Chapter Three

Network management

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

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 adminstrator.
- 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

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

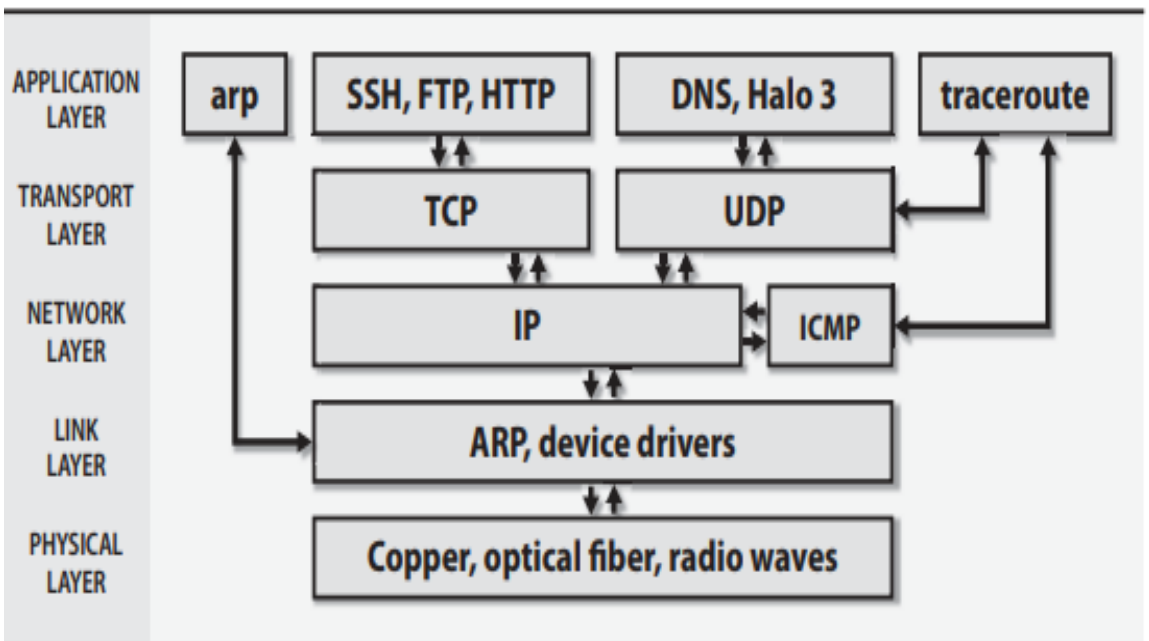
Cont....

- 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

Cont....

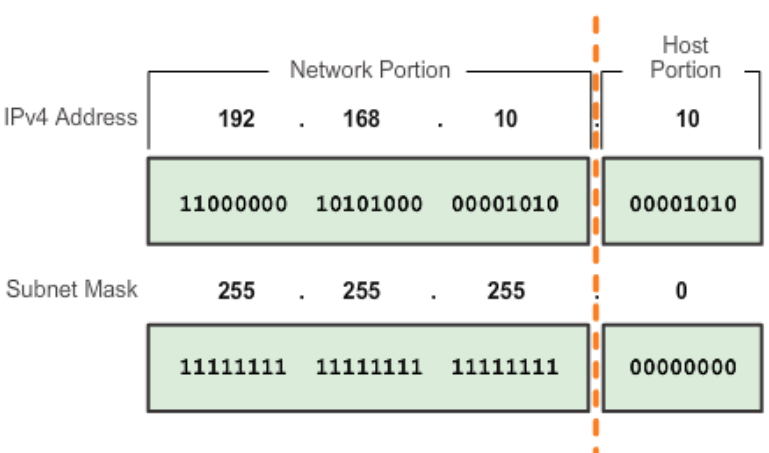
- These protocols are arranged in a hierarchy or “stack”,
- With the higher-level protocols making use of the protocols beneath them.
- TCP/IP is conventionally described as a five-layer system

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 work devices already support I



Cont....

Subnet mask

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

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

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

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.

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.

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 cheek available interfaces
- Linux network configuration file location
- File location /etc/network/interfaces

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

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

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
```

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

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)

Cont....

- but if the network manager is not installd
- 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 chenges in netplan
- sudo netplan apply for WSL
- For other Linux os
- sudo nano /etc/network/interfaces

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

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:

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

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:

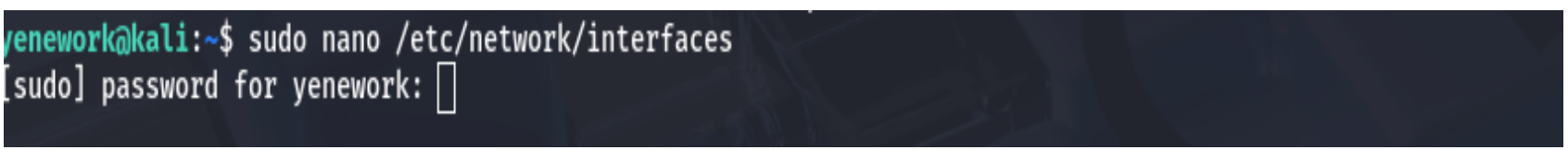
auto lo eth0
iface lo inet loopback
iface eth0 inet static
address 192.168.1.101
netmask 255.255.255.0
gateway 192.168.1.1

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**

Cont....

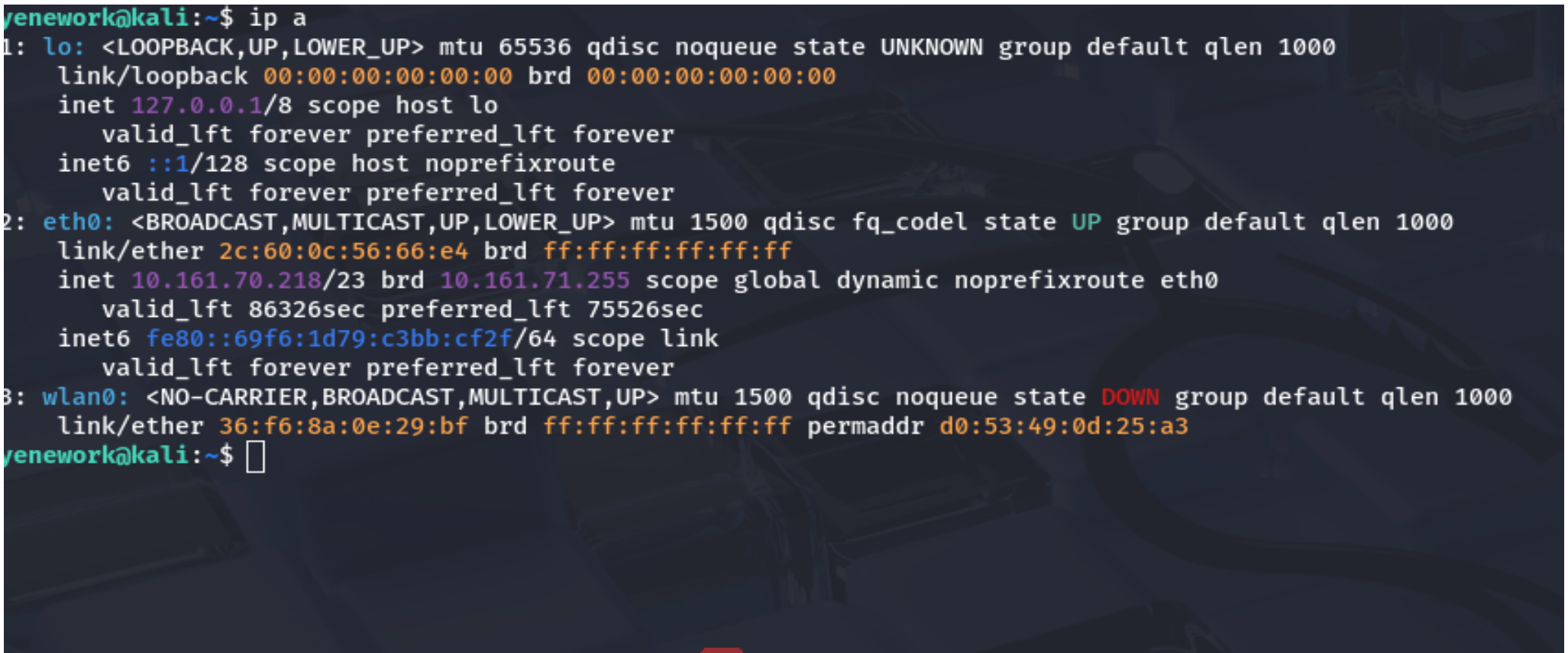
- Static network configuration and automatic
- DHCP Linux network config



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

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
```



Configuring DNS server....

- DNS is a database system that translates a computers fully qualified domain name in to IP address
- www.amazon.com to 207.171.166.48

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*

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

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]

- ……

Cont....

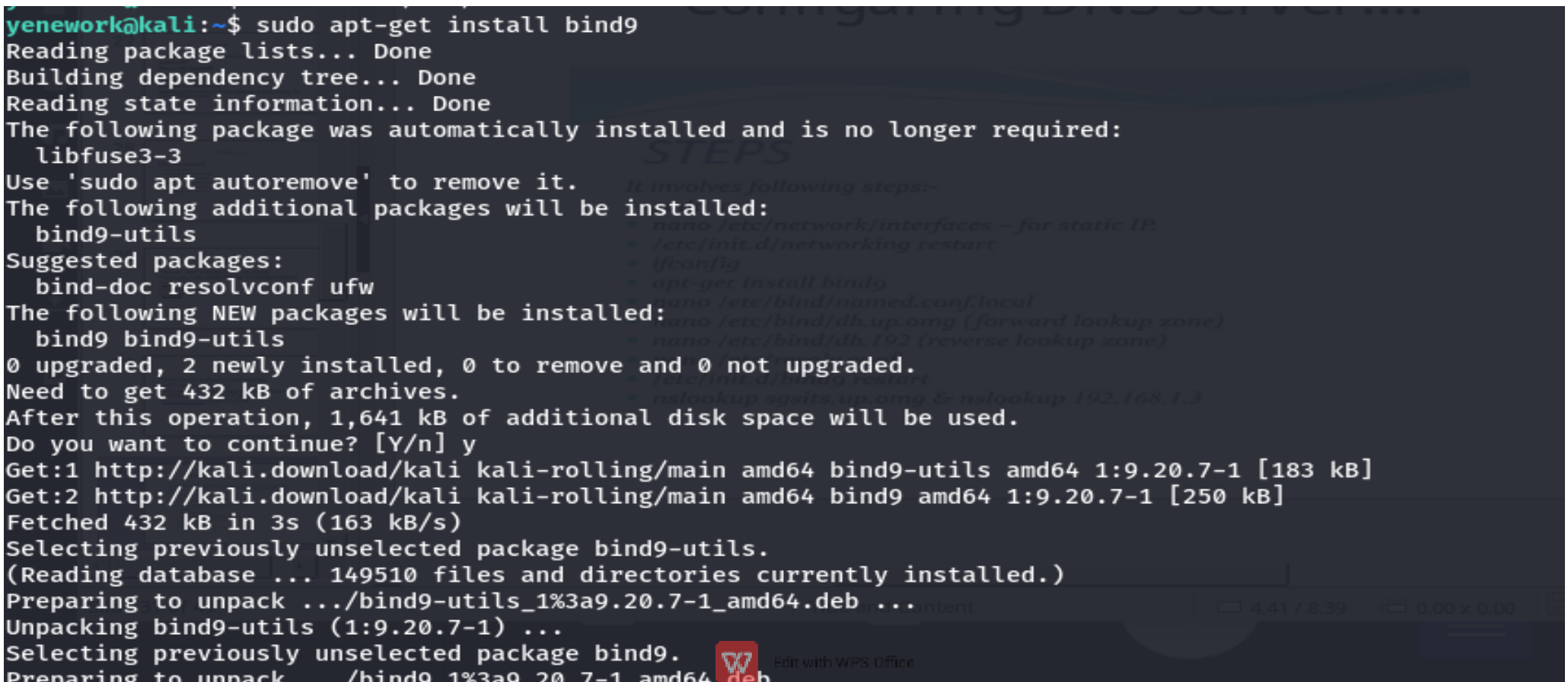
- To see the upgrade content
- tsion@DESKTOP-3L0GAMB:~$ apt list –upgradable
- After this installing BIND9 DNS server
- sudo apt install bind9 bind9utils bind9-doc
- tsion@DESKTOP-3L0GAMB:~$ sudo apt install bind9 bind9utils bind9-doc
- sudo nano /etc/bind/named.conf.options
- Open this configuration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

Cont....

- To install and configure DNS
- Sudo apt update
- Sudo apt upgrade // update systems to get installation packeges

- sudo nano /etc/bind/named.conf.local

To install bind9



Configure a local DNS name server

```
Processing triggers for kali-menu (2025.2.0) ...
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;
};

//
```

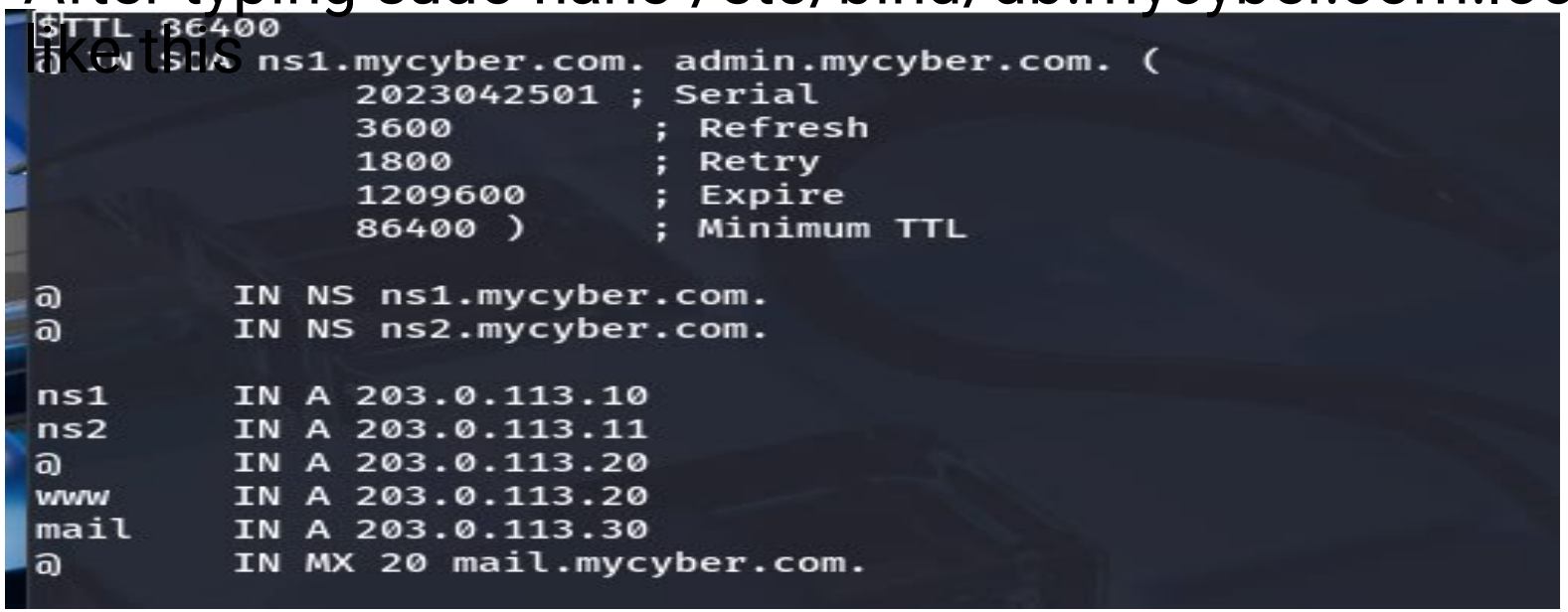
Cont…

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

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

You can edit as shown below

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



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
```

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:~$
```

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: cdfc539a1ba41f1901000000680b891f0ad5468c71e9fcd7 (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
```

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:~$
```

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:~$
```

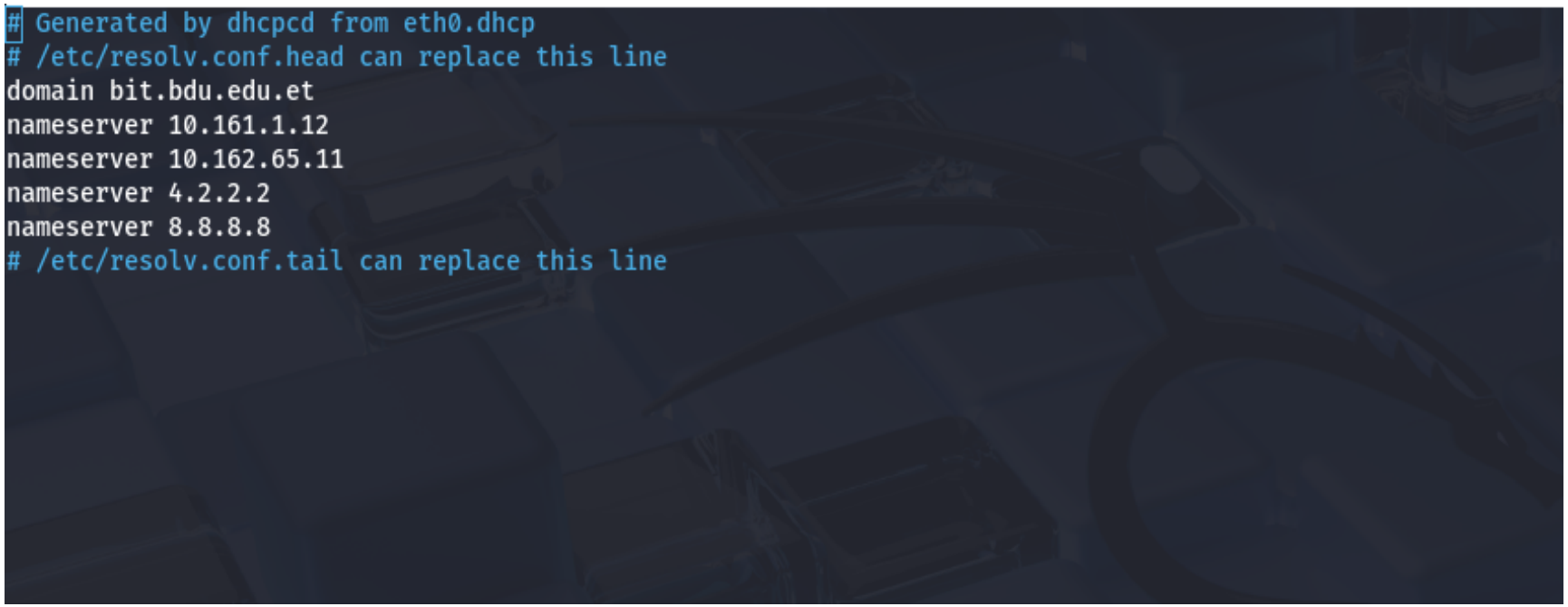
Cont.....

```
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:~$
```

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.

Cont....



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

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....

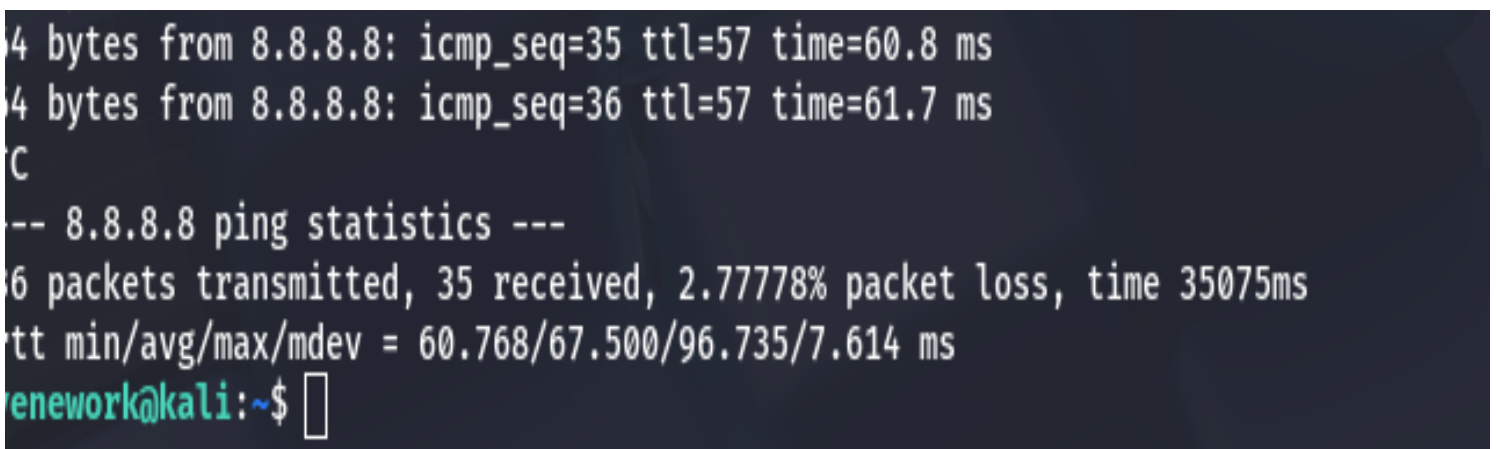
- cover several essential tools, including **ping**, **traceroute**, **netstat**, **tcpdump**, and Wireshark
  PING: CHECK TO SEE IF A HOST IS ALIVE
- The ping command is embarrassingly simple, but in many situations it is the only
- command you need for network debugging. It sends an ICMP ECHO_REQUEST
- 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.2 The syntax is simply
- traceroute *hostname*

Cont....

Ping 8.8.8.8



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 speeding up a web server by caching repeated requests , www,

Dns and other network looks up a groupe of people for sharing network resources and aiding security by filtering trafic

Sudo apt update

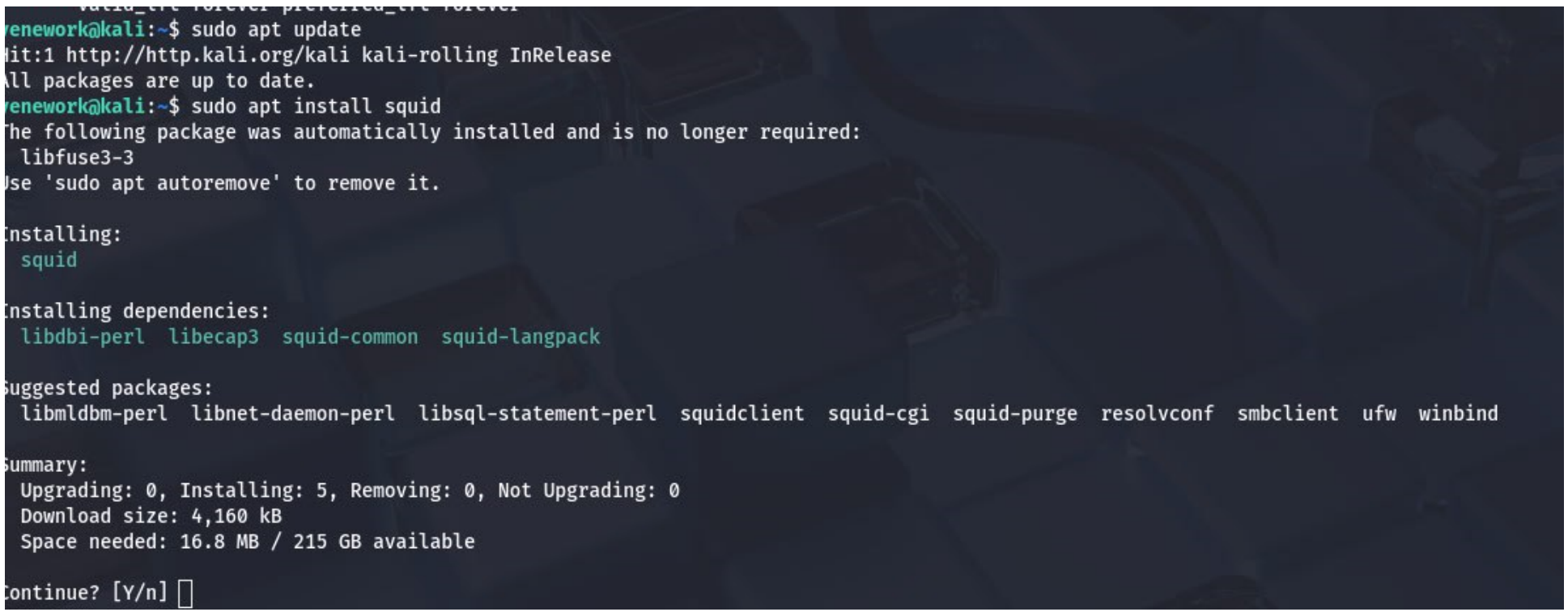
Apt-get insatall squid

Systemctl start squid

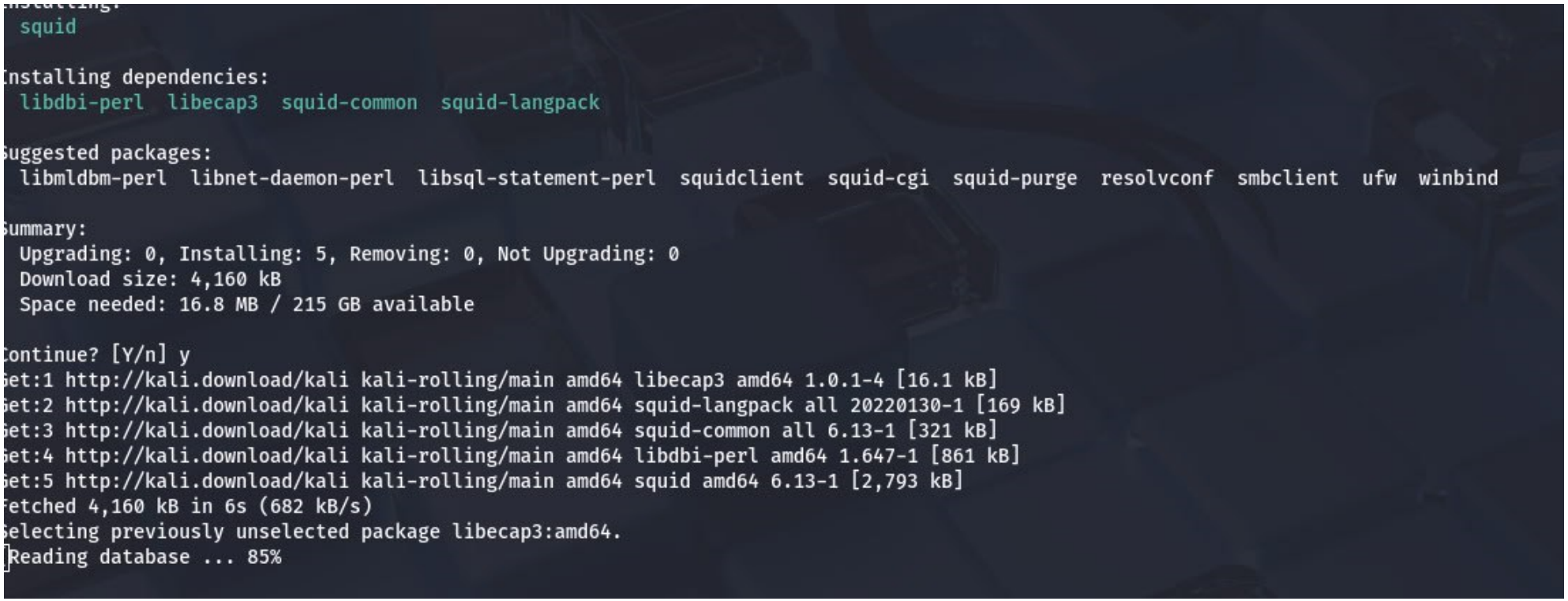
Systemctl status squid // after installation can configure as needed

Nano /etc/squid/squid.conf is the file location

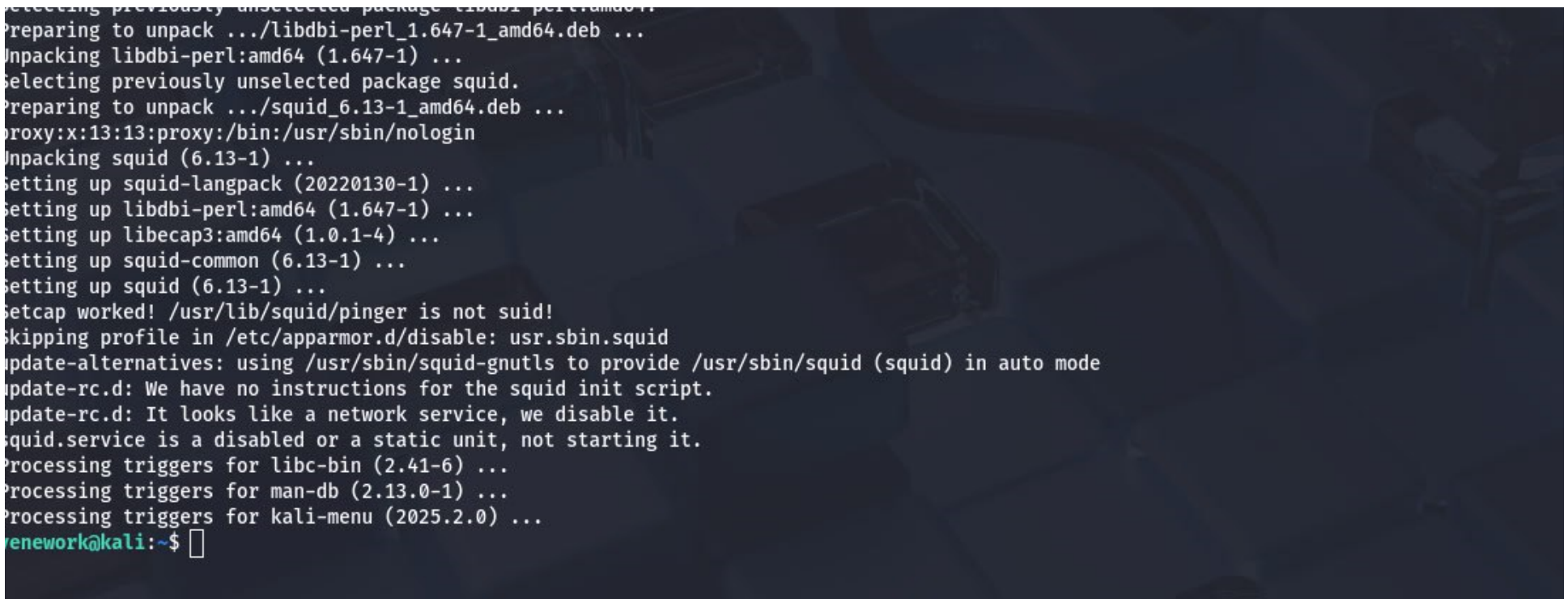
Cont.....



Cont....



Cont....

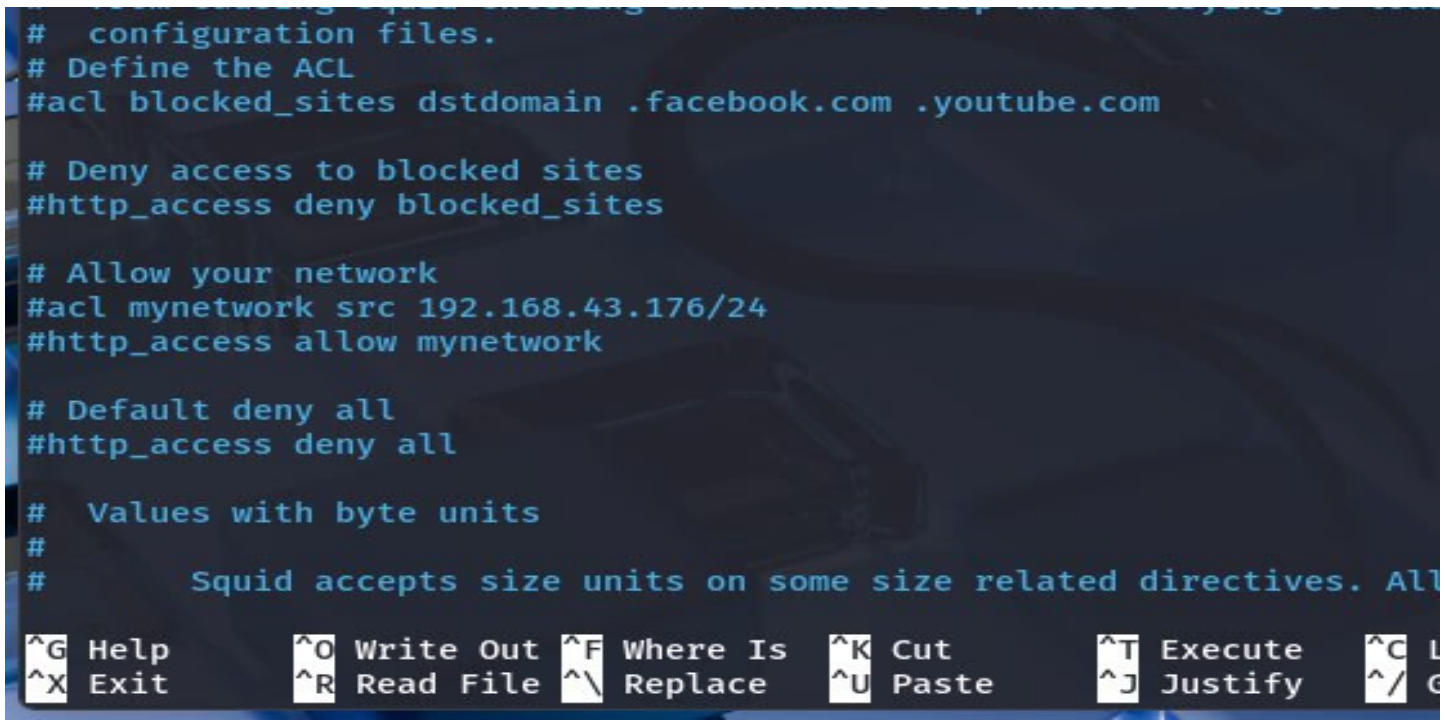


Cont....

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

Cont....

cont. ....



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.

Cont....

Add

acl newlist src 192.168.6.133

acl block dstdomain “/etc/squid/block.txt”

http _access deny newlist block……

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

Cont.....

Options

Internet site

Satellite system

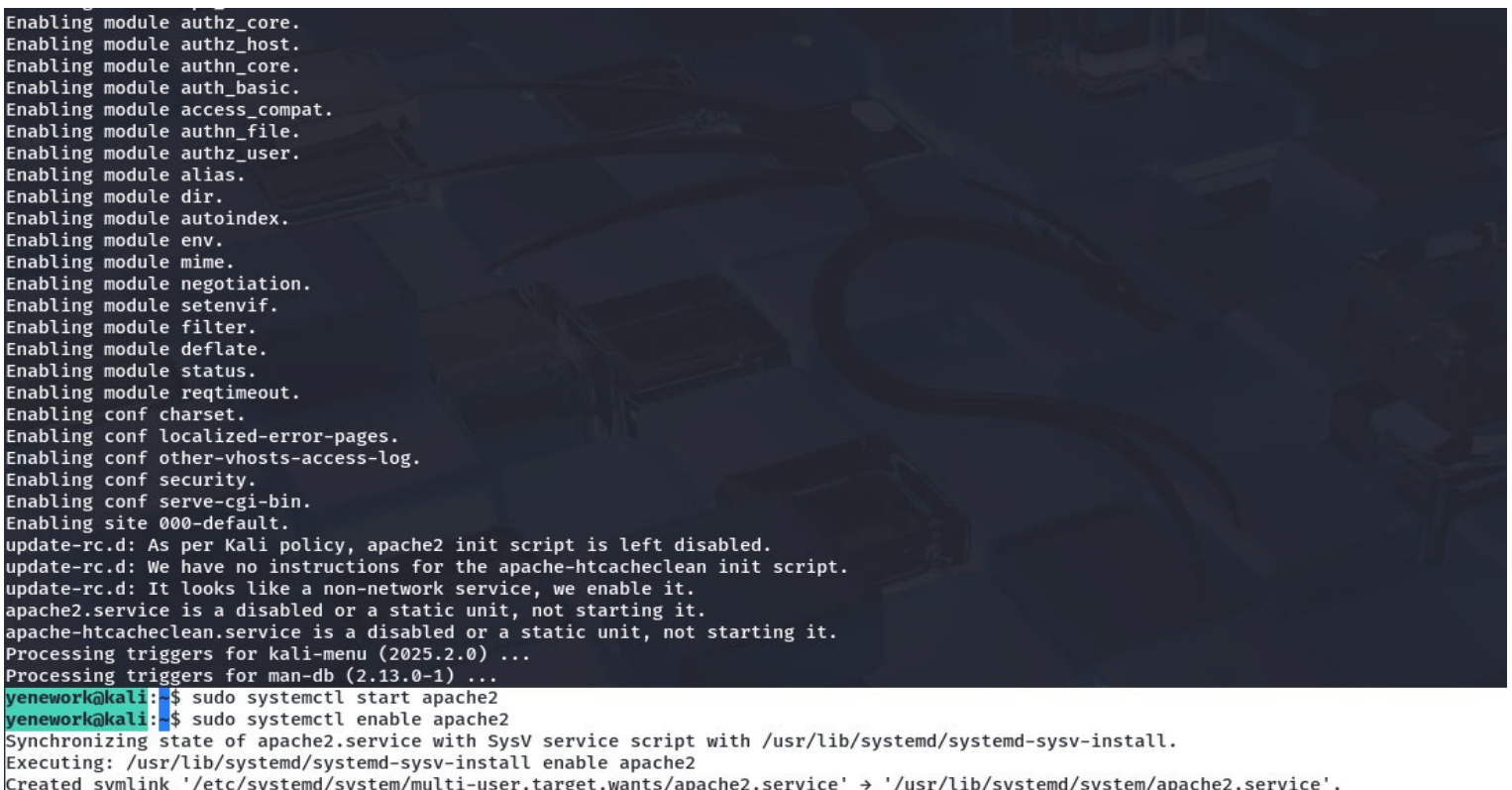
Local only etc.

you have to run

sudo dpkg-reconfigure postfix

To check is the postfix is installed fully or not

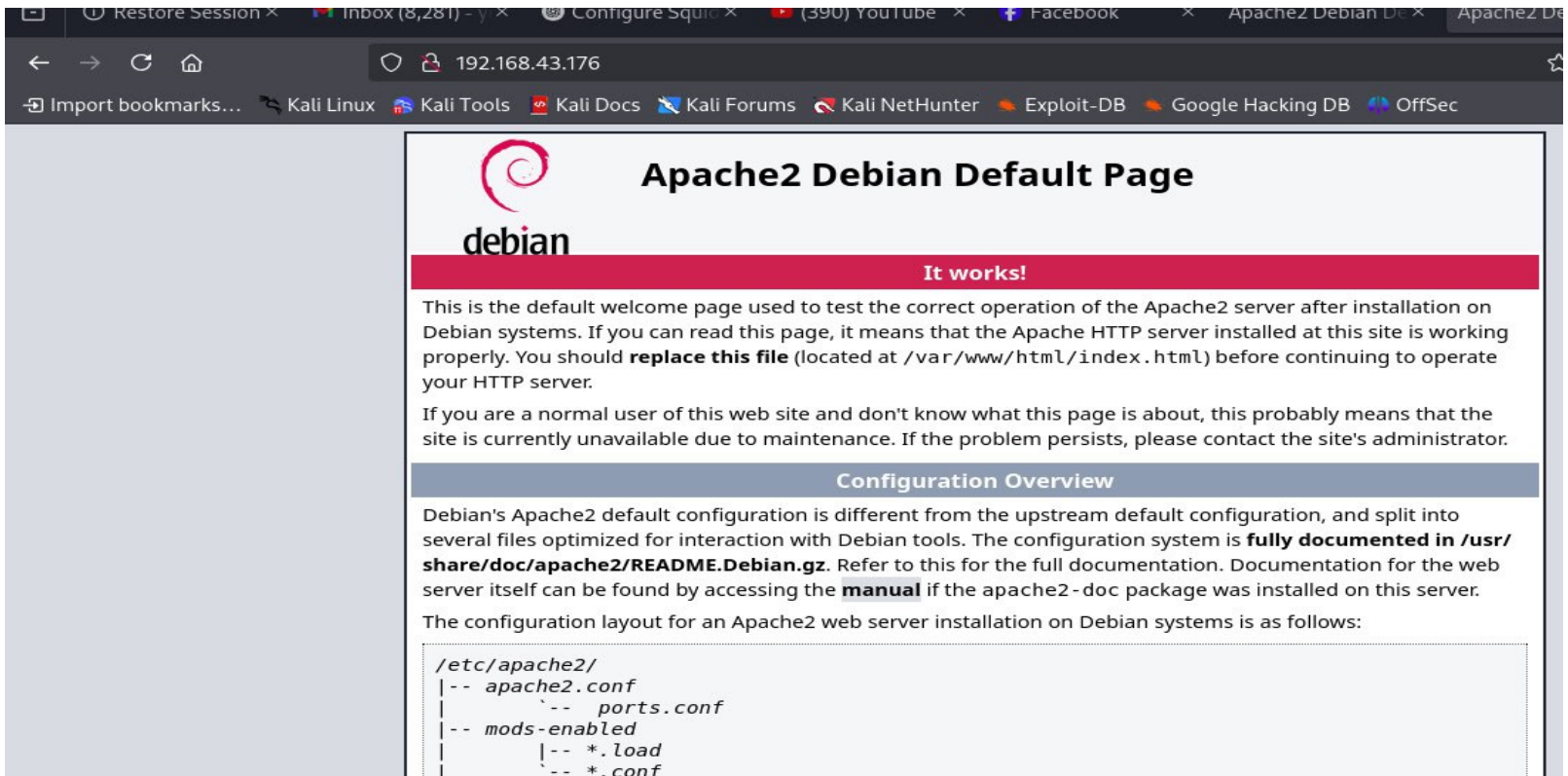
configuring web server



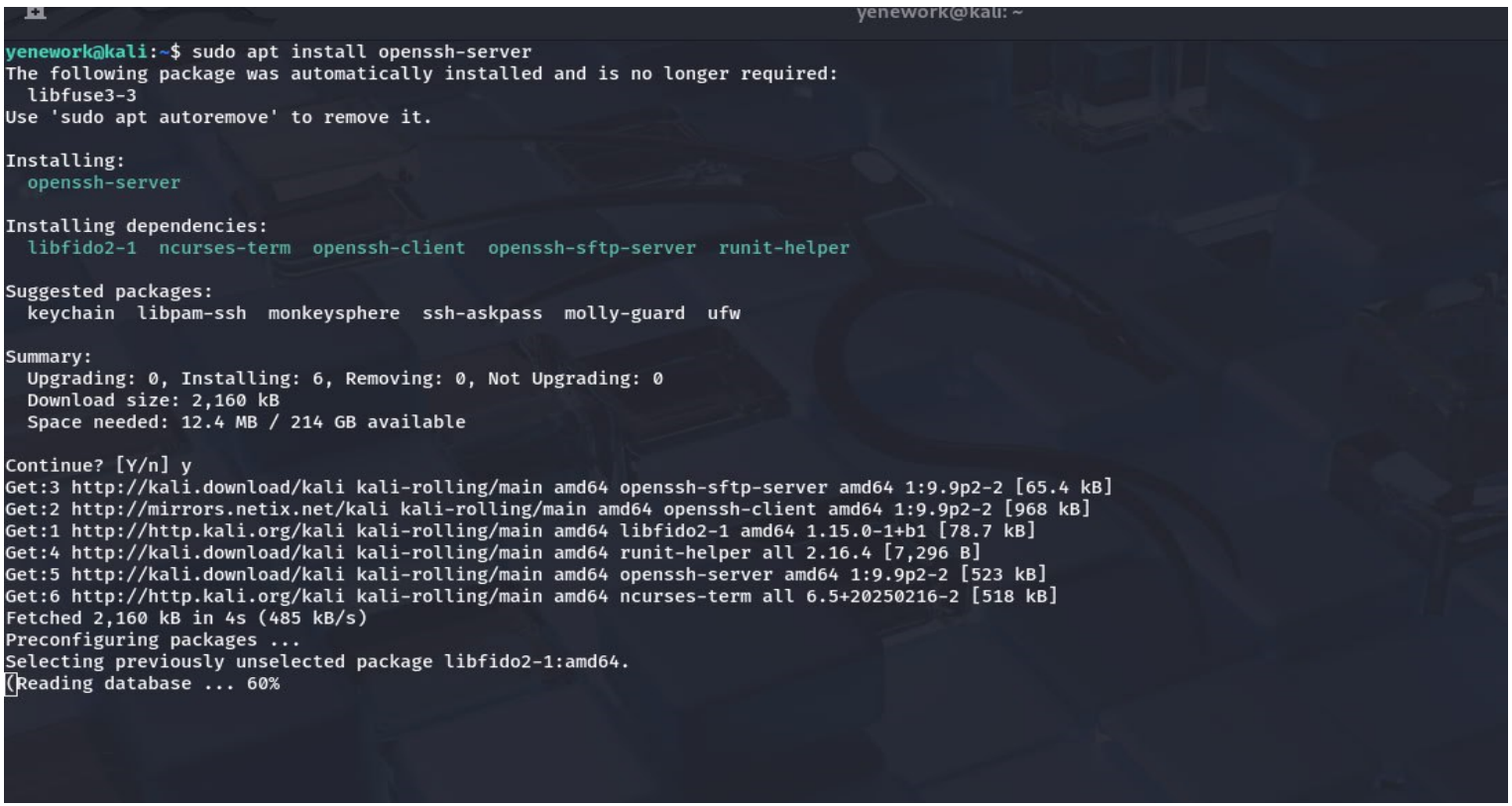
Cont ....

```
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.
```

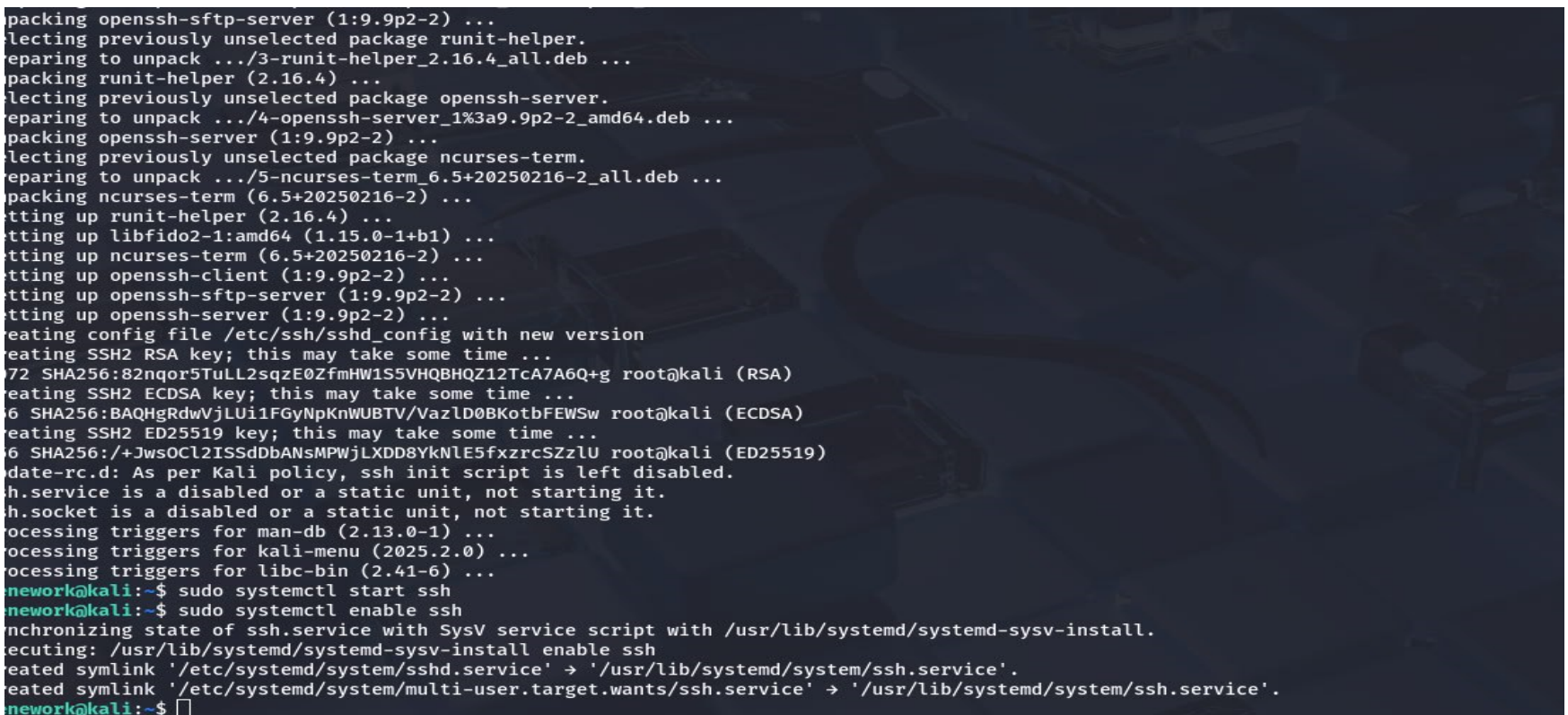
Cont.....



SSH Installation



Cont ....



Cont....

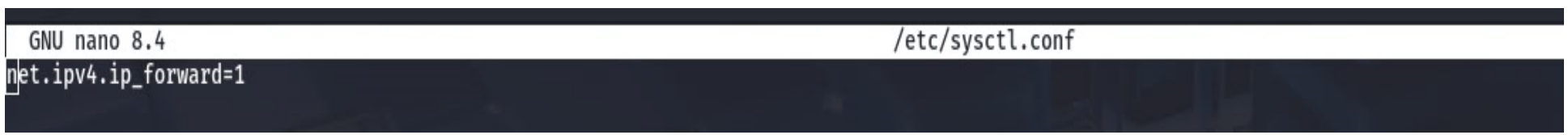
```
nework@kali:~$ sudo systemctl enable ssh
nchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
ecuting: /usr/lib/systemd/systemd-sysv-install enable ssh
eated symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system/ssh.service'.
eated symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.
nework@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
nvocation: 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"

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

configuring Linux box as router

Allow forward packets between two or more networks

Open nano /etc/sysctl.conf

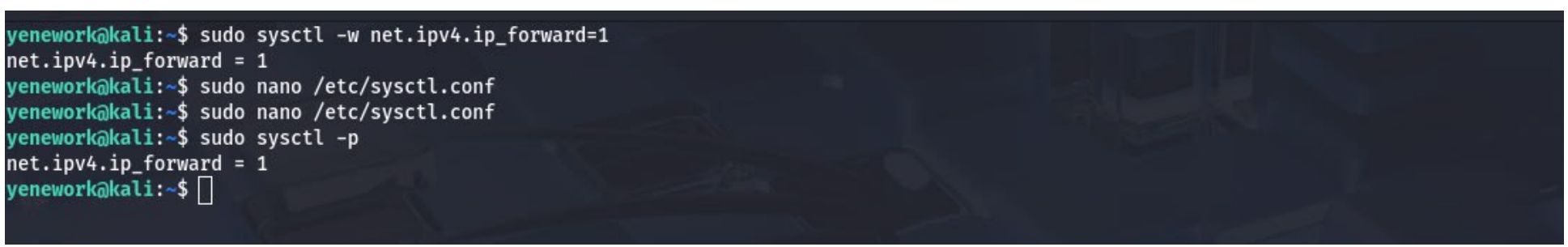
Add this line ctrl+0, enter and ctrl+x



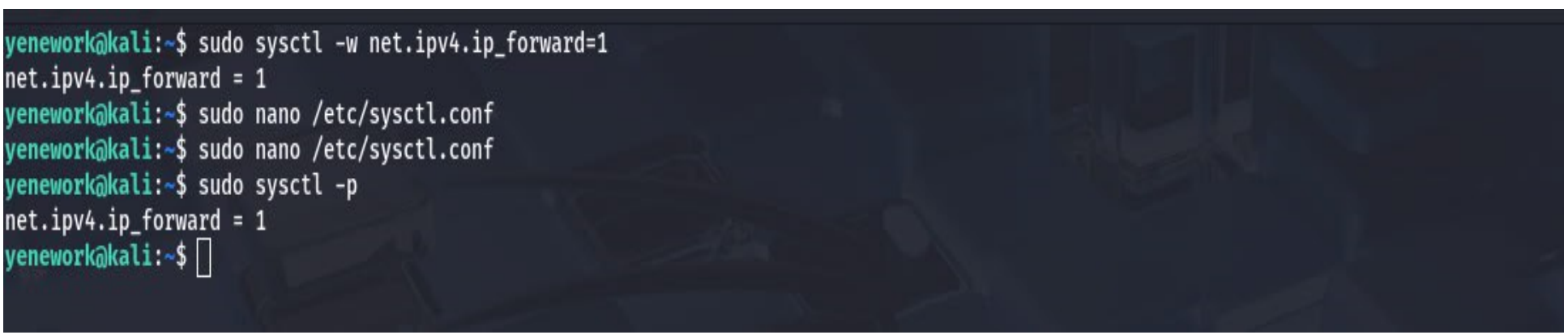
Cont.....

Set up nat as shown below

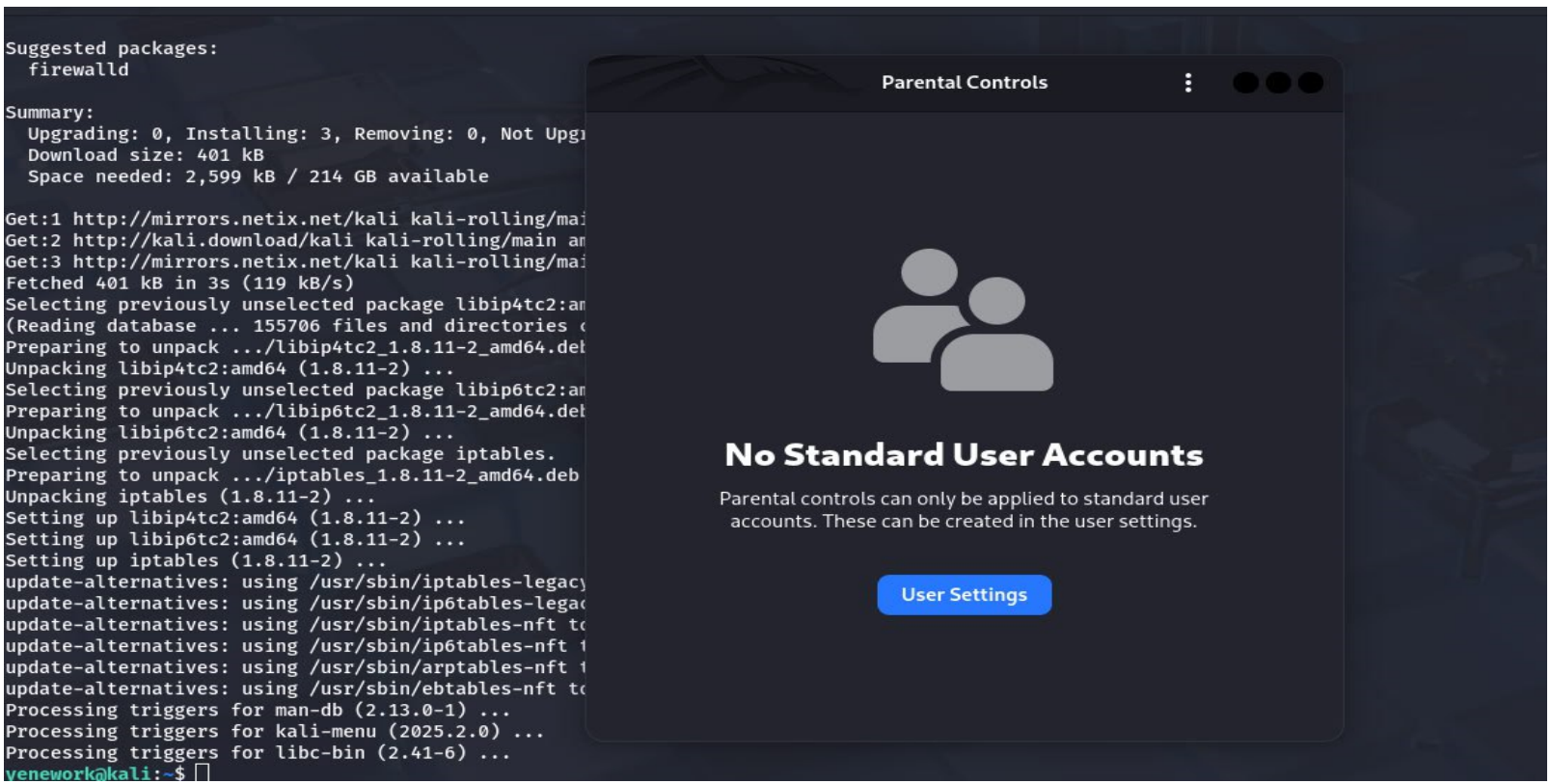
```
yenework@kali:~$ sudo iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
yenework@kali:~$ sudo iptables -A FORWARD -i eth0 -o wlan0 -j ACCEPT
yenework@kali:~$ sudo iptables -A FORWARD -i eth0 -o wlan0 -j ACCEPT
yenework@kali:~$
```



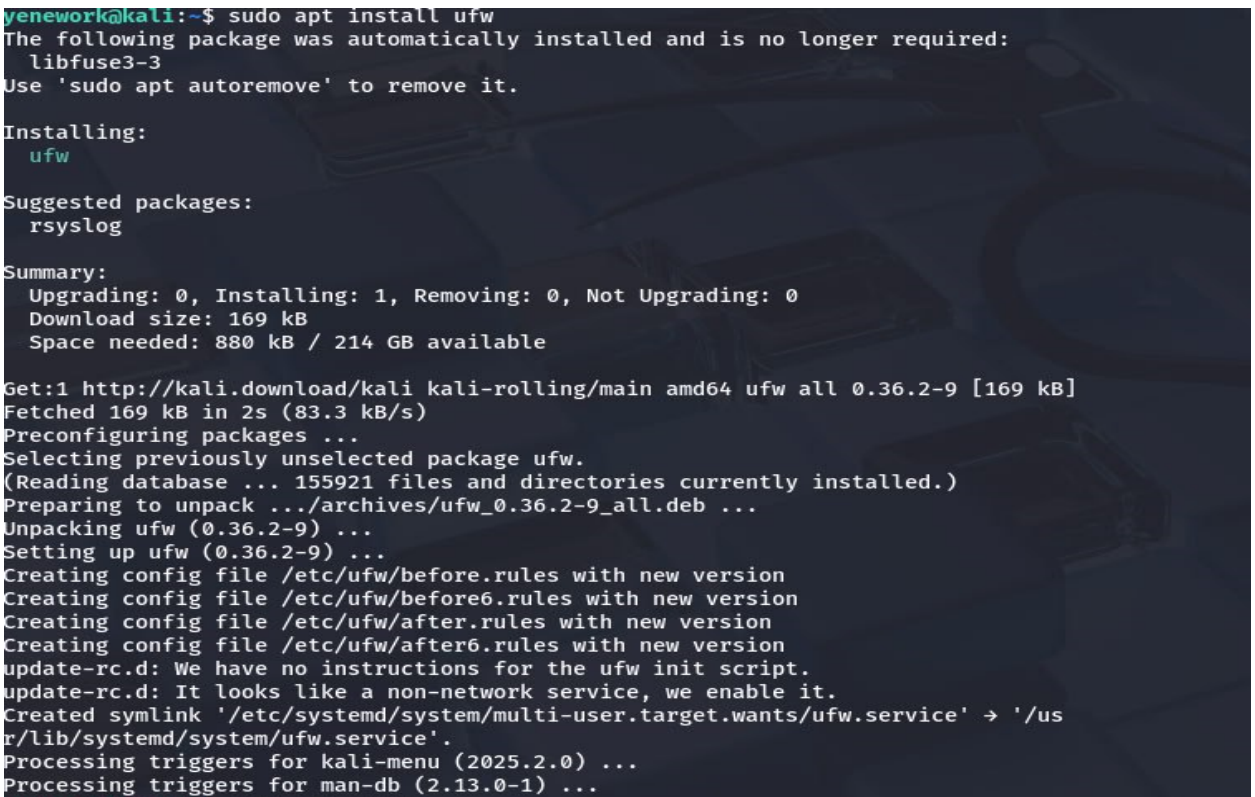
Cont....



Cont....



Configuration of firewalls



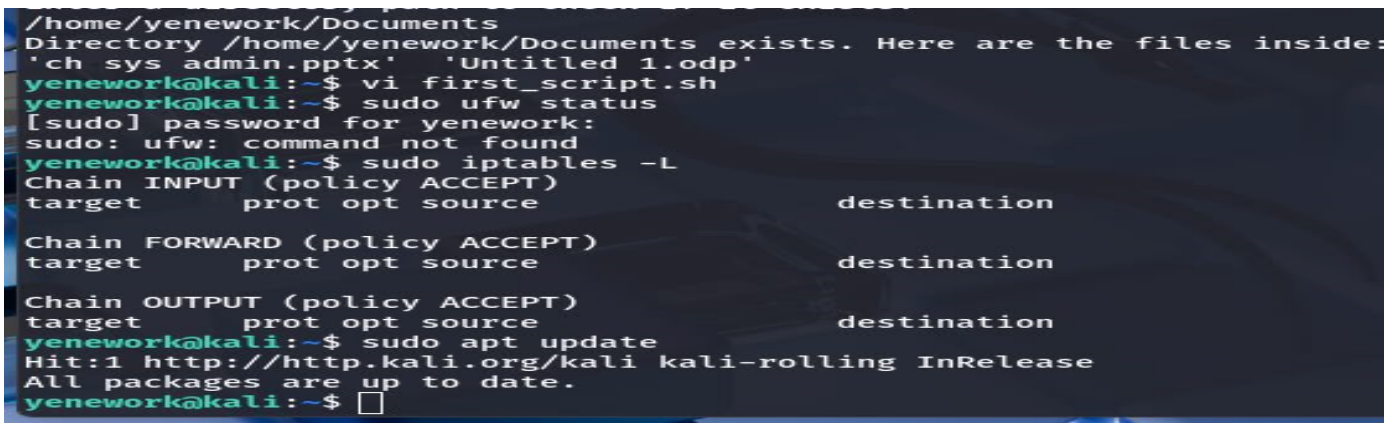
Cont.....

And then allow and deny specific traffic as shown below

iptables

Before making any changes view existing rule

Sudo iptables –L as shown below



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:~$
```

Cont....

Save ip table rules

sudo apt install iptables-persistent

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:~$
```

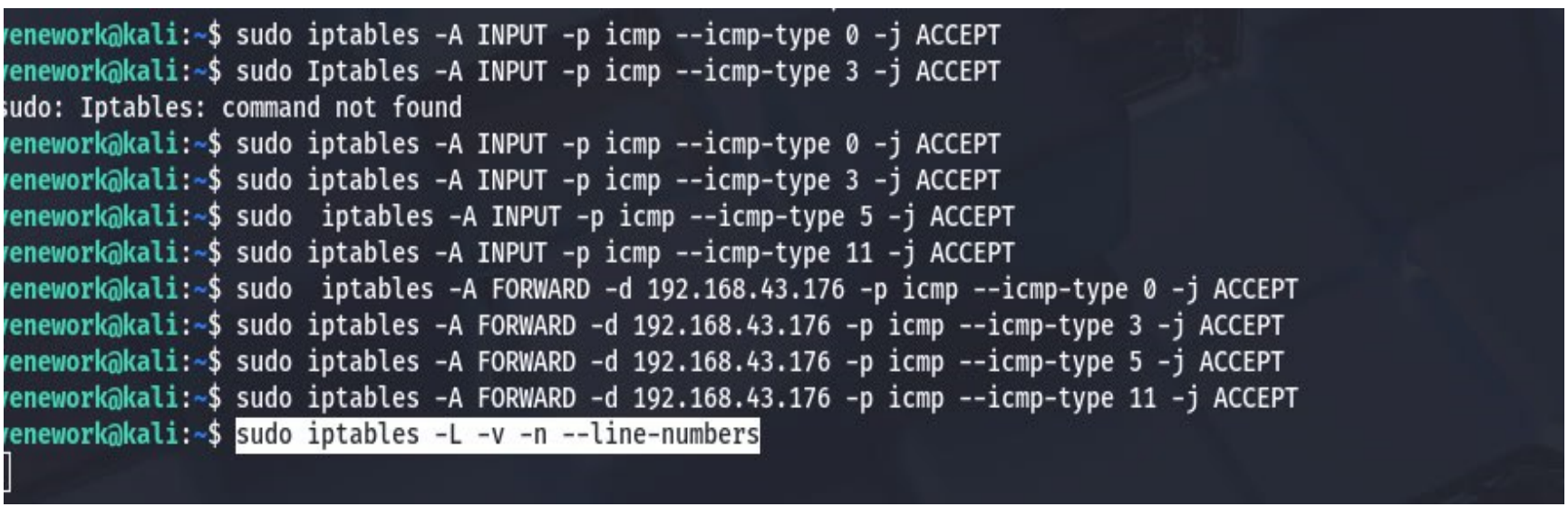
Cont.....

The above result is shown due to override by ufw

The current default policy is still DROP

So you have to make iptables persistent

Cont....



cont.....

If you use Debian based Linux system dont for get save the configuration