Q5

Security Engineer Firewall Configuration Report

Introduction

This document consists of the commands that were run to setup configurations as desired in Question 5 of our assignment

Firewall Configuration Steps

1. Flush Existing Firewall Rules

Before configuring new rules, we flush any existing rules to start with a clean slate.

```
sudo iptables -F
sudo iptables -X
sudo iptables -t nat -F
sudo iptables -t nat -X
sudo iptables -t mangle -F
sudo iptables -t mangle -X
sudo iptables -t raw -F
sudo iptables -t raw -X
```

2. Allow SSH/RDP Access Only for Admin IP

To prevent unauthorized access, SSH (port 22) and RDP (port 3389) are only allowed from the admin IP `192.168.1.3`.

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.1.3 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3389 -s 192.168.1.3 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
sudo iptables -A INPUT -p tcp --dport 3389 -j DROP
```

3. Allow HTTP/HTTPS Traffic but Block Blacklisted IP Range

To ensure web traffic is accessible while blocking known malicious IPs (`103.25.231.0/24`), we use the following rules:

```
sudo iptables -A INPUT -p tcp --dport 80 -s 103.25.231.0/24 -j DROP
sudo iptables -A INPUT -p tcp --dport 443 -s 103.25.231.0/24 -j DROP
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

4. Restrict Database Access to Internal Network

To secure database access, only internal IPs (`192.168.1.0/24`) can connect to database ports (MySQL: 3306, PostgreSQL: 5432).

```
sudo iptables -A INPUT -p tcp --dport 3306 -s 192.168.1.0/24 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 5432 -s 192.168.1.0/24 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
sudo iptables -A INPUT -p tcp --dport 5432 -j DROP
```

5. Enable Logging

Logging is configured to track unauthorized access attempts for debugging and security auditing.

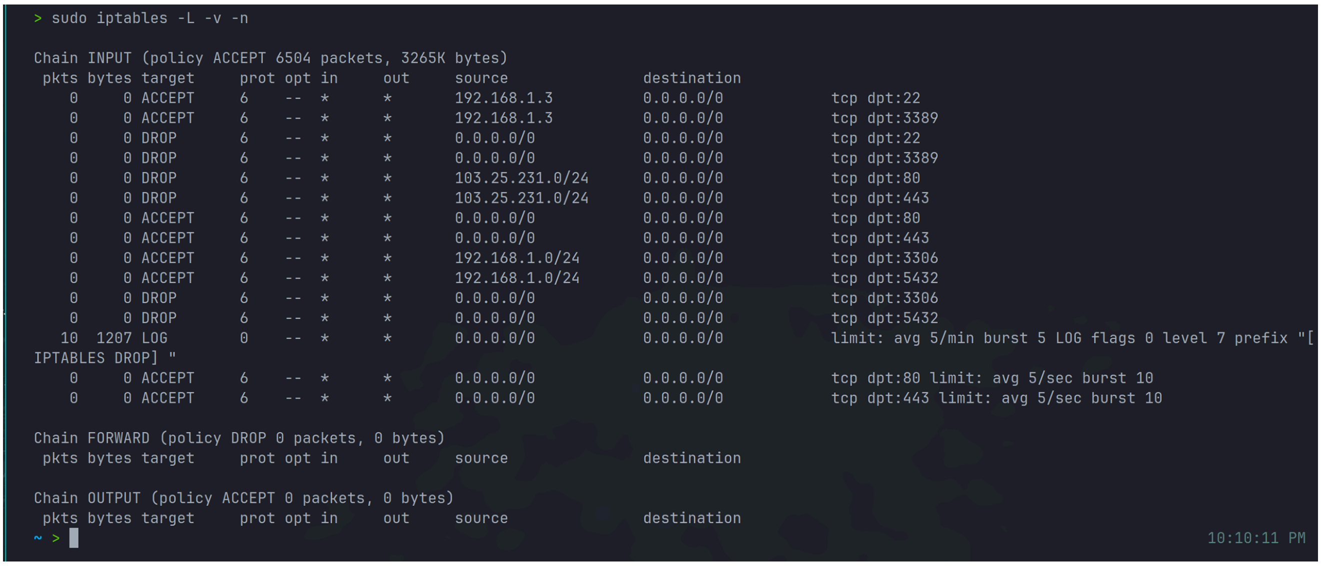
```
sudo iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "
[IPTABLES DROP] " --log-level 7
```

6. Implement Rate Limiting to Prevent DDoS

To prevent excessive HTTP requests from a single IP, we limit connections to 5 per second.

```
sudo iptables -A INPUT -p tcp --dport 80 -m limit --limit 5/sec --limit-
burst 10 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -m limit --limit 5/sec --limit-
burst 10 -j ACCEPT
```

Screenshots



```
> sudo iptables -L -v -n

Chain INPUT (policy ACCEPT 6504 packets, 3265K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     6    --  *      *       192.168.1.3          0.0.0.0/0            tcp dpt:22
    0     0 ACCEPT     6    --  *      *       192.168.1.3          0.0.0.0/0            tcp dpt:3389
    0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
    0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3389
    0     0 DROP       6    --  *      *       103.25.231.0/24      0.0.0.0/0            tcp dpt:80
    0     0 DROP       6    --  *      *       103.25.231.0/24      0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     6    --  *      *       192.168.1.0/24       0.0.0.0/0            tcp dpt:3306
    0     0 ACCEPT     6    --  *      *       192.168.1.0/24       0.0.0.0/0            tcp dpt:5432
    0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:3306
    0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:5432
   10  1207 LOG        0    --  *      *       0.0.0.0/0            0.0.0.0/0            limit: avg 5/min burst 5 LOG flags 0 level 7 prefix "[
IPTABLES DROP] "
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 limit: avg 5/sec burst 10
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443 limit: avg 5/sec burst 10

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
~ >                                                                                                                     10:10:11 PM
```

Conclusion

The implemented firewall rules effectively secure SSH/RDP access, restrict database connections to internal IPs, block malicious IPs, log unauthorized access, and apply rate limiting to mitigate DDoS attacks. This configuration enhances security while ensuring seamless business operations.