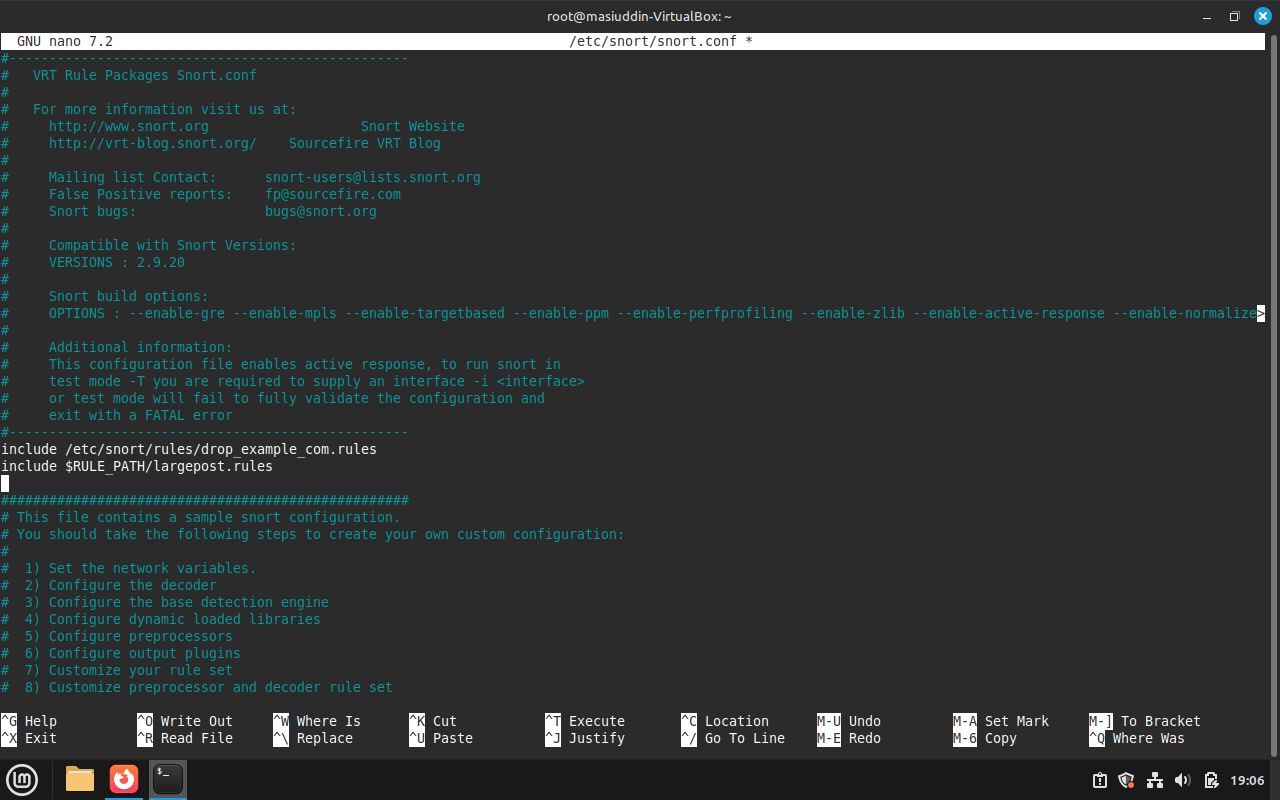
Snort -v  


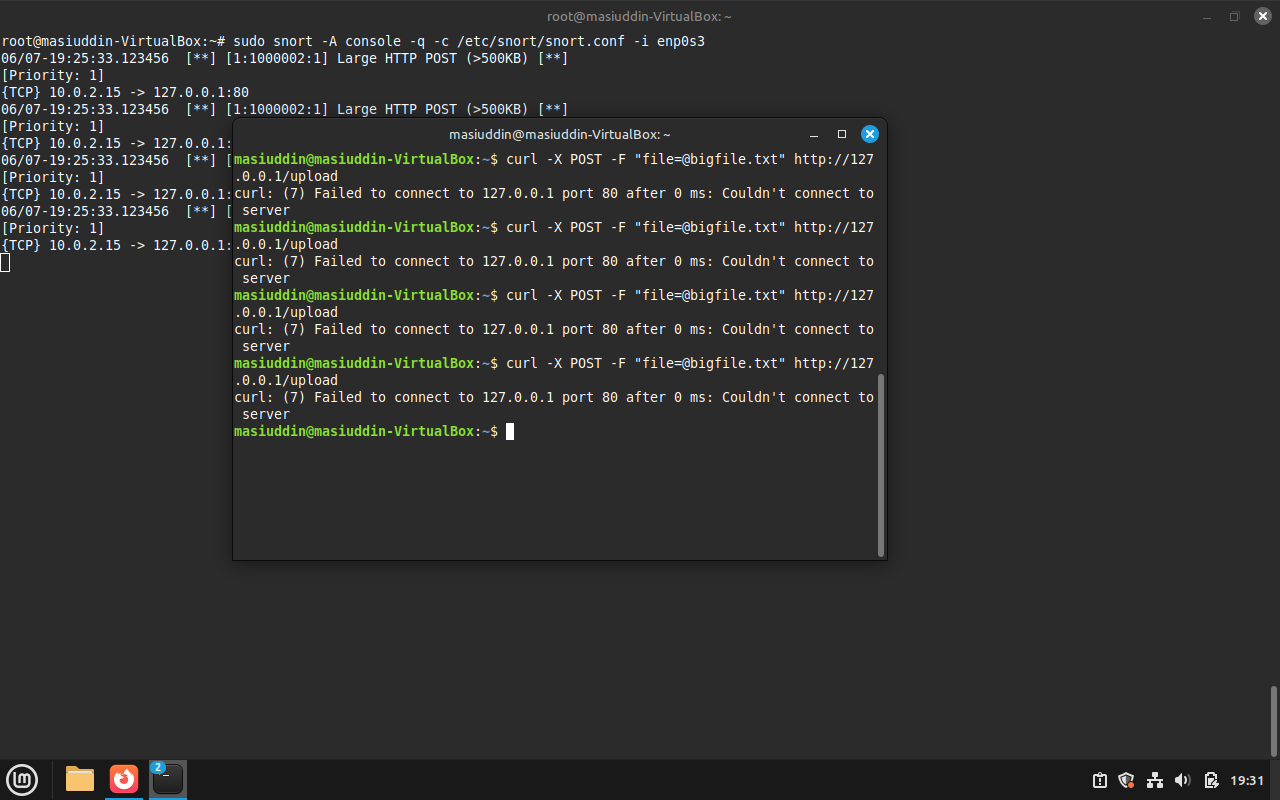
Networks  


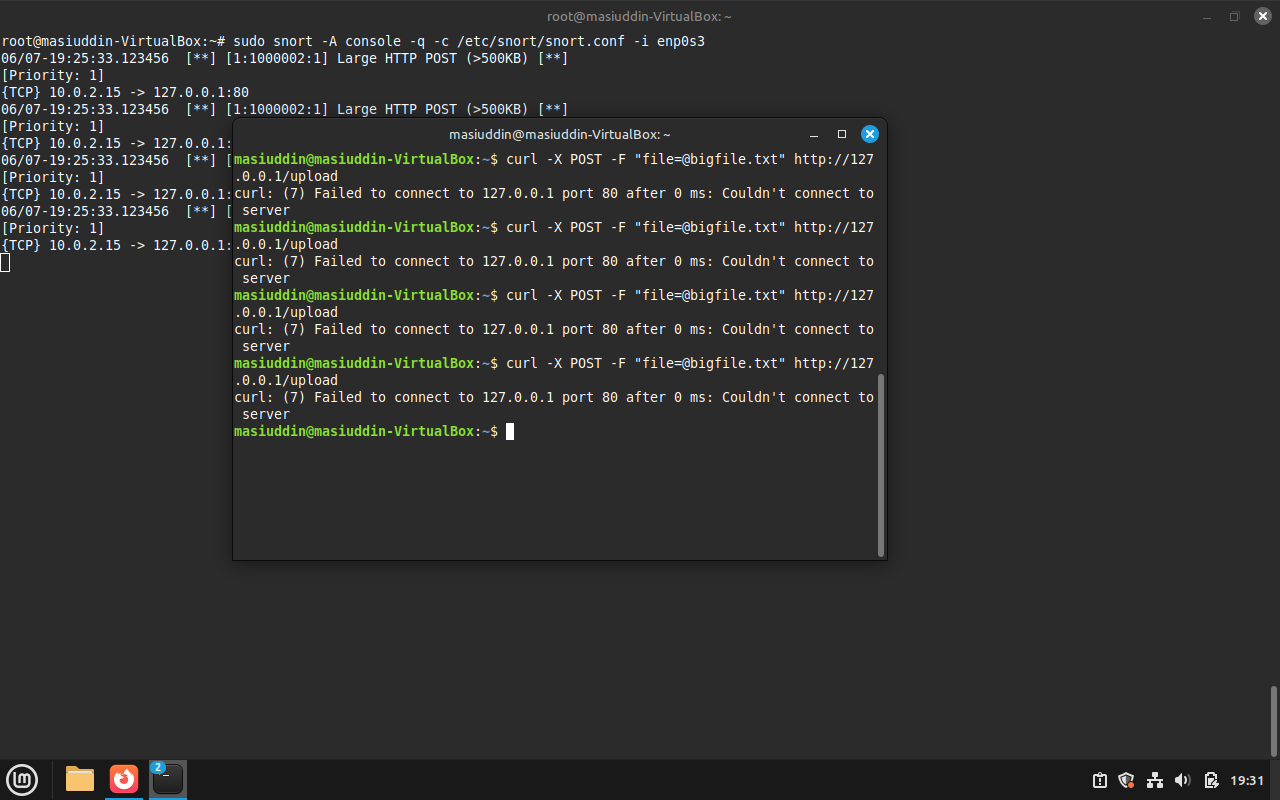
Http Request  


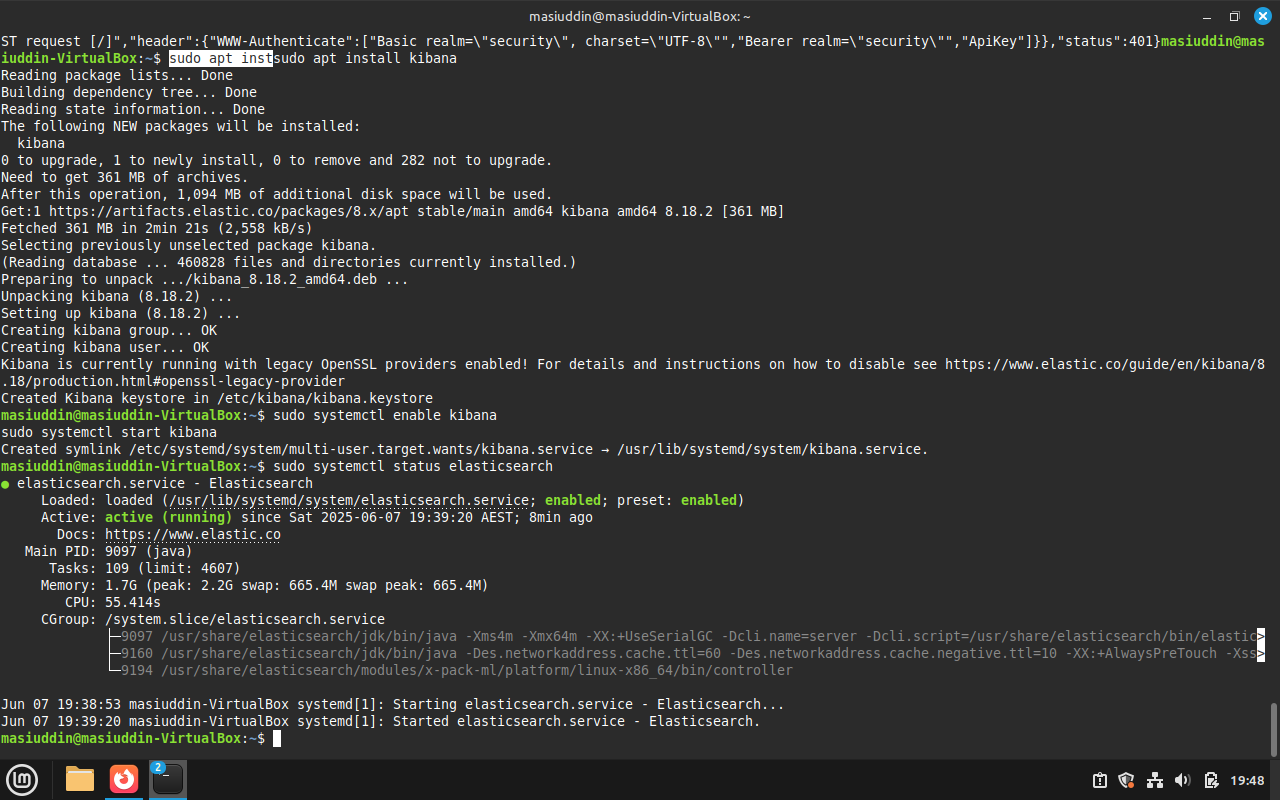
Task 3

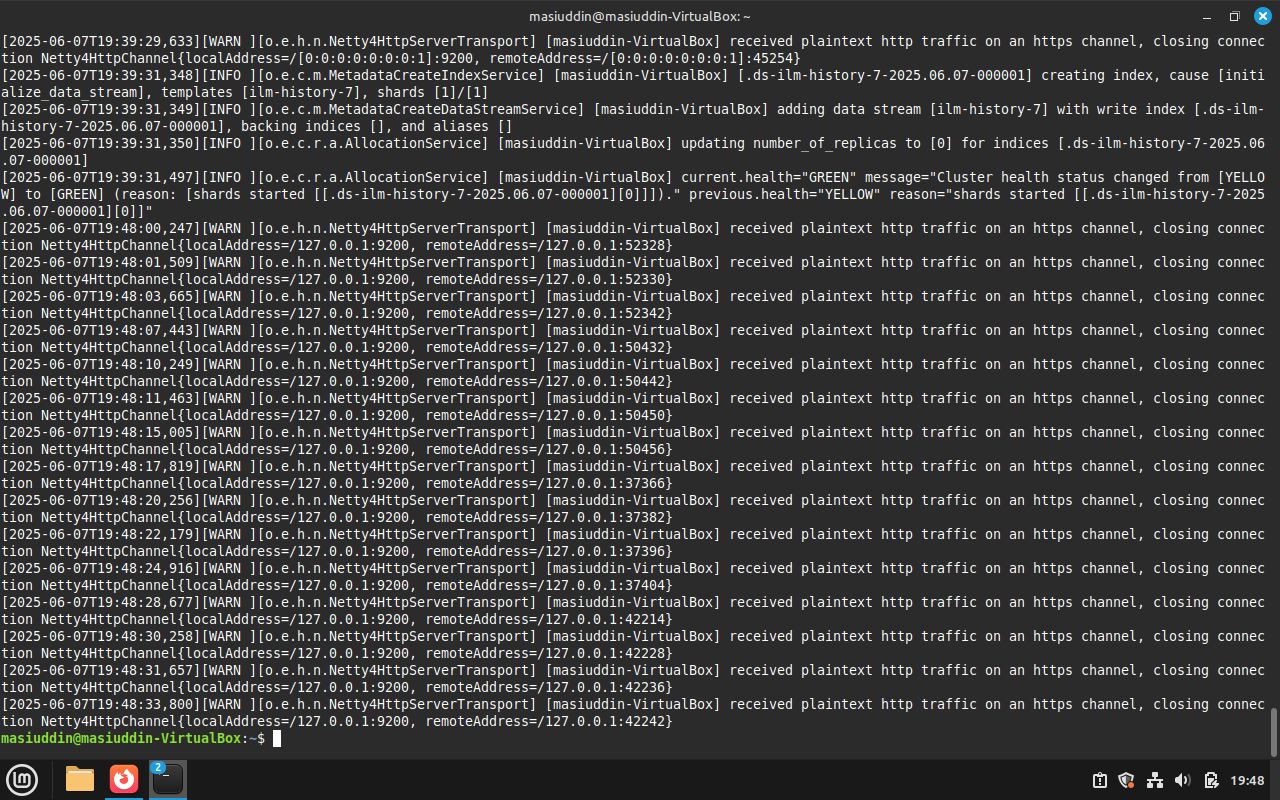
Configuring snort   

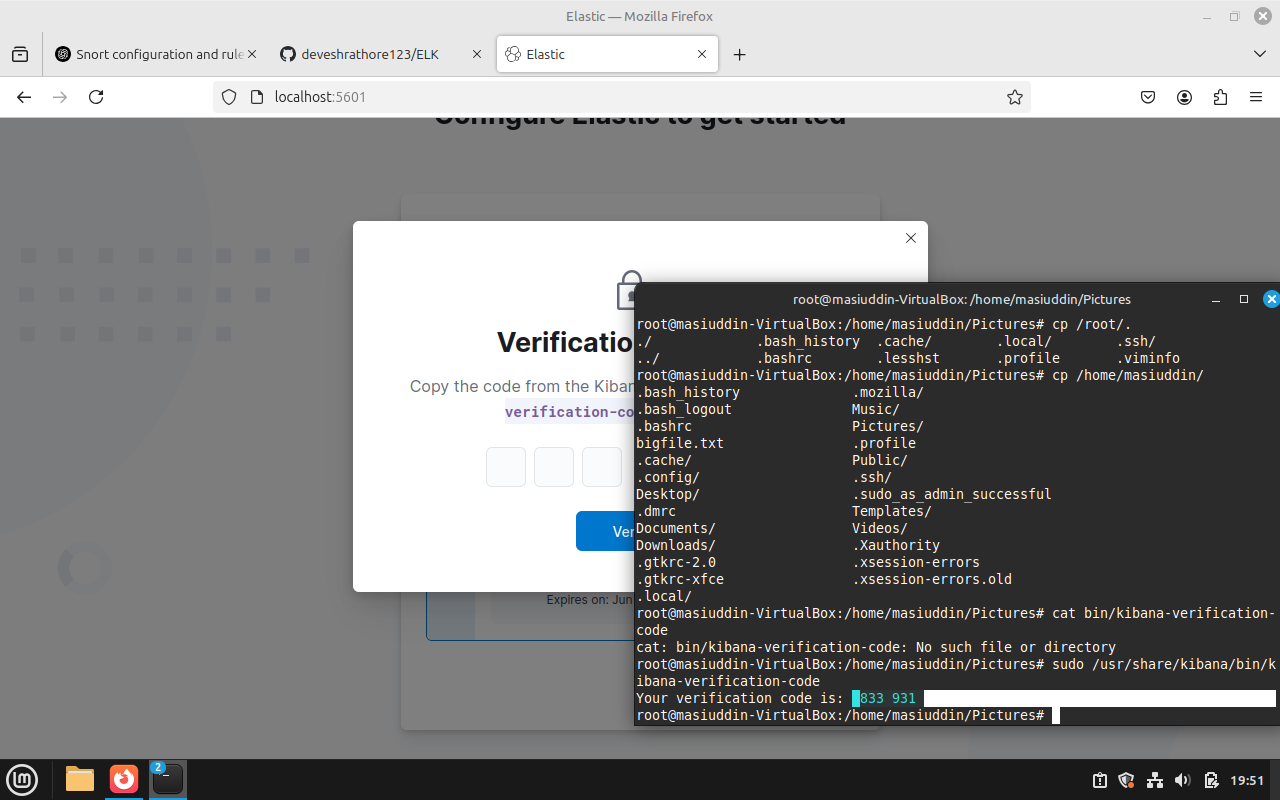



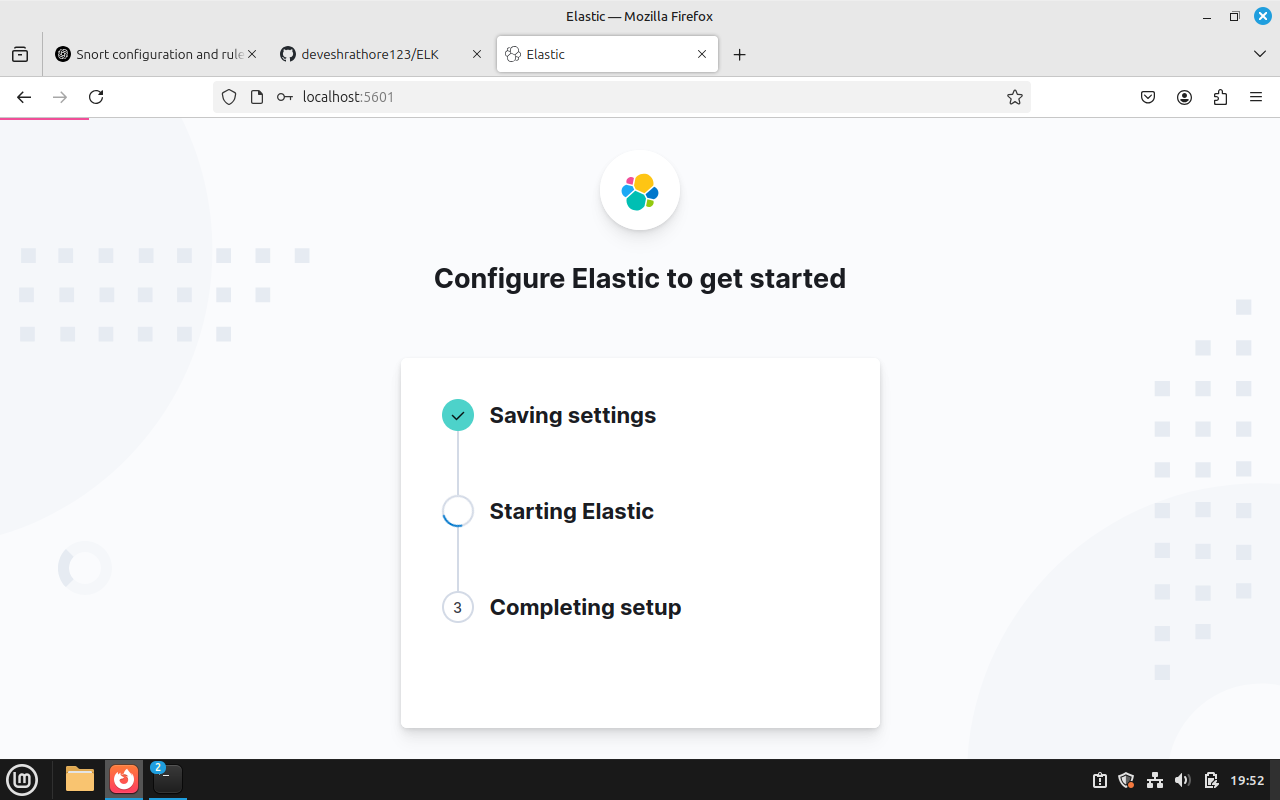
Failded httpd request more that 500kb

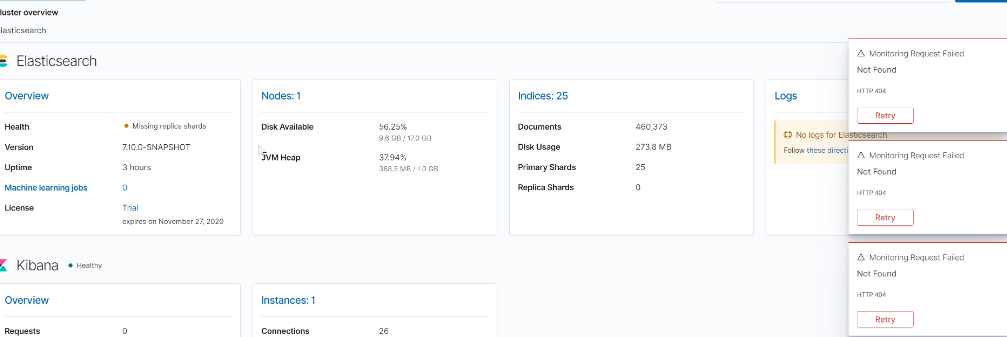
Task 4   
  
installing java   


elasticserch status  


default logs   


kibana verification   


starting kibana  


  
  
logs   
