241901025 DHARANI K

Ex.No:9 **Date:10/10/2025**

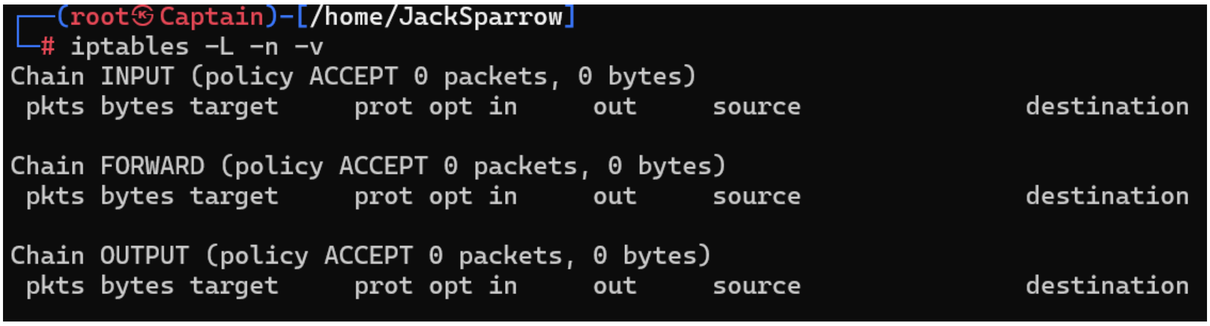
INSTALL AND CONFIGURE IPTABLES FIREWALL

AIM:

To install iptables and configure it for variety of options.

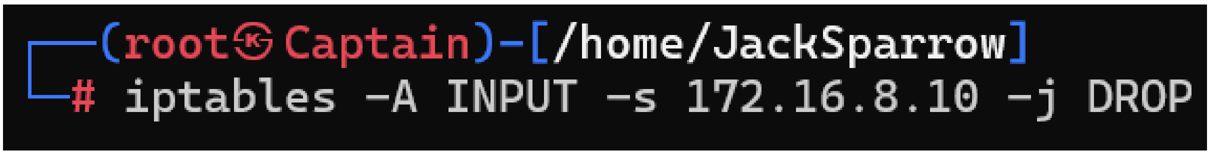
COMMON CONFIGURATIONS & OUTPUTS:

Check all exitsting IPtables Firewall Rules:



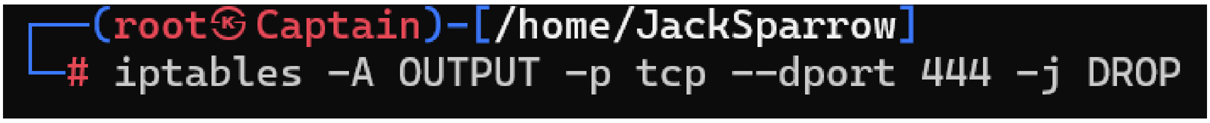
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 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
```

Block specific IP Address(eg. 172.16.8.10) in IPtables Firewall:



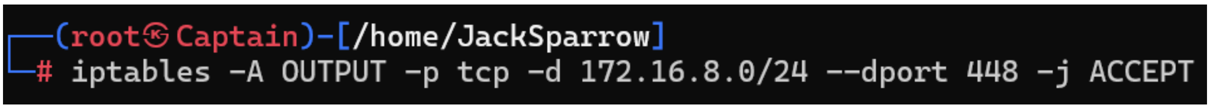
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -A INPUT -s 172.16.8.10 -j DROP
```

Block specifig port on IPtables Firewall:



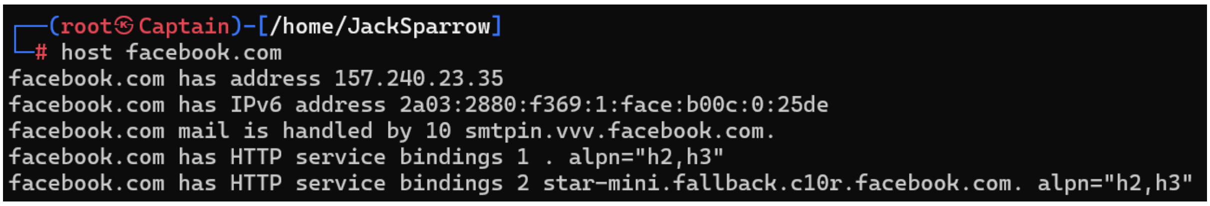
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -A OUTPUT -p tcp --dport 444 -j DROP
```

Allow specific network range on particular port on iptables:

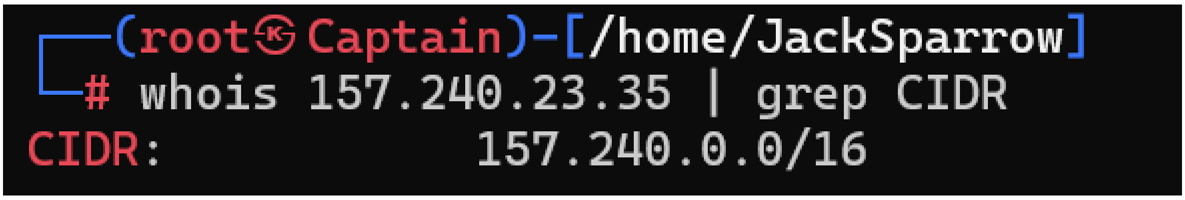


```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -A OUTPUT -p tcp -d 172.16.8.0/24 --dport 448 -j ACCEPT
```

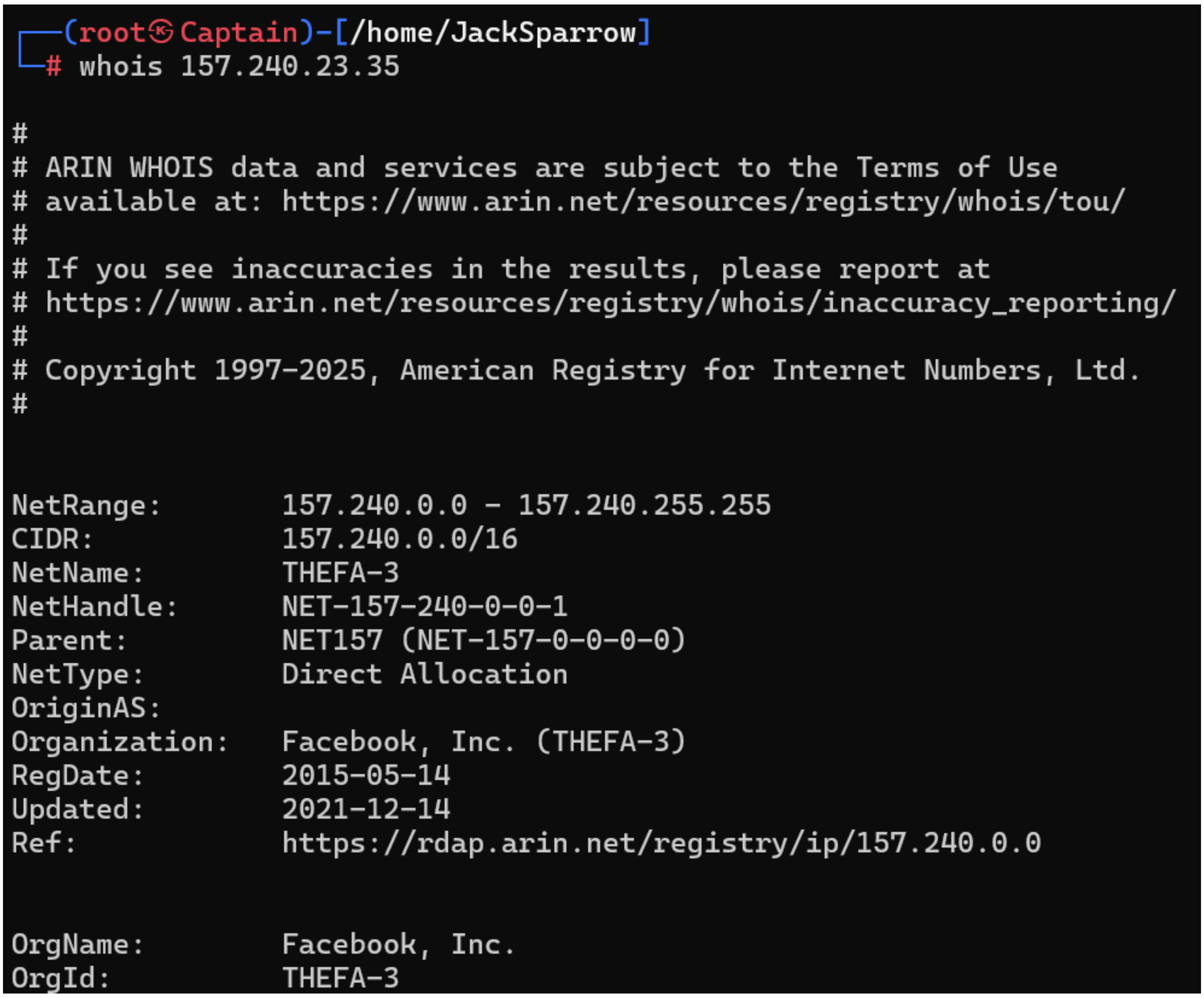
Block Facebook on IPTables:



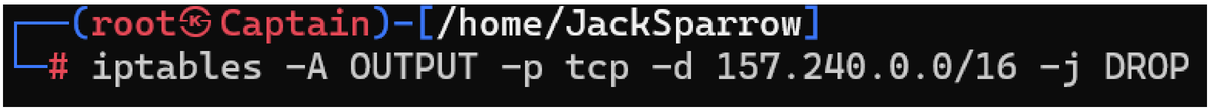
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# host facebook.com
facebook.com has address 157.240.23.35
facebook.com has IPv6 address 2a03:2880:f369:1:face:b00c:0:25de
facebook.com mail is handled by 10 smtpin.vvv.facebook.com.
facebook.com has HTTP service bindings 1 . alpn="h2,h3"
facebook.com has HTTP service bindings 2 star-mini.fallback.c10r.facebook.com. alpn="h2,h3"
```



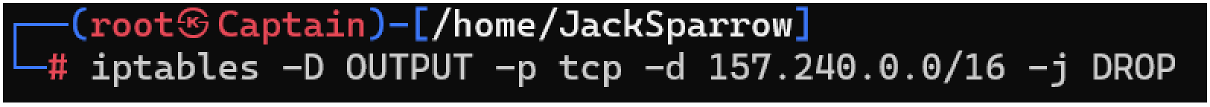
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# whois 157.240.23.35 | grep CIDR
CIDR:           157.240.0.0/16
```



```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# whois 157.240.23.35

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       157.240.0.0 - 157.240.255.255
CIDR:           157.240.0.0/16
NetName:        THEFA-3
NetHandle:      NET-157-240-0-0-1
Parent:         NET157 (NET-157-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Facebook, Inc. (THEFA-3)
RegDate:        2015-05-14
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/157.240.0.0


OrgName:        Facebook, Inc.
OrgId:          THEFA-3
```

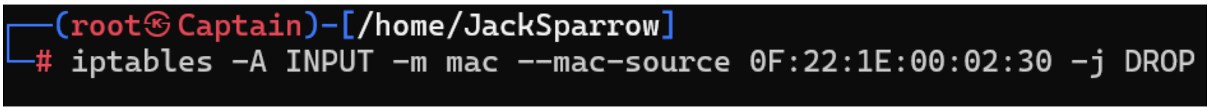


```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -A OUTPUT -p tcp -d 157.240.0.0/16 -j DROP
```



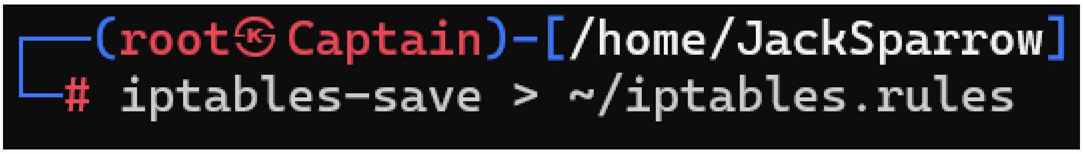
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -D OUTPUT -p tcp -d 157.240.0.0/16 -j DROP
```

Block Access to your system from specific MAC Address(say 0F:22:1E:00:02:30):



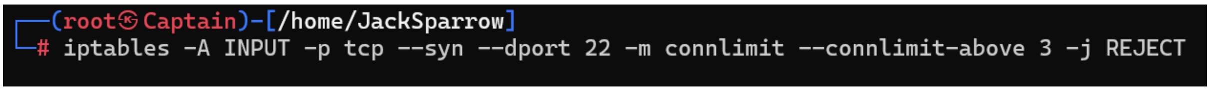
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -A INPUT -m mac --mac-source 0F:22:1E:00:02:30 -j DROP
```

Save IPtables rules to a file:



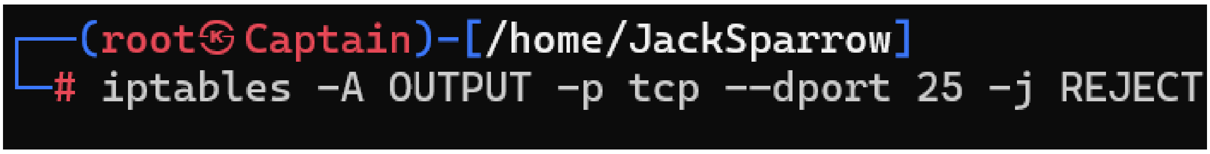
```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables-save > ~/iptables.rules
```

Restrict number of concurrent connections to a Server(Here restrict to 3 connections only):

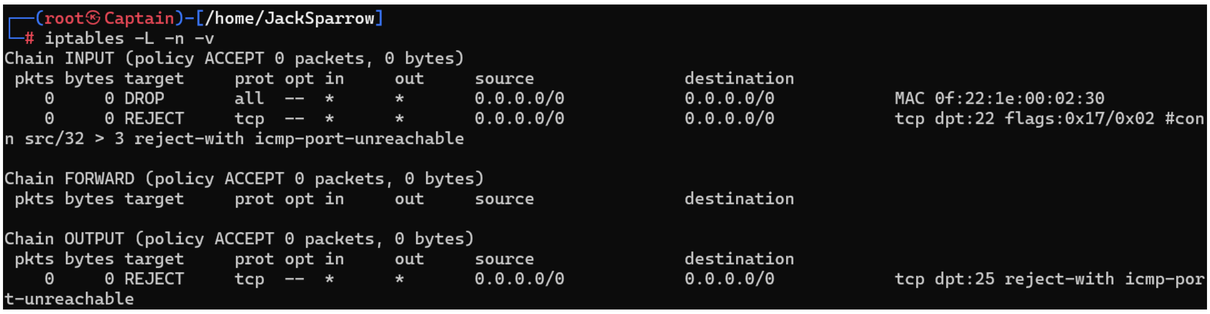


```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 3 -j REJECT
```

Disable outgoing mails through Iptables:

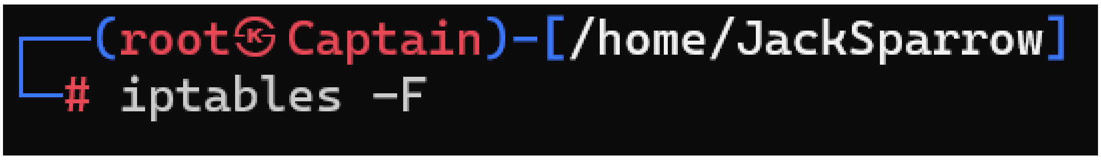


```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -A OUTPUT -p tcp --dport 25 -j REJECT
```



```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0            MAC 0f:22:1e:00:02:30
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 flags:0x17/0x02 #con
n src/32 > 3 reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT 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
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:25 reject-with icmp-por
t-unreachable
```

Flush IPtables Firewall chains or rules:



```
┌──(root㉿Captain)-[/home/JackSparrow]
└─# iptables -F
```

RESULT:

Thus, the iptables has been installed successfully and it has been configured for variety of options.