

Ex. No.: 9

Date:

INSTALL AND CONFIGURE IPTABLES FIREWALL

Aim:

To install iptables and configure it for variety of options.

Common Configurations & outputs:

1. Start/stop/restart firewalls

```
[root@localhost ~]# systemctl start firewalld
[root@localhost ~]# systemctl restart firewalld
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]#
```

2. Check all existing IPtables Firewall Rules

```
[root@localhost ~]# iptables -L -n -v
[root@localhost ~]#
```

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

```
[root@localhost ~]# iptables -A INPUT -s 172.16.8.10 -j DROP
[root@localhost ~]#
```

4. Block specific port on IPtables Firewall

```
[root@localhost ~]# iptables -A OUTPUT -p tcp --dport xxx -j DROP
[root@localhost ~]#
```

5. Allow specific network range on particular port on iptables

```
[root@localhost ~]# iptables -A OUTPUT -p tcp -d 172.16.8.0/24 --dport xxx -j ACCEPT
[root@localhost ~]#
```

6. Block Facebook on IPTables [root@localhost

```
~]# host facebook.com facebook.com has address
157.240.24.35
```

facebook.com has IPv6 address 2a03:2880:f10c:283:face:b00c:0:25de facebook.com
mail is handled by 10 smtpin.vvv.facebook.com.

```
[root@localhost ~]# whois 157.240.24.35 | grep CIDR
CIDR:      157.240.0.0/16
[root@localhost ~]#
```

```
[root@localhost ~]# whois 157.240.24.35
[Querying whois.arin.net]
[whois.arin.net]
```

```
#
# 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 1997-2019, 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 Assignment
OriginAS:
Organization: Facebook, Inc. (THEFA-3)
RegDate:   2015-05-14
Updated:   2015-05-14
Ref:       https://rdap.arin.net/registry/ip/157.240.0.0
```

```
OrgName:   Facebook, Inc.
OrgId:     THEFA-3 Address:
1601 Willow Rd.
City:      Menlo Park
StateProv: CA
PostalCode: 94025
Country:   US
RegDate:   2004-08-11
Updated:   2012-04-17
Ref:       https://rdap.arin.net/registry/entity/THEFA-3
```

OrgTechHandle: OPERA82-ARIN

OrgTechName: Operations
OrgTechPhone: +1-650-543-4800
OrgTechEmail: domain@facebook.com
OrgTechRef: <https://rdap.arin.net/registry/entity/OPERA82-ARIN>

OrgAbuseHandle: OPERA82-ARIN
OrgAbuseName: Operations
OrgAbusePhone: +1-650-543-4800
OrgAbuseEmail: domain@facebook.com
OrgAbuseRef: <https://rdap.arin.net/registry/entity/OPERA82-ARIN> #
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 1997-2019, American Registry for Internet Numbers, Ltd.

[root@localhost ~]# iptables -A OUTPUT -p tcp -d 157.240.0.0/16 -j DROP Open browser and check whether <http://facebook.com> is accessible

To allow facebook use -D instead of -A option

[root@localhost ~]# iptables -D OUTPUT -p tcp -d 157.240.0.0/16 -j DROP
[root@localhost ~]#

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

[root@localhost ~]# iptables -A INPUT -m mac --mac-source 0F:22:1E:00:02:30 -j DROP
[root@localhost ~]#

7. Save IPtables rules to a file

[root@localhost ~]# iptables-save > ~/iptables.rules
[root@localhost ~]# vi iptables.rules
[root@localhost ~]#

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

[root@localhost ~]# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimitabove 3 -j REJECT

9. Disable outgoing mails through IPtables

[root@localhost ~]# iptables -A OUTPUT -p tcp --dport 25 -j REJECT
[root@localhost ~]#

10. Flush IPtables Firewall chains or rules

```
[root@localhost ~]# iptables -F
```

```
[root@localhost ~]#
```

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