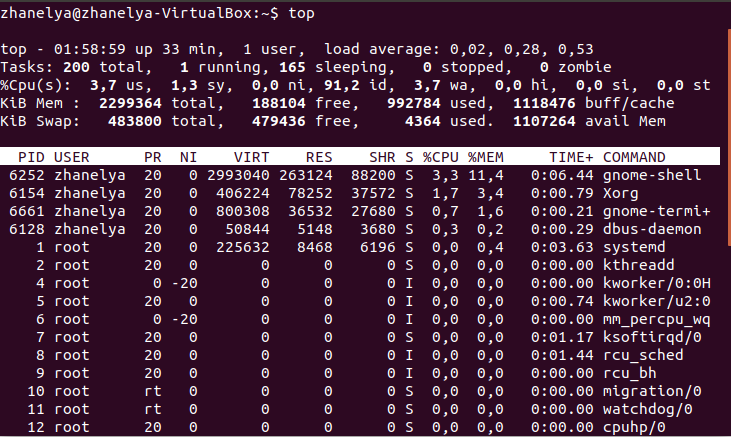
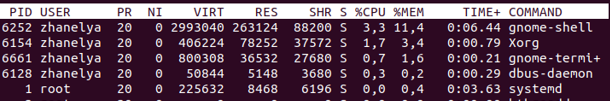
1. Show list of all processes and system’s resource usage, put the screenshot and briefly describe what you see in the output.

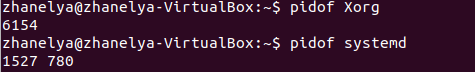


1. Launch some program and try to find it in process list. Find the process id of this program and all ids of processes that is launched by this program.

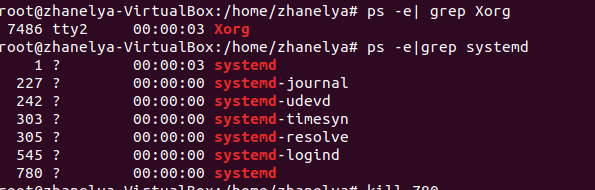
\*Find in process list



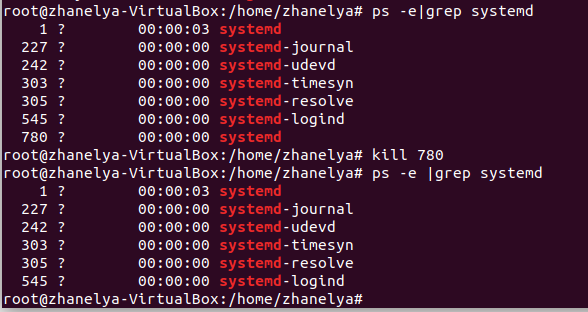
\*Find id of programs



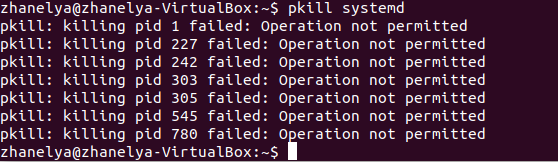
\*Find all processes in program



1. Try to kill these processes one by one

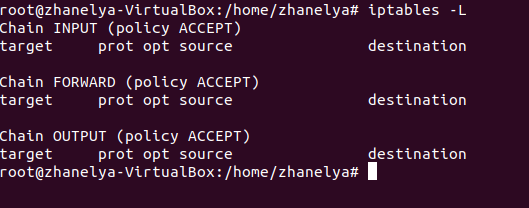


1. Try to kill all related processes at once.

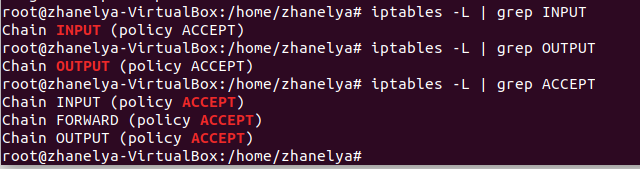


PART 2

Firewall 1. Display the current status of firewall with detailed information. Attach the screenshot of output and explain what each of the columns means?

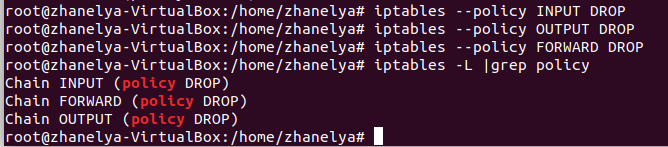


2. Give the definition to each of chain rule and display firewall status for each rule.

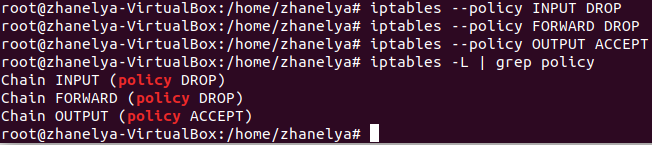


3. Set default firewall rules. Test the connection after setting every rule:

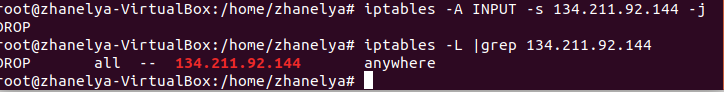
a. you won’t be able to connect to anywhere



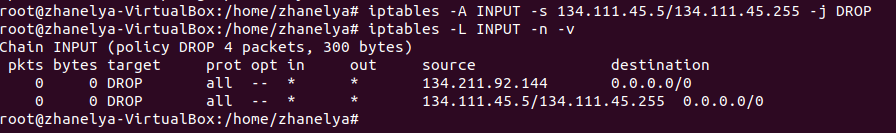
b. allow only outgoing traffic



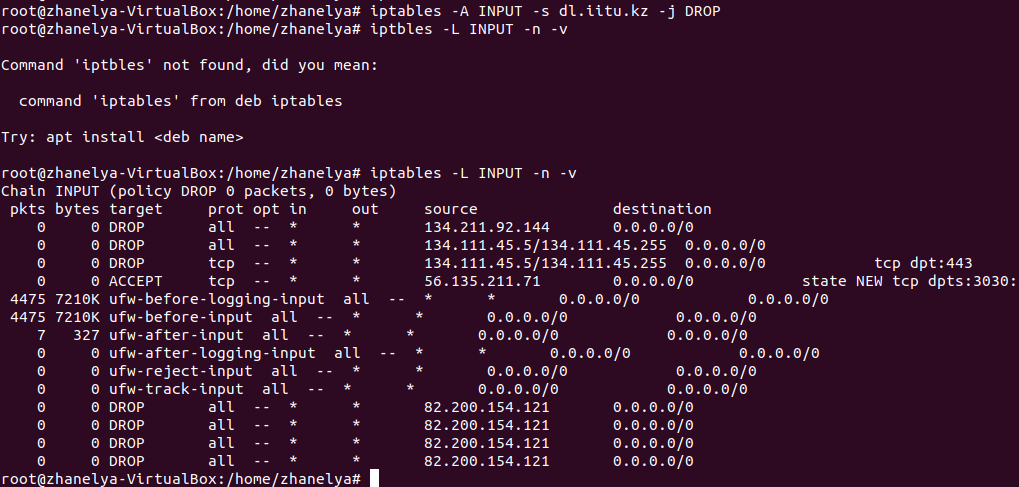
4.Suppose the server is being bruteforced from IP 134.211.92.144. You should block this IP address



1. After blocking previous IP address attackers decided to change IP addresses from 134.111.45.5 to 134.111.45.255. Block all these IP addresses.

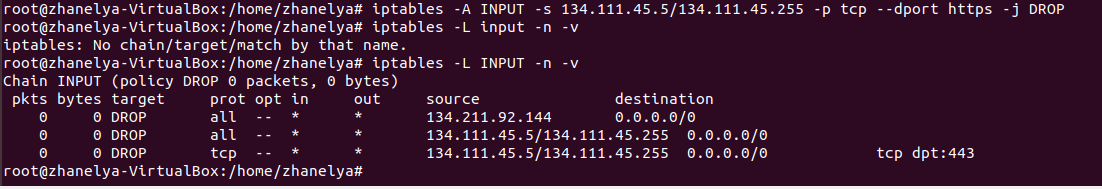


1. Block connection to dl.iitu.kz

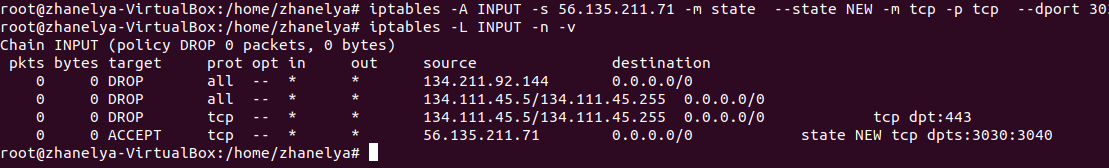


7. Block all incoming HTTP and SSL requests

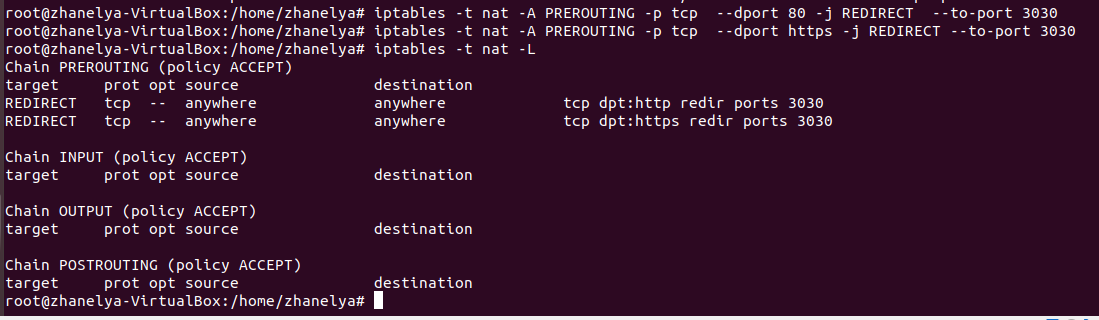
a. block incoming requests from attackers’ IP address



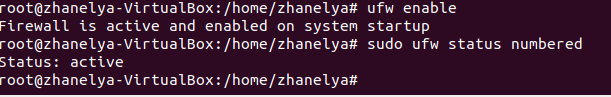
8.You wrote a program that opens ports from 3030 to 3040. The company A uses these ports to connect to your server. This company has an IP address 56.135.211.71. Allow only this IP address to connect to given ports.



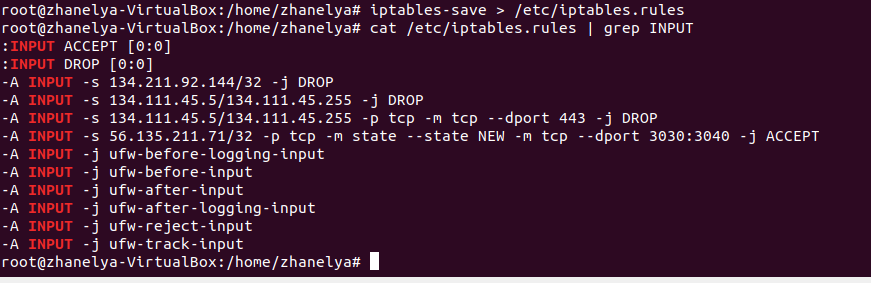
9. Some month later you decided to redirect all HTTP and SSL request to port 3030. How will you do?



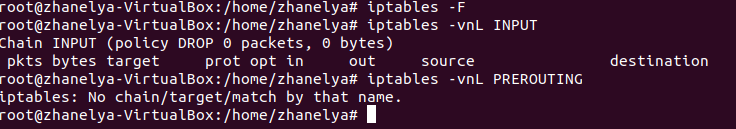
10. Test your firewall



11. Save all firewall rules



12. Delete all rules



10. Restore saved firewall rules

