QUESTION-5

Initially, I wrote the command which ensured that already established connections were accepted.

- sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

We know for SSH the port is 22 and for RDP the port is 3389. To Allow only admin IPs to access SSH/RDP in my case i have taken “192.168.1.3” as admin IP and log unauthorized attempts.

To achieve this:

- First I have created a new chain `SSH_RDP_RULES` to manage SSH and RDP traffic separately. For good organization purposes i am using different chain.
  sudo iptables -N SSH_RDP_RULES
- Now I am forwarding all incoming SSH and RDP requests to the SSH_RDP_RULES chain.
  sudo iptables -A INPUT -p tcp --dport 22 -j SSH_RDP_RULES
  sudo iptables -A INPUT -p tcp --dport 3389 -j SSH_RDP_RULES
- Now allowing only admin IP to access SSH and RDP
  sudo iptables -A SSH_RDP_RULES -s 192.168.1.3 -j ACCEPT
- Now Logged unauthorized attempts which helps in monitoring suspicious activity.
  sudo iptables -A SSH_RDP_RULES -p tcp --dport 22 -j LOG --log-prefix "Unauthorized Access to SSH"
  sudo iptables -A SSH_RDP_RULES -p tcp --dport 3389 -j LOG --log-prefix "Unauthorized Access to RDP"
- Finally Dropped packets from unauthorized sources.
  sudo iptables -A SSH_RDP_RULES -p tcp --dport 22 -j DROP
  sudo iptables -A SSH_RDP_RULES -p tcp --dport 3389 -j DROP

In this part our objective is to allow web traffic on ports 80 (HTTP) and 443 (HTTPS) while blocking access from blacklisted IP range 103.25.231.0/24.

To achieve this:

- First I have created a new chain `HTTP_RULES` to manage SSH and RDP traffic separately. For good organization purposes i am using different chain.
  sudo iptables -N HTTP_RULES
- Now ensuring that all HTTP (port 80) and HTTPS (port 443) traffic is processed using the `HTTP_RULES` chain.
  sudo iptables -A INPUT -p tcp --dport 80 -j HTTP_RULES
  sudo iptables -A INPUT -p tcp --dport 443 -j HTTP_RULES

- Now according to the question, blocking requests from the blacklisted IP range 103.25.231.0/24
  sudo iptables -A HTTP_RULES -s 103.25.231.0/24 -j DROP
- Appling Rate Limiting to HTTP/HTTPS because there can be multiple traffic coming to the port. Allowing a maximum of **5 new connections per second**, with a burst limit of 10.
  sudo iptables -A HTTP_RULES -m conntrack --ctstate NEW -m limit --limit 5/second --limit-burst 10 -j ACCEPT
- Now allowing all remaining legitimate HTTP/HTTPS traffic after filtering.
  sudo iptables -A HTTP_RULES -j ACCEPT

In this part objective is to Ensure that only internal network IPs (`192.168.1.0/24`) can access the database server on default MySQL (`3306`) and PostgreSQL (`5432`) ports. Unauthorized access is logged and dropped.

To achieve this:

- First I have created a new chain `DB_RULES`to manage SSH and RDP traffic separately. For good organization purposes i am using different chain.
  sudo iptables -N DB_RULES
- Now all MySQL (port 3306) and PostgreSQL (port 5432) requests are forwarded to the `DB_RULES` chain.
  sudo iptables -A INPUT -p tcp --dport 3306 -j DB_RULES
  sudo iptables -A INPUT -p tcp --dport 5432 -j DB_RULES
- Now allowing only internal ips to access the database
  sudo iptables -A DB_RULES -s 192.168.1.0/24 -j ACCEPT
- Logged unauthorized access attempts to MySQL and PostgreSQL.
  sudo iptables -A DB_RULES -p tcp --dport 3306 -j LOG --log-prefix "Unauthorized MySQL Access"
  sudo iptables -A DB_RULES -p tcp --dport 5432 -j LOG --log-prefix "Unauthorized Access to PostGre"
- Finally Drop any unauthorized database connections.
  sudo iptables -A DB_RULES -p tcp --dport 3306 -j DROP
  sudo iptables -A DB_RULES -p tcp --dport 5432 -j DROP

Finally, Log and Drop Any Other Unmatched Traffic
sudo iptables -A INPUT -j LOG --log-prefix "Packets Dropped"
sudo iptables -A INPUT -j DROP

Here are the ScreenShots of my commands and IP table

```
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -N SSH_RDP_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 22 -j SSH_RDP_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 3389 -j SSH_RDP_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A SSH_RDP_RULES -s 192.168.1.3 -j ACCEPT
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A SSH_RDP_RULES -p tcp --dport 22 -j LOG --log-prefix "Unauthorized Access to SSH"
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A SSH_RDP_RULES -p tcp --dport 22 -j DROP
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A SSH_RDP_RULES -p tcp --dport 3389 -j LOG --log-prefix "Unauthorized Access to RDP"
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A SSH_RDP_RULES -p tcp --dport 3389 -j DROP
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -N HTTP_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 80 -j HTTP_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 443 -j HTTP_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A HTTP_RULES -s 103.25.231.0/24 -j DROP
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A HTTP_RULES -m conntrack --ctstate NEW -m limit --limit 5/second --limit-burst 10 -j ACCEPT
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A HTTP_RULES -j ACCEPT
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -N DB_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 3306 -j DB_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -p tcp --dport 5432 -j DB_RULES
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A DB_RULES -s 192.168.1.0/24 -j ACCEPT
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A DB_RULES -p tcp --dport 3306 -j LOG --log-prefix "Unauthorized MySQL Access: "
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A DB_RULES -p tcp --dport 5432 -j LOG --log-prefix "Unauthorized Access to PostGre"
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A DB_RULES -p tcp --dport 3306 -j DROP
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A DB_RULES -p tcp --dport 5432 -j DROP
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -j LOG --log-prefix "Packets Dropped"
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -A INPUT -j DROP
pandillapelly22345@pandillapelly22345-virtual-machine:~$ ^C
```

```
pandillapelly22345@pandillapelly22345-virtual-machine:~$ sudo iptables -L
[sudo] password for pandillapelly22345:
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
SSH_RDP_RULES  tcp  --  anywhere             anywhere             tcp dpt:ssh
SSH_RDP_RULES  tcp  --  anywhere             anywhere             tcp dpt:ms-wbt-server
HTTP_RULES  tcp  --  anywhere             anywhere             tcp dpt:http
HTTP_RULES  tcp  --  anywhere             anywhere             tcp dpt:https
DB_RULES   tcp  --  anywhere             anywhere             tcp dpt:mysql
DB_RULES   tcp  --  anywhere             anywhere             tcp dpt:postgresql
LOG        all  --  anywhere             anywhere             LOG level warning prefix "Packets Dropped"
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DB_RULES (2 references)
target     prot opt source               destination
ACCEPT     all  --  192.168.1.0/24       anywhere
LOG        tcp  --  anywhere             anywhere             tcp dpt:mysql LOG level warning prefix "Unauthorized MySQL Access: "
LOG        tcp  --  anywhere             anywhere             tcp dpt:postgresql LOG level warning prefix "Unauthorized Access to PostGr"
DROP       tcp  --  anywhere             anywhere             tcp dpt:mysql
DROP       tcp  --  anywhere             anywhere             tcp dpt:postgresql

Chain HTTP_RULES (2 references)
target     prot opt source               destination
DROP       all  --  103.25.231.0/24      anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate NEW limit: avg 5/sec burst 10
ACCEPT     all  --  anywhere             anywhere

Chain SSH_RDP_RULES (2 references)
target     prot opt source               destination
ACCEPT     all  --  192.168.1.3          anywhere
LOG        tcp  --  anywhere             anywhere             tcp dpt:ssh LOG level warning prefix "Unauthorized Access to SSH"
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
LOG        tcp  --  anywhere             anywhere             tcp dpt:ms-wbt-server LOG level warning prefix "Unauthorized Access to RDP"
DROP       tcp  --  anywhere             anywhere             tcp dpt:ms-wbt-server
pandillapelly22345@pandillapelly22345-virtual-machine:~$
```