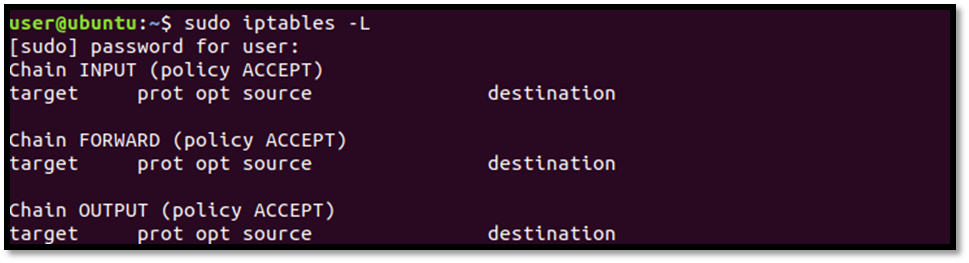
# **3.8 Guided Exercise: Configuring iptables Rules**

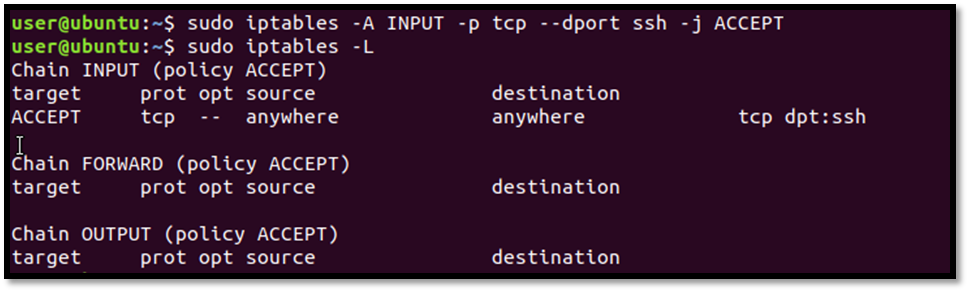
|  |  |
| --- | --- |
| **Resources** | |
| Files | None |
| Machines | Ubuntu Server |

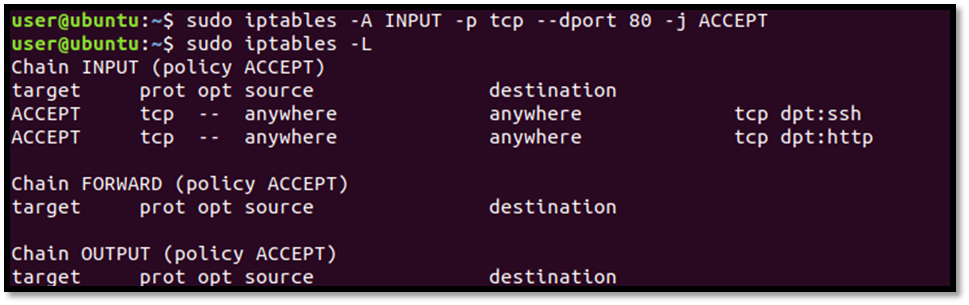
In this exercise, you are required to write custom iptables rules.

Login to Ubuntu Server and then run the command “sudo iptables -L”. It will ask for the user password. Enter the user password which is “Pa$$w0rd”, press enter and then it will show the current iptables rules.



Write the command “sudo iptables –A INPUT –p tcp --dport ssh –j ACCEPT” and if sudo asks for the user password enter “Pa$$w0rd”.  Then run the command sudo iptables –L to list the iptables rules.

  
Write the command “sudo iptables –A INPUT –p tcp --dport 80 –j ACCEPT” and if sudo asks for the user password enter “Pa$$w0rd”.  Then run the command sudo iptables –L to list the iptables rules.



To save the iptables rules run the command “sudo iptables-save”.

