6

Network Security

# Managing TCP/IP Network

## Getting Ready

cp /etc/NetworkManager/NetworkManager.conf /etc/NetworkManager/NetworkManager.conf.bak

## How to do it...

1. ifconfig
2. ifconfig -a | grep eth
3. lshw -class network
4. nano /etc/NetworkManager/NetworkManager.conf.

Change the line managed=false to managed=true and save the file.

1. nano /etc/network/interfaces

auto eth0

iface eth0 inet static

address 192.168.1.101

netmask 255.255.255.0

network 192.168.1.0

broadcast 192.168.1.255

gateway 192.168.1.1

1. Add lines in /etc/network/interfaces file, as shown –

auto eth0:0

iface eth0:0 inet static

address 192.168.1.110

netmask 255.255.255.0

gateway 192.168.1.1

1. service network-manager restart

or

/etc/init.d/networking restart

1. Edit the file /etc/resolv.conf

nameserver 192.168.1.1

nameserver 192.168.1.1

# Using IP Tables for configuring Firewall

## How to do it...

1. iptables -V
2. iptables -L
3. iptables -S
4. lsmod | grep ip\_tables
5. iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
6. iptables -L
7. iptables -A INPUT -p tcp --dport 22 -j ACCEPT
8. iptables -I INPUT 1 -i lo -j ACCEPT
9. iptables -L -v
10. iptables –A INPUT –j DROP
11. apt-get install iptables-persistent
12. service iptables-persistent start

# Blocking Spoofed Addresses

## How to do it...

1. iptables -A INPUT -i lo -j ACCEPT
2. iptables -L -v
3. iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
4. iptables -N blocked\_ip
5. iptables -I INPUT 2 -j blocked\_ip
6. iptables -A blocked\_ip -s 192.168.1.115 -j DROP
7. iptables –L
8. nano /etc/host.conf

Now add or edit the following lines in the file-

orderbind,hosts

nospoof on

# Blocking Incoming Traffic

## How to do it

1. iptables -A INPUT -i lo -j ACCEPT
2. iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
3. iptables -L
4. iptables -A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
5. iptables -A INPUT -p icmp -m icmp --icmp-type 3/4 -j ACCEPT
6. iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
7. iptables -L
8. iptables -N allowed\_ip
9. iptables -A INPUT -j allowed\_ip
10. iptables -A allowed\_ip -p tcp --dport 22 -j ACCEPT
11. iptable -L
12. iptables -A INPUT -j REJECT --reject-with icmp-host-unreachable
13. iptables -L

# Configuring and using TCP Wrapper

## How to do it?

1. which sshd
2. ldd /usr/sbin/sshd
3. ssh tajinder@192.168.1.107
4. Edit the file /etc/hosts.deny and add the line –

sshd : 192.168.1.106

1. ssh tajinder@192.168.1.107
2. Add the following line in /etc/hosts.allow file

ALL : ALL

1. Add the following line in the /etc/hosts.allow file

ALL : 192.168.1.106

1. Do the following changes in the /etc/hosts.allow file

sshd : 192.168.1.100 : DENY

sshd : 192.168.1.0/255.255.255.0 : ALLOW

1. Edit the /etc/hosts.allow file on server –

sshd : 192.168.1.103 : spawn /bin/echo ‘/bin/date’ from %h > /conn.log : deny

1. cat conn.log