

# Chapter Three

## Network management



Edit with WPS Office

# Outline

- Introduction
- TCP/IP networking basics
- IPv4 and IPv6
- Configuring Linux box for networking
- Configuring DNS server
- TCP/IP troubleshooting
- Configuring mail transfer agents
- Configuring web server
- configuring Linux box as router



Edit with WPS Office

# Introduction

- Computers are connected in a network to exchange information or resource with each other .
- Two or more computers are connected through network media called computer media.
- There are number of devices that are involved to form network
- Maintaining of system or network up running is a task of system or network administrator.
- Troubleshooting and configuration commands in Linux.



# Cont....

- The Linux kernel names interface with a specific prefix
- depending on the type of interface
- All interface starts with eth.
- Other interfaces include wlan0 for the first wireless device



Edit with WPS Office

# TCP/IP networking basics

- IP, the Internet Protocol, which routes data packets from one machine to another
- ICMP, the Internet Control Message Protocol, which provides several kinds of low-level support for IP, including error messages, routing assistance, and debugging help
- ARP, the Address Resolution Protocol, which translates IP addresses to hardware addresses



# Cont....

- UDP, the User Datagram Protocol, which provides unverified, one-way data delivery
- TCP, the Transmission Control Protocol, which implements reliable, full duplex, flow-controlled, error-corrected conversations
- TCP/IP is a protocol “suite,”
- a set of network protocols designed to work smoothly together



Edit with WPS Office

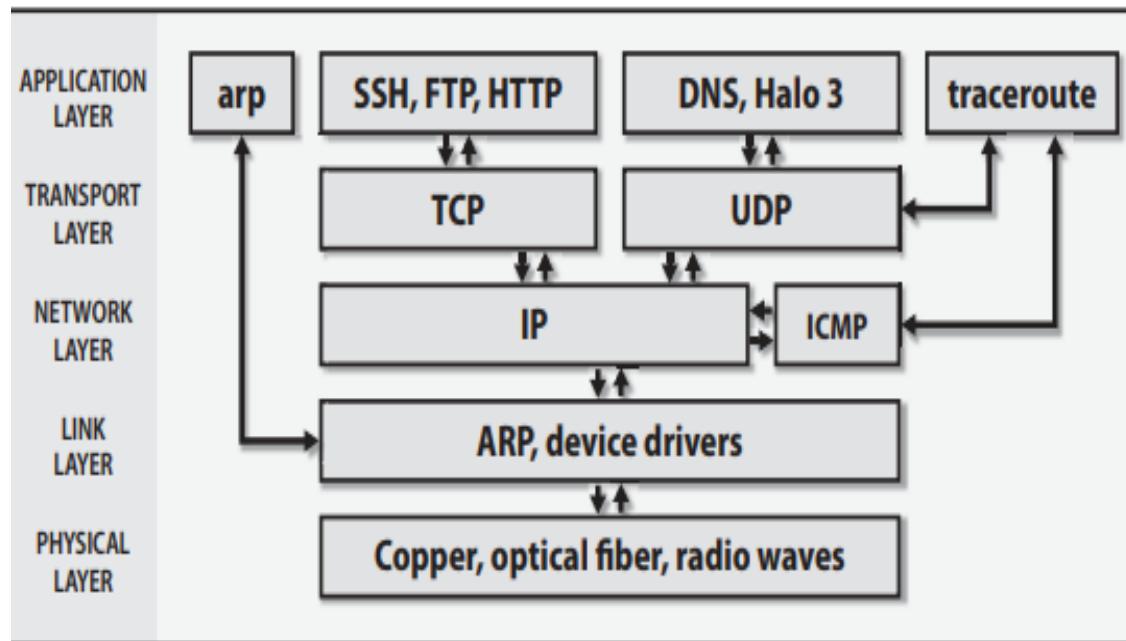
# Cont....

- These protocols are arranged in a hierarchy or “stack”,
- With the higher-level protocols making use of the protocols beneath them.
- TCP/IP is conventionally described as a five-layer system



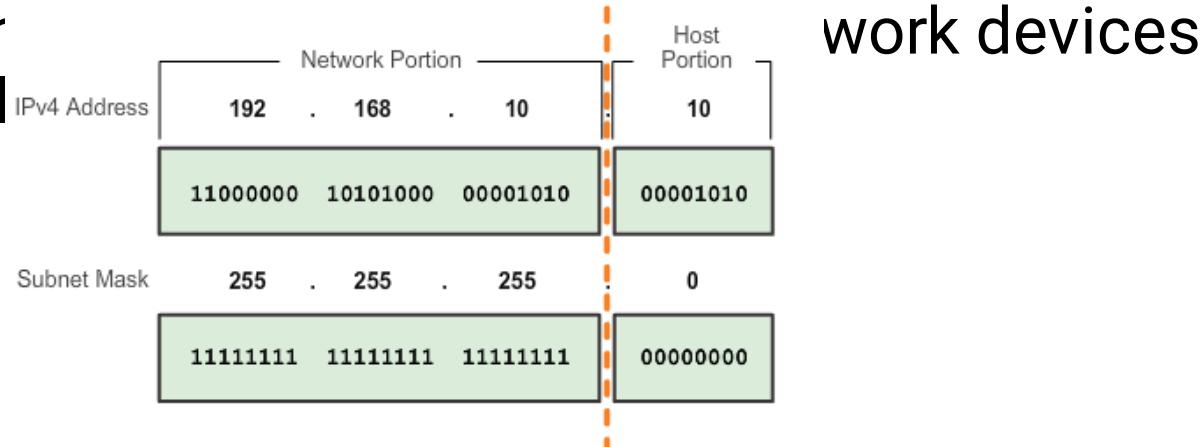
Edit with WPS Office

# Cont....



# IPv4 and IPv6

- IPv4 uses 4 byte ip address or 32 bit hierarchical address
- That is made up of network portion and host portion
- Subnet mask is used to determine network portion and host portion
- All modern oper already support I



# Cont....

## Subnet mask

- Within each network area three types of IP address
- Network address
- Broadcast address
- Host address
- From ip address and subnet mask we identify those address



Edit with WPS Office

# Cont....

- Ipv4 unicast, broadcast and multicast
- Broadcast is sending a packet to all other destination
- Unicast transmission is sending a packet to one destination IP address
- Multicast transmission is sending a packet to multicast address group



Edit with WPS Office

# Cont....

Types of ipv4 address

Private and public ip address

- Public ipv4 address is globally routed between ISP routers
- Private ip address are common blocks of address used by most organization to assign ipv4 address.
- NAT is used to translates private ipv4 address to public ipv4 address
- Loopback address used on host weather tcp/ip is operational or not and NIC is work or not



# Cont....

- Ipv4 is running out of address
- Ipv6 has much larger 128 bit
- Ipv6 fixes ipv4 limitations and other enhancements
- Both ipv4 and ipv6 coexist
- The transition will take several years
- All modern operating systems and many network devices already support IPv6



Edit with WPS Office

# Cont....

- Like letters or email messages, network packets must be properly addressed in order to reach their destinations.
- MAC (media access control) addresses for use by hardware
- IPv4 and IPv6 network addresses for use by software
- Hostnames for use by people
- subnetting
- To make better use of these addresses, you can now reassign part of the host portion to the network portion by specifying an explicit 4-byte “subnet mask” or “netmask” in which the 1s correspond to the desired network portion and the 0s correspond to the host portion.



Edit with WPS Office

# Cont....

- On Ubuntu you can install **ipcalc** through **apt-get**.
- For performing ip address and subnet calculation
- Routing is the process of directing a packet through the maze of networks that stand between its source and its destination.
- In the TCP/IP system, it is similar to asking for directions in an unfamiliar country.



Edit with WPS Office

# Configuring Linux box for networking

- Configuring Linux box for networking means
- How to configure Linux network interface
- Network interfaces are configured either manually via commands or automatically using configuration files.
- Ip a
- Nmcli device status is if we are using NetworkManager
- Ifconfig check available interfaces
- Linux network configuration file location
- File location /etc/network/interfaces



Edit with WPS Office

# Cont....

```
tsion@DESKTOP-3L0GAMB:~$ ethtool -i eth0 // to view specific interface details
```

```
driver: hv_netvsc
```

- version: 5.10.102.1-microsoft-standard-W
- firmware-version: N/A
- expansion-rom-version:
- bus-info:
- supports-statistics: yes
- supports-test: no
- supports-eeprom-access: no
- supports-register-dump: yes
- supports-priv-flags: no



Edit with WPS Office

# Cont....

- In WSL or windows subsystem for Linux
- Sudo apt install net-tools
- Ifconfig
- sudo nano /etc/netplan/00-installer-config.yaml
- To view interfaces
- tsion@DESKTOP-3L0GAMB:~\$ ls /sys/class/net/
- bond0 bonding masters dummy0 eth0 lo sit0 tunl0



Edit with WPS Office

# Cont.....

```
network:  
  version: 2  
  renderer: networkd  
  ethernets:  
    eth0:  
      dhcp4: no  
      addresses: 192.168.1.0/24  
      gateway4: 192.168.1.1  
      nameservers:  
        addresses:  
          - 8.8.8.8  
          - 8.8.4.4
```



Edit with WPS Office

# Cont.....

- In this case network manager or other tools might be manage interfaces , if those tools is set to use DHCP, it might be override the static ip configuration .
- If you have get un expected ip address



Edit with WPS Office

# Cont....

- To verify the network manager is installed or not
- tsion@DESKTOP-3L0GAMB:~\$ dpkg -l | grep network-manager
- ii network-manager 1.46.0-1ubuntu2.2  
amd64 network management framework (daemon and userspace tools)
- ii network-manager-pptp 1.2.12-3build2  
amd64 network management framework (PPTP plugin core)



Edit with WPS Office

# Cont....

- but if the network manager is not installed
- sudo apt update
- sudo apt install network-manager
- after installation you can enable and start network manager
- sudo systemctl enable NetworkManager
- sudo systemctl start NetworkManager
- then check the status of network manager



# Cont....

- sudo systemctl stop NetworkManager
- sudo systemctl disable NetworkManager
- is used to apply changes in netplan
- sudo netplan apply for WSL
- For other Linux os
- sudo nano /etc/network/interfaces



Edit with WPS Office

# Cont....

- auto eth0
- iface eth0 inet static
- address 192.168.1.100
- netmask 255.255.255.0
- gateway 192.168.1.1
- sudo systemctl restart networking //to apply changes



Edit with WPS Office

# Cont....

- In this step you will manually configure your network interface by editing the following files using your preferred text editor (**nano, gedit, vi, vim, etc**).
- For the purpose of this example let's use the "nano" editor.
- You can edit the appropriate file by entering the following command into the terminal:



Edit with WPS Office

# Cont....

- *sudo nano /etc/network/interfaces // for debian based systems*
- */etc/sysconfig/network-scripts/ifcfg-interface name //redhat*
- Enter your root password, once your preferred editor opens the file, you can see...  
*auto lo eth0*  
*iface lo inet loopback*  
*iface eth0 inet dynamic*



Edit with WPS Office

# Cont....

- Statically configured network cards will have a section like:

**auto lo eth0**

**iface lo inet loopback**

**iface eth0 inet static**

**address xxx.xxx.xxx.xxx**(enter your ip here)

**netmask xxx.xxx.xxx.xxx**

**gateway xxx.xxx.xxx.xxx**(enter gateway ip here,usually the address of the router)



# Cont.....

Here is an example:

```
auto lo eth0
iface lo inet loopback
iface eth0 inet static
address 192.168.1.101
netmask 255.255.255.0
gateway 192.168.1.1
```



Edit with WPS Office

# Cont....

- If you use "nano" editor, type ***Ctrl+x*** to save changes.
- *Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES)*
- <--Type "y"
- *File Name to Write: interfaces*
- <--ENTER



Edit with WPS Office

# Cont....

- Static network configuration and automatic
- DHCP Linux network config

```
yenework@kali:~$ sudo nano /etc/network/interfaces  
[sudo] password for yenework: []
```

- It will overrides any static ip configuration
- The DHCP services are like NetworkManager, dhclient and systemd- networked



Edit with WPS Office

# Cont....

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp

    # wireless-* options are implemented by the wireless-tools package
    wireless-mode managed
    wireless-essid Hiruy
    wireless-key1 21232729
    # dns-* options are implemented by the resolvconf package, if installed
#    dns-nameservers 8.8.8.8
#        dns-search www.bdu.edu.et
#    dns-nameservers 4.4.4.4
```



```
yenework@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 2c:60:0c:56:66:e4 brd ff:ff:ff:ff:ff:ff
        inet 10.161.70.218/23 brd 10.161.71.255 scope global dynamic noprefixroute eth0
            valid_lft 86326sec preferred_lft 75526sec
        inet6 fe80::69f6:1d79:c3bb:cf2f/64 scope link
            valid_lft forever preferred_lft forever
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 36:f6:8a:0e:29:bf brd ff:ff:ff:ff:ff:ff permaddr d0:53:49:0d:25:a3
yenework@kali:~$ 
```



Edit with WPS Office

# Configuring DNS server....

- DNS is a database system that translates a computers fully qualified domain name in to IP address
- [www.amazon.com](http://www.amazon.com) to 207.171.166.48



Edit with WPS Office

# Cont....

## *STEPS*

*It involves following steps:-*

- *sudo su*
- *nano /etc/network/interfaces – for static IP.*
- */etc/init.d/networking restart*
- *ifconfig*
- *apt-get install bind9*
- *nano /etc/bind/named.conf.local*
- *nano /etc/bind/db.up.omg (forward lookup zone)*
- *nano /etc/bind/db.192 (reverse lookup zone)*
- *nano /etc/resolv.conf*
- */etc/init.d/bind9 restart*
- *nslookup sgsits.up.omg & nslookup 192.168.1.3*



Edit with WPS Office

# Cont....

- BIND(Berkeley internet name domain ) is an implementation of DNS protocol and provides an openly redistributable reference implementation of the major components of the DNS
- BIND9 is latest version of BIND
- Features are security of DNS, IPv6,
- DNS protocol enhancement, views , multiprocessor support



Edit with WPS Office

# Cont....

- tsion@DESKTOP-3L0GAMB:~\$ sudo apt update
  - Before installing BIND9 to ensure your system is up to date
  - sudo apt upgrade -y
- [sudo] password for tsion:
- Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
- Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
- Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
- Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
- .....



Edit with WPS Office

# Cont....

- To see the upgrade content
- tsion@DESKTOP-3L0GAMB:~\$ apt list –upgradable
- After this installing BIND9 DNS server
- sudo apt install bind9 bind9utils bind9-doc
- tsion@DESKTOP-3L0GAMB:~\$ sudo apt install bind9 bind9utils bind9-doc
- sudo nano /etc/bind/named.conf.options
- Open this configuration file to make any neccessary changes
- This configuration is done in ubuntu 24.04



Edit with WPS Office

# Cont....

- To install and configure DNS
- Sudo apt update
- Sudo apt upgrade // update systems to get installation packages
  
- sudo nano /etc/bind/named.conf.local



Edit with WPS Office

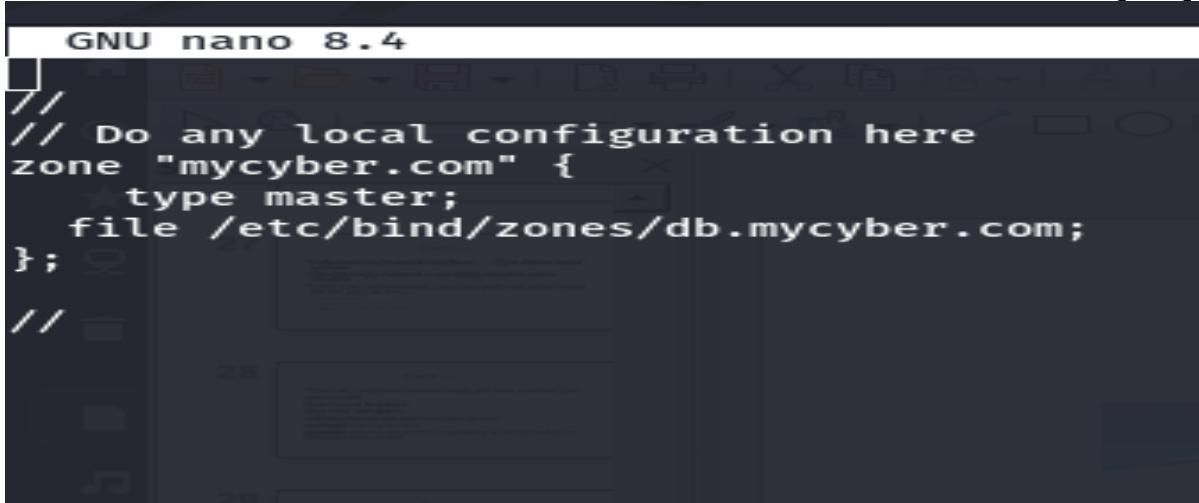
# To install bind9

```
yenework@kali:~$ sudo apt-get install bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfuse3-3
Use 'sudo apt autoremove' to remove it.      It involves following steps:-
The following additional packages will be installed:
  bind9-utils
Suggested packages:
  bind-doc resolvconf ufw
The following NEW packages will be installed:
  bind9 bind9-utils
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 432 kB of archives.
After this operation, 1,641 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 bind9-utils amd64 1:9.20.7-1 [183 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 bind9 amd64 1:9.20.7-1 [250 kB]
Fetched 432 kB in 3s (163 kB/s)
Selecting previously unselected package bind9-utils.
(Reading database ... 149510 files and directories currently installed.)
Preparing to unpack .../bind9-utils_1%3a9.20.7-1_amd64.deb ...
Unpacking bind9-utils (1:9.20.7-1) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.20.7-1_amd64.deb ...
```

# Configure a local DNS name server

```
PROCESSING TRIGGERS FOR kali-menu (2020.2.0) ...
yenework@kali:~$ sudo nano /etc/bind/named.conf.local
yenework@kali:~$ 
```

In this case file “/etc/bind/zones/db.mycyber.com”;



```
GNU nano 8.4
// Do any local configuration here
zone "mycyber.com" {
    type master;
    file /etc/bind/zones/db.mycyber.com;
};

// 
```



Edit with WPS Office

# Cont...

Sudo nano /etc/bind/db.mycyber.com.local

```
yenework@kali:~$ sudo nano /etc/bind/db.mycyber.com.local
[sudo] password for yenework:
yenework@kali:~$ 
```



Edit with WPS Office

# You can edit as shown below

After typing sudo nano /etc/bind/db.mycyber.com.local // edit like this

```
$TTL 86400
@       IN  NS  ns1.mycyber.com.  admin.mycyber.com.  (
              2023042501 ; Serial
              3600      ; Refresh
              1800      ; Retry
              1209600   ; Expire
              86400 )    ; Minimum TTL

@       IN  NS  ns1.mycyber.com.
@       IN  NS  ns2.mycyber.com.

ns1    IN  A   203.0.113.10
ns2    IN  A   203.0.113.11
@       IN  A   203.0.113.20
www    IN  A   203.0.113.20
mail   IN  A   203.0.113.30
@       IN  MX  20 mail.mycyber.com.
```



Edit with WPS Office

# Check the status of configuration

```
yenework@kali:~$ sudo named-checkconf
yenework@kali:~$ sudo systemctl restart bind9
yenework@kali:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: disabled)
   Active: active (running) since Thu 2025-04-24 21:34:03 EDT; 10s ago
     Invocation: c33c98aae0674cf0956a21142711f320
       Docs: man:named(8)
    Main PID: 9399 (named)
      Status: "running"
        Tasks: 10 (limit: 4538)
      Memory: 10.3M (peak: 11M)
        CPU: 93ms
      CGroup: /system.slice/named.service
              └─9399 /usr/sbin/named -f -u bind

Apr 24 21:34:04 kali named[9399]: validating ./NS: no valid signature found
Apr 24 21:34:04 kali named[9399]: RRSIG validity period has not begun resolving './NS/IN': 170.247.170.2#53
Apr 24 21:34:05 kali named[9399]: validating ./NS: verify failed due to bad signature (keyid=53148): RRSIG validity per
Apr 24 21:34:05 kali named[9399]: validating ./NS: no valid signature found
Apr 24 21:34:05 kali named[9399]: RRSIG validity period has not begun resolving './NS/IN': 192.112.36.4#53
Apr 24 21:34:05 kali named[9399]: validating ./NS: verify failed due to bad signature (keyid=53148): RRSIG validity per
Apr 24 21:34:05 kali named[9399]: validating ./NS: no valid signature found
Apr 24 21:34:05 kali named[9399]: RRSIG validity period has not begun resolving './NS/IN': 192.58.128.30#53
Apr 24 21:34:05 kali named[9399]: network unreachable resolving './NS/IN': 2001:dc3::35#53
Apr 24 21:34:05 kali named[9399]: resolver priming query complete: failure
```



Edit with WPS Office

# Check the configuration is correct or not

```
venework@kali:~$ sudo cp /etc/bind/db.local /etc/bind/db.mycyber.com
cp: cannot stat '/etc/bind/db.local': No such file or directory
venework@kali:~$ sudo nano /etc/bind/db.mycyber.com
venework@kali:~$ sudo named-checkzone mycyber.com /etc/bind/db.mycyber.com
zone mycyber.com/IN: loaded serial 2023042501
OK
venework@kali:~$ 
```



Edit with WPS Office

# Test DNS server by using dig command

```
yenework@kali:~$ sudo nano /etc/bind/named.conf.local
yenework@kali:~$ ls -l /etc/bind/db.mycyber.com
-rw-r--r-- 1 root bind 461 Apr 25 08:57 /etc/bind/db.mycyber.com
yenework@kali:~$ sudo named-checkzone mycyber.com /etc/bind/db.mycyber.com
zone mycyber.com/IN: loaded serial 2023042501
OK
yenework@kali:~$ sudo named-checkconf
yenework@kali:~$ sudo systemctl restart bind9
yenework@kali:~$ dig @localhost mycyber.com

; <>> DiG 9.20.7-1-Debian <>> @localhost mycyber.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3540
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: cdfc539a1ba41f1901000000680b891f0ad5468c71e9fcfd7 (good)
;; QUESTION SECTION:
;mycyber.com.           IN      A

;; ANSWER SECTION:
mycyber.com.      86400   IN      A      203.0.113.20

;; Query time: 0 msec
;; SERVER: ::1#53(localhost) (UDP)
;; WHEN: Fri Apr 25 09:07:43 EDT 2025
;; MSG SIZE  rcvd: 84
```



Edit with WPS Office

# Cont....

```
yenework@kali:~$ dig @localhost www.mycyber.com
; <>> DiG 9.20.7-1-Debian <>> @localhost www.mycyber.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 829
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ac01565a852664c601000000680b89aafb9698f0812e8203 (good)
;; QUESTION SECTION:
;www.mycyber.com.          IN      A

;; ANSWER SECTION:
www.mycyber.com.      86400   IN      A       203.0.113.20

;; Query time: 0 msec
;; SERVER: ::1#53(localhost) (UDP)
;; WHEN: Fri Apr 25 09:10:02 EDT 2025
;; MSG SIZE  rcvd: 88

yenework@kali:~$ 
```

"Screenshot From 2025-04-22 10:10:02"



Edit with WPS Office

# Cont....

```
yenework@kali:~$ dig @localhost mycyber.com MX
; <>> DiG 9.20.7-1-Debian <>> @localhost mycyber.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47621
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3003a2c3df5af5ce01000000680b8a1ba261511595c32c8f (good)
;; QUESTION SECTION:
;mycyber.com.           IN      MX
;; ANSWER SECTION:
mycyber.com.        86400   IN      MX      20 mail.mycyber.com.
;; ADDITIONAL SECTION:
mail.mycyber.com.    86400   IN      A       203.0.113.30
;; Query time: 0 msec
;; SERVER: ::1#53(localhost) (UDP)
;; WHEN: Fri Apr 25 09:11:55 EDT 2025
;; MSG SIZE  rcvd: 105
yenework@kali:~$ 
```

Screenshot From  
2025-04-25

"Screenshot From 2025-04-22"



Edit with WPS Office

# Cont.....

```
yenework@kali:~$ nslookup mycyber.com 127.0.0.1
Server:      127.0.0.1
Address:     127.0.0.1#53
```

```
Name:    mycyber.com
Address: 203.0.113.20
```

```
yenework@kali:~$ 
```

Screenshot From  
2025-04-25

Screenshot From  
2025-04-25

"Screenshot From 2025-04-22 2



Edit with WPS Office

# configuring DNS client

- Each host on the network must be a name server client.
- You configure the client side of DNS in the file /etc/resolv.conf,
- which lists the DNS servers the host can query when a user attempts to resolve a hostname.

```
venework@kali:~$ sudo nano /etc/resolv.conf
```



Edit with WPS Office

# Cont....

```
# Generated by dhcpcd from eth0.dhcp
# /etc/resolv.conf.head can replace this line
domain bit.bdu.edu.et
nameserver 10.161.1.12
nameserver 10.162.65.11
nameserver 4.2.2.2
nameserver 8.8.8.8
# /etc/resolv.conf.tail can replace this line
```



Edit with WPS Office

# Cont....

- If your host gets its IP address and network parameters from a DHCP server,
- The /etc/resolv.conf file should be set up for you automatically. Otherwise you must edit the file manually



Edit with WPS Office

# Cont....

- For newer Ubuntu versions, the nameservers get configured in the **/etc/network/interfaces** file.

```
sudo nano /etc/network/interfaces
```

```
auto lo eth0
```

```
iface lo inet loopback
```

```
iface eth0 inet static
```

```
address 192.168.1.101
```

```
netmask 255.255.255.0
```

```
gateway 192.168.1.1
```

```
dns-nameservers 8.8.8.8
```

```
dns-nameservers 8.8.4.4
```



# TCP/IP Troubleshooting

- Routing information is stored in a table in the kernel.
- Each table entry has several parameters, including a mask for each listed network.
- To route a packet to a particular address, the kernel picks the most specific of the matching routes—that is, the one with the longest mask.
- If the kernel finds no relevant route and no default route, then it returns a “network unreachable” ICMP error to the sender.
- The word “routing” is commonly used to mean two distinct things
- Looking up a network address in the routing table to forward a packet toward its destination Building the routing table in the first place



# Cont....

- You can examine a machine's routing table with **netstat -r**.
- Use **netstat -rn** to avoid DNS lookups and present all the information numerically, which is generally more useful
- Routing tables can be configured statically, dynamically, or with a combination of the two approaches.
- A static route is one that you enter explicitly with the **route** command.
- Static routes remain in the routing table as long as the system is up;
- They are often set up at boot time from one of the system startup scripts. For example, the Linux commands



# Cont....

- route add -net 132.236.220.64 netmask 255.255.255.192 gw 132.236.212.6 eth1
- route add default gw 132.236.227.1 eth0
- Although IP addresses are hardware-independent, hardware addresses must still be used to actually transport data across a network's link layer.13 ARP, the Address Resolution Protocol, discovers the hardware address associated with a particular IP address.



# Cont....

- It can be used on any kind of network that supports broadcasting but is most commonly described in terms of Ethernet.
- If host A wants to send a packet to host B on the same Ethernet, it uses ARP to discover B's hardware address.
- If B is not on the same network as A, host A uses the routing system to determine the next-hop router along the route to B and then uses ARP to find that router's hardware address.



# Cont....

- cover several essential tools, including **ping**, **traceroute**, **netstat**, **tcpdump**, and **Wireshark**  
**PING: CHECK TO SEE IF A HOST IS ALIVE**
- The ping command is embarrassingly simple, but in many situations it is the only
- command you need for network debugging. It sends an ICMP ECHO\_REQUEST
- packet to a target host and waits to see if the host answers back



# Cont...

- To check the status of individual hosts and to test segments of the network.
- Routing tables, physical networks, and gateways are all involved in processing a ping,
- So the network must be more or less working for ping to succeed

## TRACEROUTE: TRACE IP PACKETS

- traceroute, originally written by Van Jacobson, uncovers the sequence of gateways through which an IP packet travels to reach its destination. All modern operating systems come with some version of traceroute.<sup>2</sup> The syntax is simply
- traceroute *hostname*



# Cont....

## Ping 8.8.8.8

```
4 bytes from 8.8.8.8: icmp_seq=35 ttl=57 time=60.8 ms
4 bytes from 8.8.8.8: icmp_seq=36 ttl=57 time=61.7 ms
C
-- 8.8.8.8 ping statistics --
6 packets transmitted, 35 received, 2.77778% packet loss, time 35075ms
rtt min/avg/max/mdev = 60.768/67.500/96.735/7.614 ms
venework@kali:~$ 
```



Edit with WPS Office

# Cont....

- **NETSTAT: GET NETWORK STATISTICS**
- **netstat** collects a wealth of information about the state of your computer's networking software, including interface statistics, routing information, and connection tables. There isn't really a unifying theme to the different sets of output, except that they all relate to the network. Think of **netstat** as the "kitchen sink" of network tools—it exposes a variety of network information that doesn't fit anywhere else. Here, we discuss the five most common uses of **netstat**:
  - Inspecting interface configuration information
  - Monitoring the status of network connections
  - Identifying listening network services
  - Examining the routing table
  - Viewing operational statistics for various network protocols



# Cont....

- On Linux, you may want to use **ifconfig -a** instead of **netstat -i**.
- It prints similar information in a more detailed and more verbose format.
- **tcpdump** and Wireshark belong to a class of tools known as packet sniffers.
- They listen to network traffic and record or print packets that meet criteria of your choice.
- For example, you can inspect all packets sent to or from a particular host, or TCP packets related to one particular network connection.



# Configuring proxy caches (squid )

- Squid is a caching and forwarding web proxy
- Squid is a caching and proxy server that supports several protocols,
- Including HTTP, FTP, and SSL.
- It speeds up a web server by caching repeated requests , www, Dns and other network looks up a group of people for sharing network resources and aiding security by filtering traffic

Sudo apt update

Apt-get install squid

Systemctl start squid

Systemctl status squid // after installation can configure as needed  
Nano /etc/squid/squid.conf is the file location



# Cont.....

```
venework@kali:~$ sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
All packages are up to date.
venework@kali:~$ sudo apt install squid
The following package was automatically installed and is no longer required:
  libfuse3-3
Use 'sudo apt autoremove' to remove it.

Installing:
  squid

Installing dependencies:
  libdbi-perl  libcap3  squid-common  squid-langpack

Suggested packages:
  libmldb-perl  libnet-daemon-perl  libsql-statement-perl  squidclient  squid-cgi  squid-purge  resolvconf  smbclient  ufw  winbind

Summary:
  Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 0
  Download size: 4,160 kB
  Space needed: 16.8 MB / 215 GB available

Continue? [Y/n] 
```



Edit with WPS Office

# Cont....

```
mesg n;s*  
squid  
  
Installing dependencies:  
  libdbi-perl  libcap3  squid-common  squid-langpack  
  
Suggested packages:  
  libmldb perl  libnet-daemon-perl  libsql-statement-perl  squidclient  squid-cgi  squid-purge  resolvconf  smbclient  ufw  winbind  
  
Summary:  
  Upgrading: 0, Installing: 5, Removing: 0, Not Upgrading: 0  
  Download size: 4,160 kB  
  Space needed: 16.8 MB / 215 GB available  
  
Continue? [Y/n] y  
get:1 http://kali.download/kali kali-rolling/main amd64 libcap3 amd64 1.0.1-4 [16.1 kB]  
get:2 http://kali.download/kali kali-rolling/main amd64 squid-langpack all 20220130-1 [169 kB]  
get:3 http://kali.download/kali kali-rolling/main amd64 squid-common all 6.13-1 [321 kB]  
get:4 http://kali.download/kali kali-rolling/main amd64 libdbi-perl amd64 1.647-1 [861 kB]  
get:5 http://kali.download/kali kali-rolling/main amd64 squid amd64 6.13-1 [2,793 kB]  
Fetched 4,160 kB in 6s (682 kB/s)  
Selecting previously unselected package libcap3:amd64.  
Reading database ... 85%
```



Edit with WPS Office

# Cont....

```
Selecting previously unselected package libdbi-perl:amd64.
Preparing to unpack .../libdbi-perl_1.647-1_amd64.deb ...
Unpacking libdbi-perl:amd64 (1.647-1) ...
Selecting previously unselected package squid.
Preparing to unpack .../squid_6.13-1_amd64.deb ...
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
Unpacking squid (6.13-1) ...
Setting up squid-langpack (20220130-1) ...
Setting up libdbi-perl:amd64 (1.647-1) ...
Setting up libecap3:amd64 (1.0.1-4) ...
Setting up squid-common (6.13-1) ...
Setting up squid (6.13-1) ...
Setcap worked! /usr/lib/squid/pinger is not uid!
Skipping profile in /etc/apparmor.d/disable: usr.sbin.squid
update-alternatives: using /usr/sbin/squid-gnutls to provide /usr/sbin/squid (squid) in auto mode
update-rc.d: We have no instructions for the squid init script.
update-rc.d: It looks like a network service, we disable it.
squid.service is a disabled or a static unit, not starting it.
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.2.0) ...
venework@kali:~$ 
```



Edit with WPS Office

# Cont....

```
yenework@kali:~$ sudo nano /etc/squid/squid.conf
yenework@kali:~$ sudo systemctl start squid
yenework@kali:~$ sudo systemctl restart squid
```



Edit with WPS Office

# Cont....

```
yenework@kali:~$ sudo nano /etc/squid/squid.conf  
yenework@kali:~$ sudo systemctl start squid  
yenework@kali:~$ sudo systemctl restart squid
```



Edit with WPS Office

# cont. ....

```
# configuration files.
# Define the ACL
#acl blocked_sites dstdomain .facebook.com .youtube.com

# Deny access to blocked sites
#http_access deny blocked_sites

# Allow your network
#acl mynetwork src 192.168.43.176/24
#http_access allow mynetwork

# Default deny all
#http_access deny all

# Values with byte units
#
# Squid accepts size units on some size related directives. All
^G Help      ^O Write Out ^F Where Is   ^K Cut        ^T Execute    ^C L
^X Exit      ^R Read File  ^\ Replace   ^U Paste      ^J Justify    ^/ D
```



Edit with WPS Office

# Cont.....

- Squid not only caches information from local user requests but also allows construction of a hierarchy of Squid servers.
- To make effective use of Squid, you'll likely want to force your users to use the cache. Either configure a default proxy through Active Directory (in a Windows based environment) or configure your router to redirect all web-based traffic to the Squid cache by using the Web Cache Communication Protocol, WCCP.
- Squid is easy to install and configure.
- Since Squid needs space to store its cache, you should run it on a dedicated machine that has plenty of free memory and disk space.



# Cont....

- A configuration for a large cache would be a machine with 32GiB of RAM and 8TB of disk.
- Once you've installed Squid, you must localize the squid.conf configuration file.
- See the QUICKSTART file in the distribution directory for a list of the changes you need to make to the sample squid.conf file.



Edit with WPS Office

# Cont....

Add

```
acl newlist src 192.168.6.133  
acl block dstdomain "/etc/squid/block.txt"  
http _access deny newlist block.....
```



Edit with WPS Office

# Configuring mail transfer agents

- Configuring mail transfer agents means setting up a system to send, receive and manage emails
- The most popular mail transfer agents are postfix, send email etc.
- To install postfix
- 1. update package list
- Sudo apt update
- Install postfix agent
- sudo apt install postfix
- After postfix is installed a configuration screen is open



Edit with WPS Office

# Cont.....

Options

Internet site

Satellite system

Local only etc.

you have to run

`sudo dpkg-reconfigure postfix`

To check is the postfix is installed fully or not



Edit with WPS Office

# configuring web server

```
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
update-rc.d: As per Kali policy, apache2 init script is left disabled.
update-rc.d: We have no instructions for the apache-htcacheclean init script.
update-rc.d: It looks like a non-network service, we enable it.
apache2.service is a disabled or a static unit, not starting it.
apache-htcacheclean.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2025.2.0) ...
Processing triggers for man-db (2.13.0-1) ...
yenework@kali:~$ sudo systemctl start apache2
yenework@kali:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/system/apache2.service'.
```



Edit with WPS Office

# Cont ....

```
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
update-rc.d: As per Kali policy, apache2 init script is left disabled.
update-rc.d: We have no instructions for the apache-htcacheclean init script.
update-rc.d: It looks like a non-network service, we enable it.
apache2.service is a disabled or a static unit, not starting it.
apache-htcacheclean.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2025.2.0) ...
Processing triggers for man-db (2.13.0-1) ...
yenework@kali:~$ sudo systemctl start apache2
yenework@kali:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/system/apache2.service'.
yenework@kali:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
   Active: active (running) since Sat 2025-04-26 21:58:19 EDT; 50s ago
     Invocation: 454319af7a9b4320a03370f574ce8d66
      Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 8606 (apache2)
       Tasks: 55 (limit: 4538)
      Memory: 7.4M (peak: 8M)
        CPU: 75ms
       CGroup: /system.slice/apache2.service
               └─8606 /usr/sbin/apache2 -k start
                  ├─8608 /usr/sbin/apache2 -k start
                  ├─8609 /usr/sbin/apache2 -k start

Apr 26 21:58:19 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Apr 26 21:58:19 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```



Edit with WPS Office

# Cont.....

The screenshot shows a web browser window with multiple tabs open at the top. The active tab displays the Apache2 Debian Default Page. The page features the Debian logo and the title "Apache2 Debian Default Page". A red banner across the middle contains the text "It works!". Below the banner, there is explanatory text about the purpose of the page and instructions for configuration. A section titled "Configuration Overview" provides details about the configuration files used by Apache2 on Debian systems. At the bottom of the page, there is a code block showing the directory structure of configuration files in /etc/apache2/.

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

#### Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   |-- *.load
|   '-- *.conf
```



Edit with WPS Office

# SSH Installation

```
+1                                         yenework@kali: ~
yenework@kali:~$ sudo apt install openssh-server
The following package was automatically installed and is no longer required:
  libfuse3-3
Use 'sudo apt autoremove' to remove it.

Installing:
  openssh-server

Installing dependencies:
  libfido2-1  ncurses-term  openssh-client  openssh-sftp-server  runit-helper

Suggested packages:
  keychain  libpam-ssh  monkeysphere  ssh-askpass  molly-guard  ufw

Summary:
  Upgrading: 0, Installing: 6, Removing: 0, Not Upgrading: 0
  Download size: 2,160 kB
  Space needed: 12.4 MB / 214 GB available

Continue? [Y/n] y
Get:3 http://kali.download/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:9.9p2-2 [65.4 kB]
Get:2 http://mirrors.netix.net/kali kali-rolling/main amd64 openssh-client amd64 1:9.9p2-2 [968 kB]
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libfido2-1 amd64 1.15.0-1+b1 [78.7 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 runit-helper all 2.16.4 [7,296 B]
Get:5 http://kali.download/kali kali-rolling/main amd64 openssh-server amd64 1:9.9p2-2 [523 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 ncurses-term all 6.5+20250216-2 [518 kB]
Fetched 2,160 kB in 4s (485 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libfido2-1:amd64.
(Reading database ... 60%
```



Edit with WPS Office

# Cont ....

```
packing openssh-sftp-server (1:9.9p2-2) ...
selecting previously unselected package runit-helper.
preparing to unpack .../3-runit-helper_2.16.4_all.deb ...
packing runit-helper (2.16.4) ...
selecting previously unselected package openssh-server.
preparing to unpack .../4.openssh-server_1%3a9.9p2-2_amd64.deb ...
packing openssh-server (1:9.9p2-2) ...
selecting previously unselected package ncurses-term.
preparing to unpack .../5-ncurses-term_6.5+20250216-2_all.deb ...
packing ncurses-term (6.5+20250216-2) ...
etting up runit-helper (2.16.4) ...
etting up libfido2-1:amd64 (1.15.0-1+b1) ...
etting up ncurses-term (6.5+20250216-2) ...
etting up openssh-client (1:9.9p2-2) ...
etting up openssh-sftp-server (1:9.9p2-2) ...
etting up openssh-server (1:9.9p2-2) ...
eating config file /etc/ssh/sshd_config with new version
eating SSH2 RSA key; this may take some time ...
72 SHA256:82nqor5TuLL2sqzE0ZfmHW1S5VHQHQZ12TcA7A6Q+g root@kali (RSA)
eating SSH2 ECDSA key; this may take some time ...
6 SHA256:BAQHgRdwVjLUi1FGyNpKmWUBTV/VazlD0BKotbFEWSw root@kali (ECDSA)
eating SSH2 ED25519 key; this may take some time ...
6 SHA256:+JwsOCl2ISSdDbANsMPWjLXDD8YkNLE5fxzrcSzU root@kali (ED25519)
date-rc.d: As per Kali policy, ssh init script is left disabled.
h.service is a disabled or a static unit, not starting it.
h.socket is a disabled or a static unit, not starting it.
rocessing triggers for man-db (2.13.0-1) ...
rocessing triggers for kali-menu (2025.2.0) ...
rocessing triggers for libc-bin (2.41-6) ...
nework@kali:~$ sudo systemctl start ssh
nework@kali:~$ sudo systemctl enable ssh
nchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
ecuting: /usr/lib/systemd/systemd-sysv-install enable ssh
reated symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system/ssh.service'.
reated symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
nework@kali:~$ 
```



Edit with WPS Office

# Cont....

```
newwork@kali:~$ sudo systemctl start ssh
newwork@kali:~$ sudo systemctl enable ssh
  Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
  Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
  Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system/ssh.service'.
  Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
newwork@kali:~$ sudo systemctl status ssh
  ssh.service - OpenBSD Secure Shell server
    Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
    Active: active (running) since Sat 2025-04-26 22:08:29 EDT; 38s ago
      Invocation: fd8280383bd54f47b5032fddaf971487
        Docs: man:sshd(8)
               man:sshd_config(5)
    Main PID: 11064 (sshd)
      Tasks: 1 (limit: 4538)
     Memory: 2.1M (peak: 2.8M)
       CPU: 88ms
      CGroup: /system.slice/ssh.service
              └─11064 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Apr 26 22:08:29 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Apr 26 22:08:29 kali sshd[11064]: Server listening on 0.0.0.0 port 22.
Apr 26 22:08:29 kali sshd[11064]: Server listening on :: port 22.
Apr 26 22:08:29 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
newwork@kali:~$ █
```



Edit with WPS Office

# configuring Linux box as router

Allow forward packets between two or more networks

Open nano /etc/sysctl.conf

Add this line ctrl+0, enter and ctrl+x

```
GNU nano 8.4                               /etc/sysctl.conf
net.ipv4.ip_forward=1
```



Edit with WPS Office

# Cont.....

Set up nat as shown below

```
yenework@kali:~$ sudo iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
yenework@kali:~$ sudo iptables -A FORWARD -i eth0 -o wlan0 -j ACCEPT
yenework@kali:~$ sudo iptables -A FORWARD -i eth0 -o wlan0 -j ACCEPT
yenework@kali:~$ █
```



Edit with WPS Office

```
yenework㉿kali:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
yenework㉿kali:~$ sudo nano /etc/sysctl.conf
yenework㉿kali:~$ sudo nano /etc/sysctl.conf
yenework㉿kali:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
yenework㉿kali:~$ 
```



Edit with WPS Office

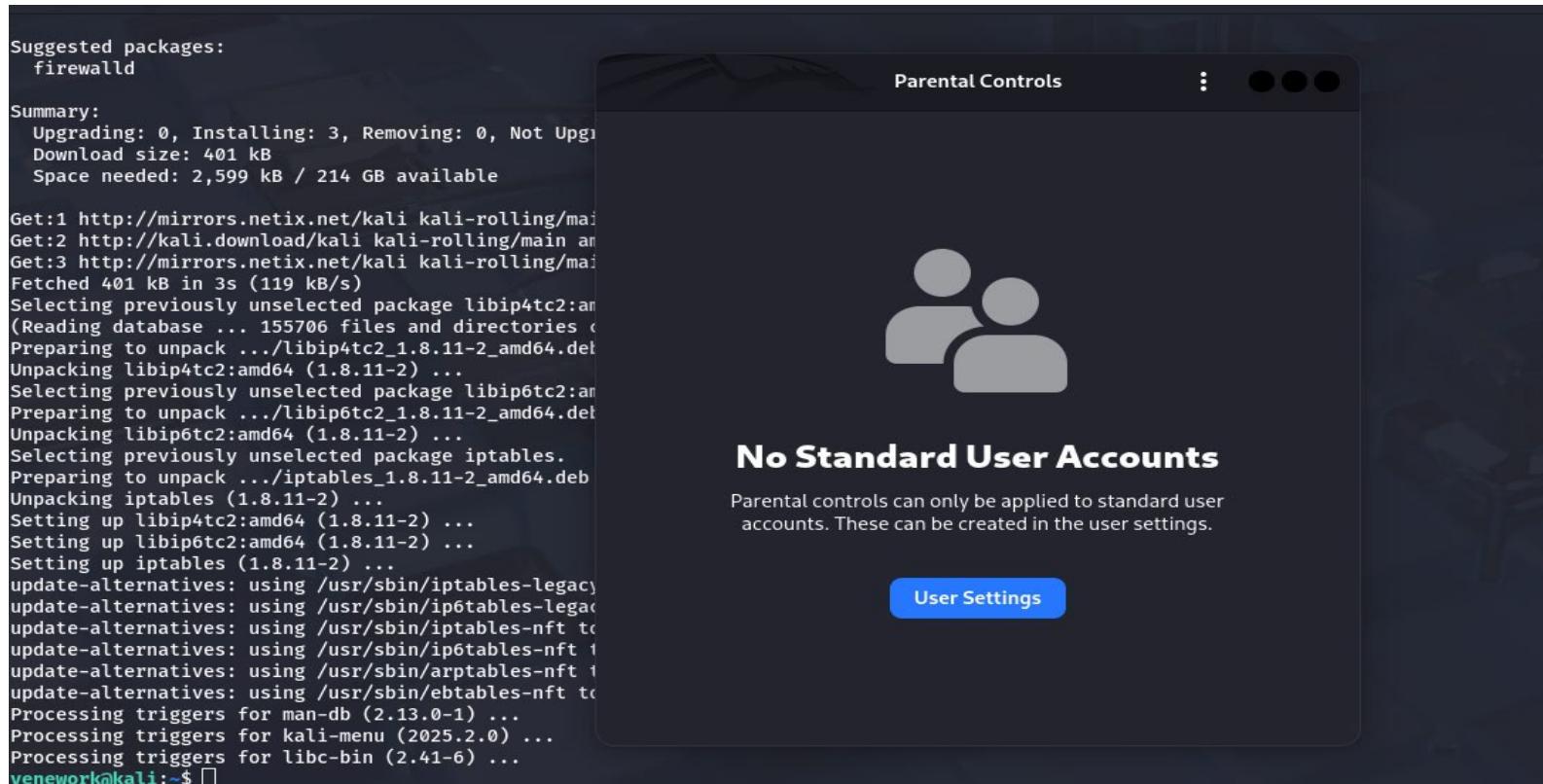
# Cont....

```
yenework@kali:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
yenework@kali:~$ sudo nano /etc/sysctl.conf
yenework@kali:~$ sudo nano /etc/sysctl.conf
yenework@kali:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
yenework@kali:~$ []
```



Edit with WPS Office

# Cont....



Suggested packages:  
firewalld

Summary:  
Upgrading: 0, Installing: 3, Removing: 0, Not Upg  
Download size: 401 kB  
Space needed: 2,599 kB / 214 GB available

```
Get:1 http://mirrors.netix.net/kali kali-rolling/main amd64 libip4tc2 amd64 1.8.11-2
Get:2 http://kali.download/kali kali-rolling/main amd64 libip6tc2 amd64 1.8.11-2
Get:3 http://mirrors.netix.net/kali kali-rolling/main amd64 iptables amd64 1.8.11-2
Fetched 401 kB in 3s (119 kB/s)
Selecting previously unselected package libip4tc2:amd64.
(Reading database ... 155706 files and directories currently installed.)
Preparing to unpack .../libip4tc2_1.8.11-2_amd64.deb ...
Unpacking libip4tc2:amd64 (1.8.11-2) ...
Selecting previously unselected package libip6tc2:amd64.
Preparing to unpack .../libip6tc2_1.8.11-2_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.11-2) ...
Selecting previously unselected package iptables.
Preparing to unpack .../iptables_1.8.11-2_amd64.deb ...
Unpacking iptables (1.8.11-2) ...
Setting up libip4tc2:amd64 (1.8.11-2) ...
Setting up libip6tc2:amd64 (1.8.11-2) ...
Setting up iptables (1.8.11-2) ...
update-alternatives: using /usr/sbin/iptables-legacy to provide /sbin/iptables (update-alternatives: using /usr/sbin/ip6tables-legacy to provide /sbin/ip6tables (update-alternatives: using /usr/sbin/iptables-nft to provide /sbin/iptables (update-alternatives: using /usr/sbin/ip6tables-nft to provide /sbin/ip6tables (update-alternatives: using /usr/sbin/arpTables-nft to provide /sbin/arpTables (update-alternatives: using /usr/sbin/eBTables-nft to provide /sbin/eBTables Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.2.0) ...
Processing triggers for libc-bin (2.41-6) ...
venework@kali:~$
```

Parental Controls



## No Standard User Accounts

Parental controls can only be applied to standard user accounts. These can be created in the user settings.

[User Settings](#)



Edit with WPS Office

# Configuration of firewalls

```
venework@kali:~$ sudo apt install ufw
The following package was automatically installed and is no longer required:
  libfuse3-3
Use 'sudo apt autoremove' to remove it.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 169 kB
  Space needed: 880 kB / 214 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 2s (83.3 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 155921 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.2.0) ...
Processing triggers for man-db (2.13.0-1) ...
venework@kali:~$ sudo ufw enable
```



Edit with WPS Office

# Cont.....

And then allow and deny specific traffic as shown below

```
venework@kali:~$ sudo ufw allow 22
Rule added
Rule added (v6)
venework@kali:~$ 
```



Edit with WPS Office

# iptables

Before making any changes view existing rule

Sudo iptables -L as shown below

```
/home/yenework/Documents  
Directory /home/yenework/Documents exists. Here are the files inside:  
'ch sys admin.pptx'  'Untitled 1.odp'  
yenework@kali:~$ vi first_script.sh  
yenework@kali:~$ sudo ufw status  
[sudo] password for yenework:  
sudo: ufw: command not found  
yenework@kali:~$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target     prot opt source          destination  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination  
yenework@kali:~$ sudo apt update  
Hit:1 http://http.kali.org/kali kali-rolling InRelease  
All packages are up to date.  
yenework@kali:~$ █
```



Edit with WPS Office

# Cont....

Allow specific traffic by using the following command

```
iptables v1.8.11 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be root)
yenework@kali:~$ sudo iptables -A INPUT -i wlan0 -d 192.168.43.176 -p tcp --dport 22 -j ACCEPT
yenework@kali:~$ sudo iptables -A INPUT -i wlan0 -d 192.168.43.176 -p icmp --icmp-type 8 -j ACCEPT
yenework@kali:~$ sudo iptables -A INPUT -i lo -d 127.0.0.1 -j ACCEPT
yenework@kali:~$ 
```



Edit with WPS Office

# Cont....

Save ip table rules

`sudo apt install iptables-persistent`



Edit with WPS Office

# Cont....

To view current firewall rules with detail statics

Run the command `sudo iptables -L input v -n -line numbers`

```
yenework@kali:~$ iptables -L INPUT -v -n --line-numbers
iptables v1.8.11 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be root)
yenework@kali:~$ sudo iptables -L INPUT -v -n --line-numbers
Chain INPUT (policy DROP 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out      source          destination
1    2162  521K ufw-before-logging-input  all  --  *      *      0.0.0.0/0          0.0.0.0/0
2    2162  521K ufw-before-input   all  --  *      *      0.0.0.0/0          0.0.0.0/0
3      0     0 ufw-after-input   all  --  *      *      0.0.0.0/0          0.0.0.0/0
4      0     0 ufw-after-logging-input all  --  *      *      0.0.0.0/0          0.0.0.0/0
5      0     0 ufw-reject-input  all  --  *      *      0.0.0.0/0          0.0.0.0/0
6      0     0 ufw-track-input  all  --  *      *      0.0.0.0/0          0.0.0.0/0
7      0     0 ACCEPT     tcp  --  wlan0  *      0.0.0.0/0          10.1.1.1           tcp dpt:22
8      0     0 ACCEPT     tcp  --  wlan0  *      0.0.0.0/0          10.1.1.1           tcp dpt:22
9      0     0 ACCEPT     tcp  --  wlan0  *      0.0.0.0/0          10.1.1.1           tcp dpt:22
10     0     0 ACCEPT     all  --  lo     *      0.0.0.0/0          127.0.0.1
11     0     0 ACCEPT     icmp --  wlan0  *      0.0.0.0/0          10.1.1.1           icmptype 8
12     0     0 ACCEPT     icmp --  wlan0  *      0.0.0.0/0          192.168.43.176    icmptype 8
13     0     0 ACCEPT     all  --  lo     *      0.0.0.0/0          127.0.0.1
14     0     0 ACCEPT     tcp  --  wlan0  *      0.0.0.0/0          192.168.43.176    tcp dpt:22
15     0     0 ACCEPT     icmp --  wlan0  *      0.0.0.0/0          192.168.43.176    icmptype 8
16     0     0 ACCEPT     all  --  lo     *      0.0.0.0/0          127.0.0.1
yenework@kali:~$ 
```



# Cont.....

The above result is shown due to override by ufw  
The current default policy is still DROP  
So you have to make iptables persistent



Edit with WPS Office

# Cont....

```
venework@kali:~$ sudo iptables -A INPUT -p icmp --icmp-type 0 -j ACCEPT
venework@kali:~$ sudo Iptables -A INPUT -p icmp --icmp-type 3 -j ACCEPT
sudo: Iptables: command not found
venework@kali:~$ sudo iptables -A INPUT -p icmp --icmp-type 0 -j ACCEPT
venework@kali:~$ sudo iptables -A INPUT -p icmp --icmp-type 3 -j ACCEPT
venework@kali:~$ sudo iptables -A INPUT -p icmp --icmp-type 5 -j ACCEPT
venework@kali:~$ sudo iptables -A INPUT -p icmp --icmp-type 11 -j ACCEPT
venework@kali:~$ sudo iptables -A FORWARD -d 192.168.43.176 -p icmp --icmp-type 0 -j ACCEPT
venework@kali:~$ sudo iptables -A FORWARD -d 192.168.43.176 -p icmp --icmp-type 3 -j ACCEPT
venework@kali:~$ sudo iptables -A FORWARD -d 192.168.43.176 -p icmp --icmp-type 5 -j ACCEPT
venework@kali:~$ sudo iptables -A FORWARD -d 192.168.43.176 -p icmp --icmp-type 11 -j ACCEPT
venework@kali:~$ sudo iptables -L -v -n --line-numbers
```



Edit with WPS Office

# cont.....

If you use Debian based Linux system dont forget save the configuration



Edit with WPS Office