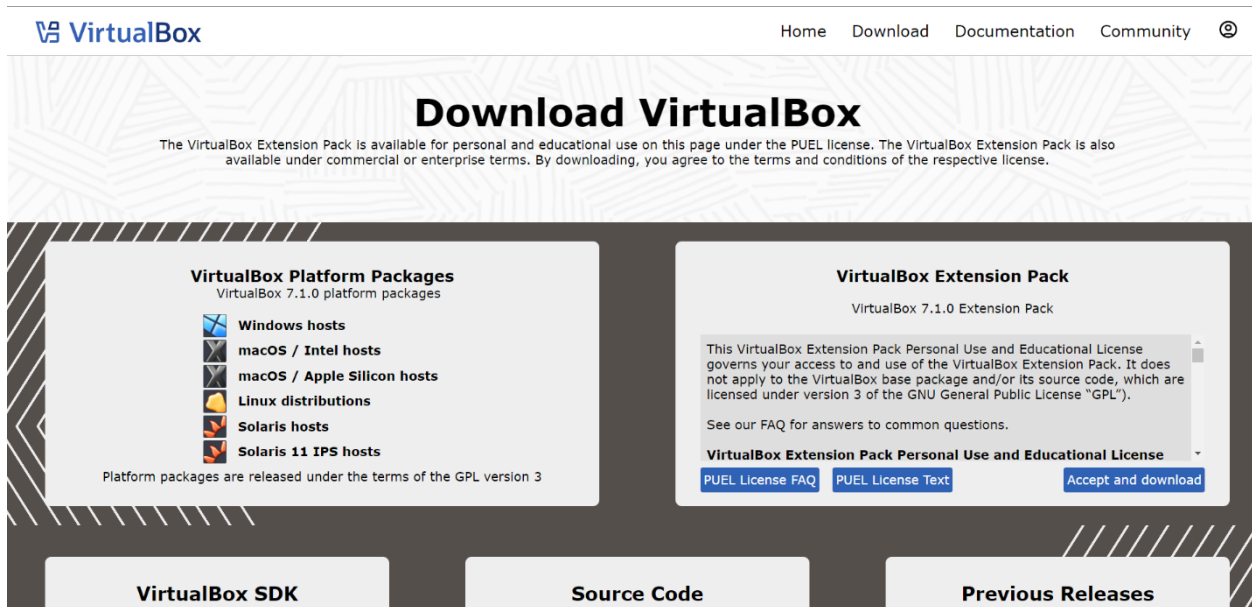


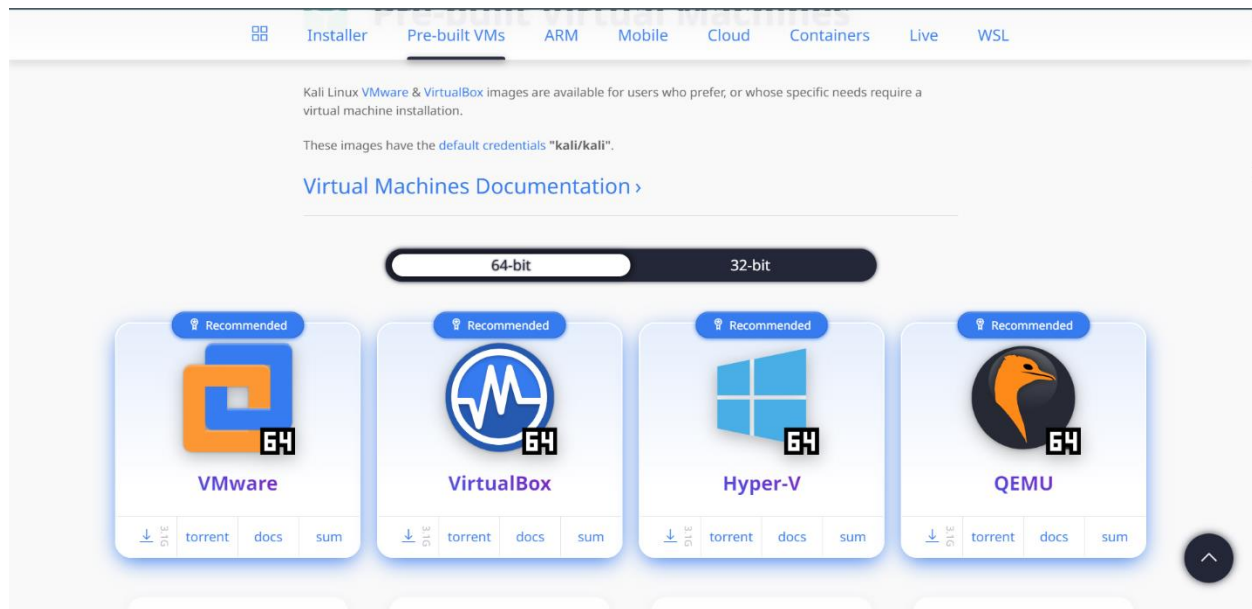
1. Basics of Linux environments.

1.1 Virtual machine setup.

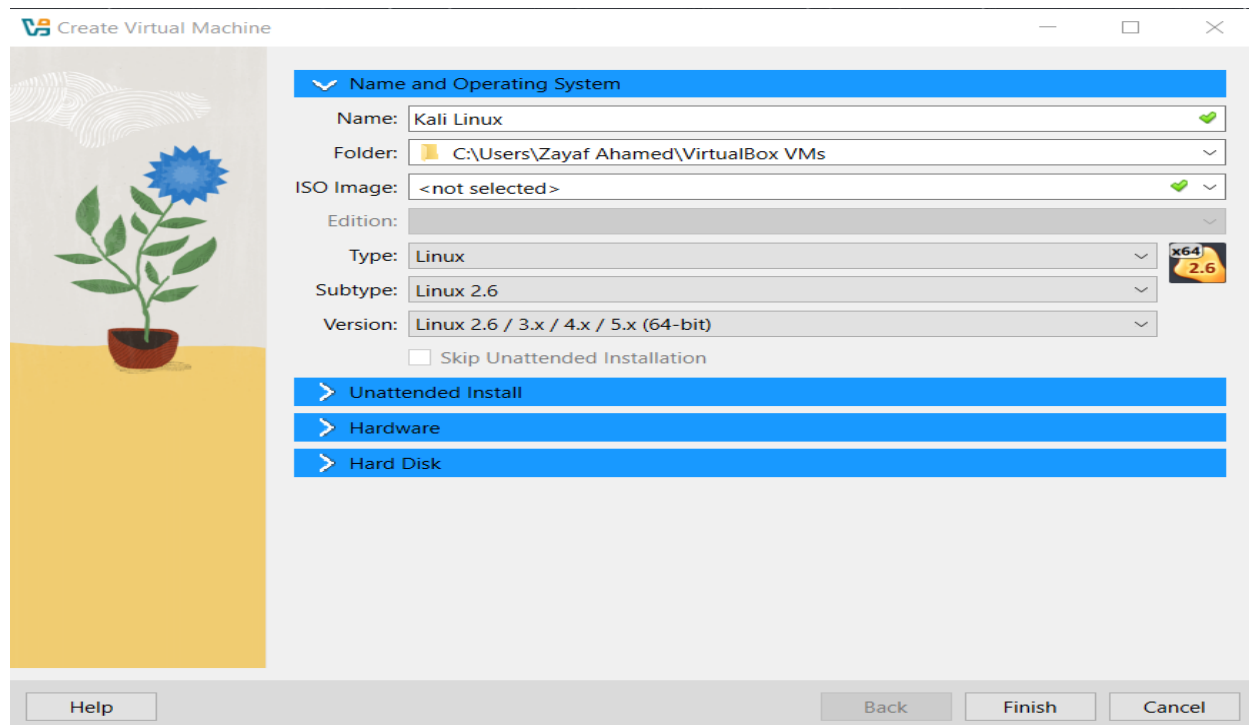
- Installation process of Oracle virtual box.
- Download the windows hosts.



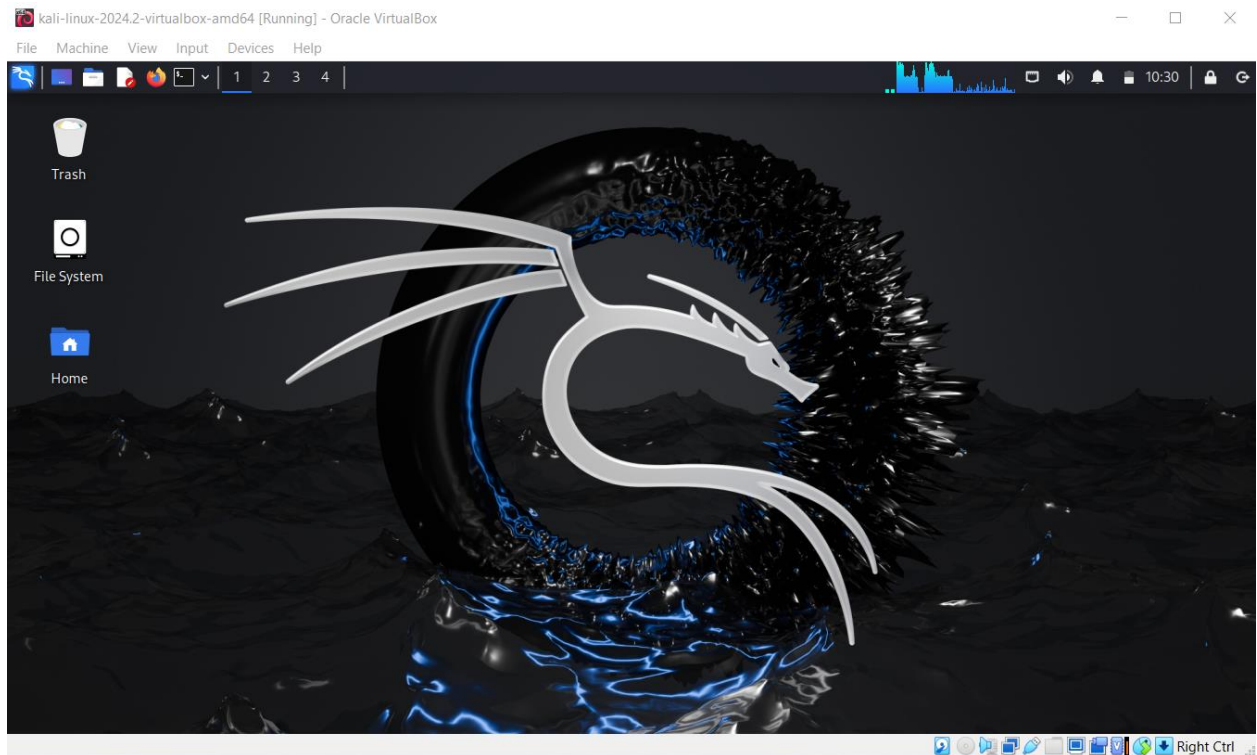
- Downloading an appropriate Linux distribution. I chose Kali.



- Configuring the VM



- Your virtual machine should be up and running.



1.2 Command line introduction.

Basic commands in Linux environments.

- **who:** show who is logged in.

```
(kali㉿kali)-[~]  
$ who  
kali    tty7      2024-09-16 10:30 (:0)
```

- **whoami:** Displays who is currently logged in.

```
(kali㉿kali)-[~]  
$ whoami  
kali
```

- **ls**: List the directories.

```
(kali㉿kali)-[~]  
$ ls  
Desktop Downloads Music Pictures sshkey17.private student userinfo.sh  
Documents IT23400368 natas15.py Public sshkey.private Templates Videos
```

- **ls -l**: Lists files with detailed information (permissions, size, date).

```
(kali㉿kali)-[~]  
$ ls -l  
total 56  
drwxr-xr-x 2 kali kali 4096 Jul 24 06:54 Desktop  
drwxr-xr-x 2 kali kali 4096 Jul 24 06:54 Documents  
drwxr-xr-x 2 kali kali 4096 Jul 24 06:54 Downloads  
drwxr-xr-x 2 kali kali 4096 Jul 28 06:58 IT23400368  
drwxr-xr-x 2 kali kali 4096 Jul 24 06:54 Music  
-rw-rw-r-- 1 kali kali 1054 Aug 21 01:23 natas15.py  
drwxr-xr-x 2 kali kali 4096 Aug 12 03:06 Pictures  
drwxr-xr-x 2 kali kali 4096 Jul 24 06:54 Public  
-rw----- 1 kali kali 1675 Aug 13 12:36 sshkey17.private  
-rwx----- 1 kali kali 1679 Aug 12 03:51 sshkey.private  
drwxrwxr-x 2 kali kali 4096 Jul 29 23:55 student  
drwxr-xr-x 2 kali kali 4096 Jul 24 06:54 Templates  
-rwxrwxr-x 1 kali kali 105 Aug 13 00:10 userinfo.sh  
drwxr-xr-x 2 kali kali 4096 Jul 24 06:54 Videos
```

- **ls -al**: Lists all files, including hidden ones, in detail.

```
(kali@kali)-[~]
$ ls -al
total 236
drwx----- 21 kali kali 4096 Sep 16 10:33 .
drwxr-xr-x  3 root root 4096 May 27 15:18 ..
-rw-r--r--  1 kali kali 220 May 27 15:18 .bash_logout
-rw-r--r--  1 kali kali 5551 May 27 15:18 .bashrc
-rw-r--r--  1 kali kali 3526 May 27 15:18 .bashrc.original
drwx----- 7 kali kali 4096 Aug 15 06:06 .BurpSuite
drwxrwxr-x 10 kali kali 4096 Aug 12 03:02 .cache
drwxr-xr-x 14 kali kali 4096 Aug 12 03:02 .config
drwxr-xr-x  2 kali kali 4096 Jul 24 06:54 Desktop
-rw-r--r--  1 kali kali 35 Jul 24 06:54 .dmrc
drwxr-xr-x  2 kali kali 4096 Jul 24 06:54 Documents
drwxr-xr-x  2 kali kali 4096 Jul 24 06:54 Downloads
-rw-r--r--  1 kali kali 11759 May 27 15:18 .face
lrwxrwxrwx  1 kali kali 5 May 27 15:18 .face.icon -> .face
drwx----- 3 kali kali 4096 Jul 24 06:54 .gnupg
-rw-----  1 kali kali 0 Jul 24 06:54 .ICEauthority
drwxr-xr-x  2 kali kali 4096 Jul 28 06:58 IT23400368
drwxr-xr-x  4 kali kali 4096 Aug 5 23:48 .java
-rw-----  1 kali kali 12288 Aug 21 23:40 .lab.c.swp
drwxr-xr-x  4 kali kali 4096 Jul 24 06:54 .local
drwx----- 4 kali kali 4096 Jul 28 07:37 .mozilla
drwxr-xr-x  2 kali kali 4096 Jul 24 06:54 Music
-rw-rw-r--  1 kali kali 1054 Aug 21 01:23 natas15.py
drwxr-xr-x  2 kali kali 4096 Aug 12 03:06 Pictures
drwx----- 3 kali kali 4096 Aug 6 00:53 .pki
-rw-r--r--  1 kali kali 807 May 27 15:18 .profile
drwxr-xr-x  2 kali kali 4096 Jul 24 06:54 Public
drwx----- 2 kali kali 4096 Jul 29 03:17 .ssh
-rw-----  1 kali kali 1675 Aug 13 12:36 sshkey17.private
-rwx-----  1 kali kali 1679 Aug 12 03:51 sshkey.private
drwxrwxr-x  2 kali kali 4096 Jul 29 23:55 student
-rw-r--r--  1 kali kali 0 Aug 13 11:45 .sudo_as_admin_successful
drwxr-xr-x  2 kali kali 4096 Jul 24 06:54 Templates
-rwxrwxr-x  1 kali kali 105 Aug 13 00:10 userinfo.sh
-rw-r-----  1 kali kali 5 Sep 16 10:30 .vboxclient-clipboard-tty7-control.pid
-rw-r-----  1 kali kali 4 Sep 16 10:30 .vboxclient-clipboard-tty7-service.pid
-rw-r-----  1 kali kali 5 Sep 16 10:30 .vboxclient-display-svga-x11-tty7-control.pid
-rw-r-----  1 kali kali 5 Sep 16 10:30 .vboxclient-display-svga-x11-tty7-service.pid
-rw-r-----  1 kali kali 5 Sep 16 10:30 .vboxclient-draganddrop-tty7-control.pid
-rw-r-----  1 kali kali 4 Sep 16 10:30 .vboxclient-draganddrop-tty7-service.pid
-rw-r-----  1 kali kali 5 Sep 16 10:30 .vboxclient-hostversion-tty7-control.pid
-rw-r-----  1 kali kali 5 Sep 16 10:30 .vboxclient-seamless-tty7-control.pid
-rw-r-----  1 kali kali 4 Sep 16 10:30 .vboxclient-seamless-tty7-service.pid
-rw-r-----  1 kali kali 5 Sep 16 10:30 .vboxclient-vmvga-session-tty7-control.pid
drwxr-xr-x  2 kali kali 4096 Jul 24 06:54 Videos
-rw-----  1 kali kali 1359 Jul 30 00:59 .viminfo
-rw-----  1 kali kali 49 Sep 16 10:30 .Xauthority
-rw-----  1 kali kali 9297 Sep 16 10:31 .xsession-errors
-rw-----  1 kali kali 7498 Aug 21 23:42 .xsession-errors.old
-rw-----  1 kali kali 5485 Aug 21 23:40 .zsh_history
-rw-r--r--  1 kali kali 10868 May 27 15:18 .zshrc
(kali@kali)-[~]
```

- **pwd**: Displays the current working directory path.

```
(kali@kali)-[~]
$ pwd
/home/kali
```

- **mkdir**: Creates a new directory.

```
(kali@kali)-[~]
$ mkdir NEW

(kali@kali)-[~]
$ ls
Desktop  Downloads  Music  NEW  Public  sshkey.private  Templates  Videos
Documents IT23400368 natas15.py Pictures sshkey17.private student userinfo.sh
```

- **rmdir**: removes a specified directory.

```
(kali㉿kali)-[~]
$ rmdir NEW

(kali㉿kali)-[~]
$ ls
Desktop  Downloads  Music  Pictures  sshkey17.private  student  userinfo.sh
Documents IT23400368 natas15.py Public  sshkey.private  Templates  Videos
```

- **cd**: Changes the current directory.

```
(kali㉿kali)-[~]
$ cd Documents

(kali㉿kali)-[~/Documents]
$
```

- **touch**: Creates an empty file.

```
(kali㉿kali)-[~/Documents]
$ touch temp

(kali㉿kali)-[~/Documents]
$ ls
temp
```

- **cp**: Copies files or directories.

```
(kali㉿kali)-[~/Documents]
$ ls
NEW temp

(kali㉿kali)-[~/Documents]
$ cp temp ./NEW

(kali㉿kali)-[~/Documents]
$ cd NEW

(kali㉿kali)-[~/Documents/NEW]
$ ls
temp
```


- **rm**: Removes files.

```
(kali㉿kali)-[~/Documents/NEW]
└─$ ls
temp

(kali㉿kali)-[~/Documents/NEW]
└─$ rm temp

(kali㉿kali)-[~/Documents/NEW]
└─$ ls

(kali㉿kali)-[~/Documents/NEW]
└─$
```

- **cat >**: Creates a new file and writes to it.

```
(kali㉿kali)-[~/Documents/NEW]
└─$ cd ..

(kali㉿kali)-[~/Documents]
└─$ cat > temp
This is a temporary file^C

(kali㉿kali)-[~/Documents]
└─$
```

- **cat**: Displays file content or concatenates files.

```
(kali㉿kali)-[~/Documents]
└─$ cat temp
This is a temporary file
```

- **chmod**: Changes file or directory permissions.

```
(kali㉿kali)-[~/Documents]
└─$ chmod 777 temp

(kali㉿kali)-[~/Documents]
└─$ ls -l
total 8
drwxrwxr-x 2 kali kali 4096 Sep 16 10:51 NEW
-rwxrwxrwx 1 kali kali  25 Sep 16 10:56 temp
```

- Nano and vi editors: built in text editors used to write code.

1.3 System information and user management.

- **uname -a:** Displays detailed system information (kernel, OS, processor, etc.).

```
(kali㉿kali)-[~/Documents]
$ uname -a
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64 GNU/Linux
(kali㉿kali)-[~/Documents]
$
```

- **cat /proc/version:** Shows Linux kernel version and build information.

```
(kali㉿kali)-[~]
$ cat /proc/version
Linux version 6.6.15-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-24) 13.2.0, GNU ld (GNU Binutils f
or Debian) 2.42) #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17)
(kali㉿kali)-[~]
$
```

- **df -h:** Displays disk space usage in a human-readable format.

```
(kali㉿kali)-[~]
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            948M   0    948M   0% /dev
tmpfs           198M  988K   197M   1% /run
/dev/sda1       79G   16G   60G   21% /
tmpfs           989M   0    989M   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           198M  124K   198M   1% /run/user/1000
(kali㉿kali)-[~]
$
```

- **free -m:** Displays memory usage (free, used, total) in megabytes.

```
(kali㉿kali)-[~]
$ free -m
              total        used        free      shared  buff/cache   available
Mem:           1976          798          871         16         463        1178
Swap:          1023           0         1023
(kali㉿kali)-[~]
$
```


- **id**: Displays user and group IDs for the current or specified

```
(kali㉿kali)-[~]  
$ id  
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),106(bluetooth),113(scanner),136(wireshark),137(kaboxer),138(vboxsf)  
  
(kali㉿kali)-[~]  
$
```

passwd: Changes the user password.

```
(kali㉿kali)-[~]  
$ passwd  
Changing password for kali.  
Current password: 
```

- **useradd**: Creates a new user account in the system.

2.DHCP, DNS and NTP Services.

2.1 DHCP (Dynamic Host Configuration Protocol)

Step 1:

- Installing DHCP server.
- **sudo apt install isc-dhcp-server.**

```
(kali@kali)~$ sudo apt install isc-dhcp-server
Installing:
isc-dhcp-server

Installing dependencies:
policycoreutils selinux-utils

Suggested packages:
isc-dhcp-server-ldap

Summary:
Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 993
Download size: 1,750 kB
Space needed: 7,845 kB / 63.5 GB available

Continue? [Y/n] y
Get:1 http://mirror.primelink.net.id/kali kali-rolling/main amd64 isc-dhcp-server amd64 4.4.3-P1-5 [1,479 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 selinux-utils amd64 3.5-2+b2 [127 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 policycoreutils amd64 3.5-2.1 [143 kB]
Fetched 1,750 kB in 7s (252 kB/s)
Preconfiguring packages ...
Selecting previously unselected package isc-dhcp-server.
(Reading database ... 391111 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-server_4.4.3-P1-5_amd64.deb ...
Unpacking isc-dhcp-server (4.4.3-P1-5) ...
Selecting previously unselected package selinux-utils.
Preparing to unpack .../selinux-utils_3.5-2+b2_amd64.deb ...
Unpacking selinux-utils (3.5-2+b2) ...
Selecting previously unselected package policycoreutils.
Preparing to unpack .../policycoreutils_3.5-2.1_amd64.deb ...
Unpacking policycoreutils (3.5-2.1) ...
Setting up selinux-utils (3.5-2+b2) ...
Setting up policycoreutils (3.5-2.1) ...
update-rc.d: We have no instructions for the selinux-autorelabel init script.
update-rc.d: It looks like a non-network service, we enable it.
Setting up isc-dhcp-server (4.4.3-P1-5) ...
Generating /etc/default/isc-dhcp-server ...
update-rc.d: We have no instructions for the isc-dhcp-server init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for man-db (2.12.1-1) ...
```

Step 2:

Configure the DHCP server.

sudo nano /etc/dhcp/dhcpd.conf this command will open the configuration file.

Edit the configuration according to our network infrastructure.

```
subnet 10.0.2.0 netmask 255.255.255.0 {
    range 10.0.2.20 10.0.2.50;
    option routers 10.0.2.1;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    option domain-name "local";
}
```

After the modification save and exit from the dhcpd.conf file.

Step 3:

Configure the network interface.

sudo nano /etc/default/isc-dhcp-server. Set INTERFACESv4 to eth0

```
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth0"
INTERFACESv6=""
```

Step 4:

After making these changes, restart the DHCP server to apply the new changes.

This code helps to do that: **sudo systemctl restart isc-dhcp-server.**

With these settings, my DHCP server will provide IP addresses in the range 10.0.2.20 to 10.0.2.50, with the default gateway set to 10.0.2.1 and the DNS server set to 8.8.8.8.

2.2 DNS (Domain Name System)

Step 1:

Install BIND.

we can use:- **sudo apt update.**

sudo apt install bind9.

```
(kali@kali):~$ sudo apt install bind9
$ sudo apt install bind9
Upgrading:
  bind9-dnswriter bind9-host bind9-libs
Installing:
  bind9
Installing dependencies:
  bind9-utils
Suggested packages:
  bind-doc resolvconf ufw
Summary:
  Upgrading: 3, Installing: 2, Removing: 0, Not Upgrading: 990
  Download size: 2,211 kB
  Space needed: 2,334 kB / 63.5 GB available
Continue? [y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 bind9-libs amd64 1:9.20.1-1 [1,480 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 bind9-host amd64 1:9.20.1-1 [325 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 bind9-dnswriter amd64 1:9.20.1-1 [435 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 bind9-utils amd64 1:9.20.1-1 [452 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 bind9 amd64 1:9.20.1-1 [519 kB]
Fetched 3,211 kB in 10s (176 kB/s)
(Reading database ... 391422 files and directories currently installed.)
Preparing to unpack .../bind9-host_1:9.20.1-1_amd64.deb ...
Unpacking bind9-host (1:9.20.1-1) over (1:9.19.21-1+b1) ...
Preparing to unpack .../bind9-dnswriter_1:9.20.1-1_amd64.deb ...
Unpacking bind9-dnswriter (1:9.20.1-1) over (1:9.19.21-1+b1) ...
Preparing to unpack .../bind9-libs_1:9.20.1-1_amd64.deb ...
Unpacking bind9-libs (1:9.20.1-1) over (1:9.19.21-1+b1) ...
Selecting previously unselected package bind9-utils.
Preparing to unpack .../bind9-utils_1:9.20.1-1_amd64.deb ...
Unpacking bind9-utils (1:9.20.1-1) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1:9.20.1-1_amd64.deb ...
Unpacking bind9 (1:9.20.1-1) ...
Setting up bind9-libs (1:9.20.1-1) ...
Setting up bind9-host (1:9.20.1-1) ...
Setting up bind9 (1:9.20.1-1) ...
info: Selecting GID from range 100 to 999 ...
info: Adding group 'bind' (GID 133) ...
info: Selecting UID from range 100 to 999 ...
info: Adding system user 'bind' (UID 133) ...
info: Adding new user 'bind' (UID 133) with group 'bind' ...
info: Not creating home directory '/var/cache/bind'.
wrote key file '/etc/bind/rndc.key'
update-rc.d: We have no instructions for the named init script.
update-rc.d: It looks like a network service, we disable it.
named-resolvconf.service is a disabled or a static unit, not starting it.
named.service is a disabled or a static unit, not starting it.
Setting up bind9-host (1:9.20.1-1) ...
Setting up bind9-dnswriter (1:9.20.1-1) ...
Processing triggers for libc-bin (2.30-10) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for kali-menu (2023.4.7) ...
```

Step 2:

After the installation. We must configure BIND to use our local DNS server or a public DNS server like Google DNS (8.8.8.8).

Add google DNS server as a forwarder using this command.

sudo nano /etc/bind/named.conf.options.

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
}
```

Step 3:

After saving changes, Restart BIND to apply them.

we can use **sudo systemctl restart named**.

Step 4:

Ensure BIND is running without issues.

we can use **sudo systemctl status named**.

```
(kali㉿kali)-[~]
└─$ sudo systemctl status named
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; preset: disabled)
   Active: active (running) since Tue 2024-09-17 02:00:37 EDT; 17s ago
     Docs: man:named(8)
    Main PID: 9381 (named)
      Status: "running"
    Tasks: 8 (limit: 2272)
   Memory: 25.1M (peak: 25.4M)
      CPU: 113ms
    CGroup: /system.slice/named.service
            └─9381 /usr/sbin/named -f -u bind

Sep 17 02:00:41 kali named[9381]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Sep 17 02:00:41 kali named[9381]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Sep 17 02:00:42 kali named[9381]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Sep 17 02:00:42 kali named[9381]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Sep 17 02:00:43 kali named[9381]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Sep 17 02:00:43 kali named[9381]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Sep 17 02:00:44 kali named[9381]: checkhints: b.root-servers.net/A (170.247.170.2) missing from hints
Sep 17 02:00:44 kali named[9381]: checkhints: b.root-servers.net/A (199.9.14.201) extra record in hints
Sep 17 02:00:44 kali named[9381]: checkhints: b.root-servers.net/AAAA (2801:1b8:10::b) missing from hints
Sep 17 02:00:44 kali named[9381]: checkhints: b.root-servers.net/AAAA (2001:500:200::b) extra record in hints
```

2.3 NTP(Network Time Protocol)

Step 1:

Install the NTP server.

we can use **sudo apt install ntp**.

```
(kali㉿kali)-[~]
$ sudo apt install ntp
[sudo] password for kali:
Installing:
ntp
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 990
Download size: 23.4 kB
Space needed: 69.6 kB / 63.5 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 ntp all 1:4.2.8p15+dfsg-2~1.2.3+dfsg1-3 [23.4 kB]
Fetched 23.4 kB in 7s (3,570 B/s)
Selecting previously unselected package ntp.
(Reading database ... 391507 files and directories currently installed.)
Preparing to unpack .../ntp_1%3a4.2.8p15+dfsg-2~1.2.3+dfsg1-3_all.deb ...
Unpacking ntp (1:4.2.8p15+dfsg-2~1.2.3+dfsg1-3) ...
Setting up ntp (1:4.2.8p15+dfsg-2~1.2.3+dfsg1-3) ...
```

Step 2:

Configure the NTP client.

Ensure the following lines are present to use public NTP servers.

We can use: **sudo nano /etc/ntpsec/ntp.conf**.

```
# pool.ntp.org maps to about 1000 low-stratum NTP servers. Your server will
# pick a different set every time it starts up. Please consider joining the
# pool: <https://www.pool.ntp.org/join.html>
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst
server pool.ntp.org
# Access control configuration; see /usr/share/doc/ntpsec-doc/html/acconfig.html
# for details.
```

Step 3:

After saving changes, Restart NTP to apply them.

we can use: **sudo systemctl restart ntpsec**.

Step 4:

Finally, verify if the time synchronizes.

we can use: **ntpq -p**.

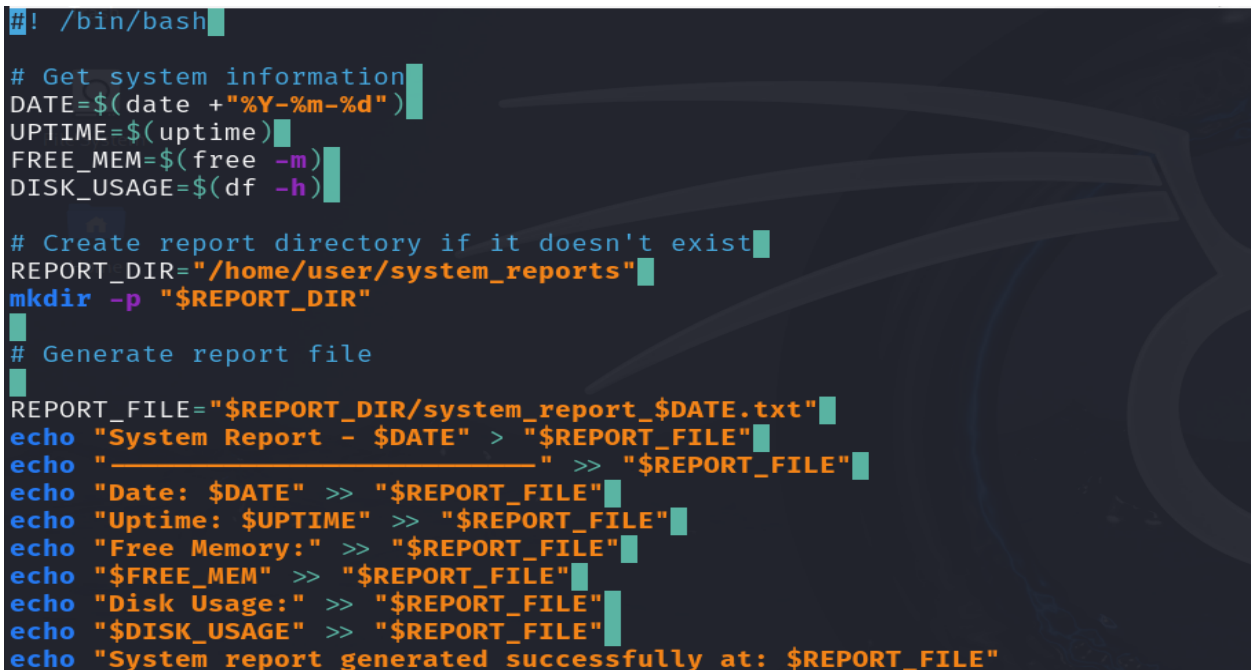
```
(kali㉿kali)-[~]  
$ ntpq -p  
remote                                refid      st t when poll reach  delay  offset  jitter  
-----  
0.debian.pool.ntp.org                 .POOL.     16 p    - 256    0  0.0000  0.0000  0.0002  
1.debian.pool.ntp.org                 .POOL.     16 p    - 256    0  0.0000  0.0000  0.0002  
2.debian.pool.ntp.org                 .POOL.     16 p    - 256    0  0.0000  0.0000  0.0002  
3.debian.pool.ntp.org                 .POOL.     16 p    - 256    0  0.0000  0.0000  0.0002  
pool.ntp.org                          .DNS.      16 u    - 512    0  0.0000  0.0000  0.0002  
+time.cloudflare.com                 10.4.8.56   3 u   54  64    1 248.6036 152.7780 85.3316  
+time.cloudflare.com                 10.4.8.56   3 u   55  64    1 248.5716 151.3735 86.6611  
time.cloudflare.com                  .INIT.      16 u    - 64     0  0.0000  0.0000  0.0002  
time.cloudflare.com                  .INIT.      16 u    - 64     0  0.0000  0.0000  0.0002
```

3. Shell Scripting and Security.

3.1 Shell Scripting

3.1.1 Script 1- automating a report that captures key system details every day.

```
#!/bin/bash
# Get system information
DATE=$(date +"%Y-%m-%d")
UPTIME=$(uptime)
FREE_MEM=$(free -m)
DISK_USAGE=$(df -h)
# Create report directory if it doesn't exist
REPORT_DIR="/home/user/system_reports"
mkdir -p "$REPORT_DIR"
# Generate report file
REPORT_FILE="$REPORT_DIR/system_report_$DATE.txt"
echo "System Report - $DATE" > "$REPORT_FILE"
echo "-----" >> "$REPORT_FILE"
echo "Date: $DATE" >> "$REPORT_FILE"
echo "Uptime: $UPTIME" >> "$REPORT_FILE"
echo "Free Memory:" >> "$REPORT_FILE"
echo "$FREE_MEM" >> "$REPORT_FILE"
echo "Disk Usage:" >> "$REPORT_FILE"
echo "$DISK_USAGE" >> "$REPORT_FILE"
echo "System report generated successfully at: $REPORT_FILE"
```

A screenshot of a terminal window with a dark background and light blue/green text. The terminal shows the execution of the shell script from the previous block. The output of the script is visible, showing the system report being generated and the final message: "System report generated successfully at: \$REPORT_FILE".

```
#!/bin/bash
# Get system information
DATE=$(date +"%Y-%m-%d")
UPTIME=$(uptime)
FREE_MEM=$(free -m)
DISK_USAGE=$(df -h)
# Create report directory if it doesn't exist
REPORT_DIR="/home/user/system_reports"
mkdir -p "$REPORT_DIR"
# Generate report file
REPORT_FILE="$REPORT_DIR/system_report_$DATE.txt"
echo "System Report - $DATE" > "$REPORT_FILE"
echo "-----" >> "$REPORT_FILE"
echo "Date: $DATE" >> "$REPORT_FILE"
echo "Uptime: $UPTIME" >> "$REPORT_FILE"
echo "Free Memory:" >> "$REPORT_FILE"
echo "$FREE_MEM" >> "$REPORT_FILE"
echo "Disk Usage:" >> "$REPORT_FILE"
echo "$DISK_USAGE" >> "$REPORT_FILE"
echo "System report generated successfully at: $REPORT_FILE"
```

3.1.2 Script 2 -automating the backup of a critical directory (/home/user/documents) containing important files.

#!/bin/bash

set source and destination directories

SOURCE_DIR="/home/user/documents"

BACKUP_DIR="/home/user/backup/documents"

Create the backup directory if it doesn't exist

mkdir -p "\$BACKUP_DIR"

Backup files with date timestamp

DATE=\$(date +"%Y-%m-%d")

BACKUP_FILE="\$BACKUP_DIR/documents_backup_\$DATE.tar.gz"

Archive and compress files

tar -czf "\$BACKUP_FILE" "\$SOURCE_DIR"

Notify user of completion

echo "Backup completed. File saved as \$BACKUP_FILE"

```
#!/bin/bash
# set source and destination directories
SOURCE_DIR="/home/user/documents"
BACKUP_DIR="/home/user/backup/documents"

# Create the backup directory if it doesn't exist
mkdir -p "$BACKUP_DIR"

# Backup files with date timestamp
DATE=$(date +"%Y-%m-%d")
BACKUP_FILE="$BACKUP_DIR/documents_backup_$DATE.tar.gz"

# Archive and compress files
tar -czf "$BACKUP_FILE" "$SOURCE_DIR"

# Notify user of completion
echo "Backup completed. File saved as $BACKUP_FILE"
```

Make the script executable using **chmod**.

```
(kali㉿kali)-[~]  
$ chmod +x system_reports.sh  
  
(kali㉿kali)-[~]  
$ chmod +x backup_script.sh
```

These scripts will automate the tasks of capturing system details and generating reports, as well as backing up a critical directory, making the system administration tasks more efficient.

3.2 SSH (Secure Shell)

Installing SSH server.

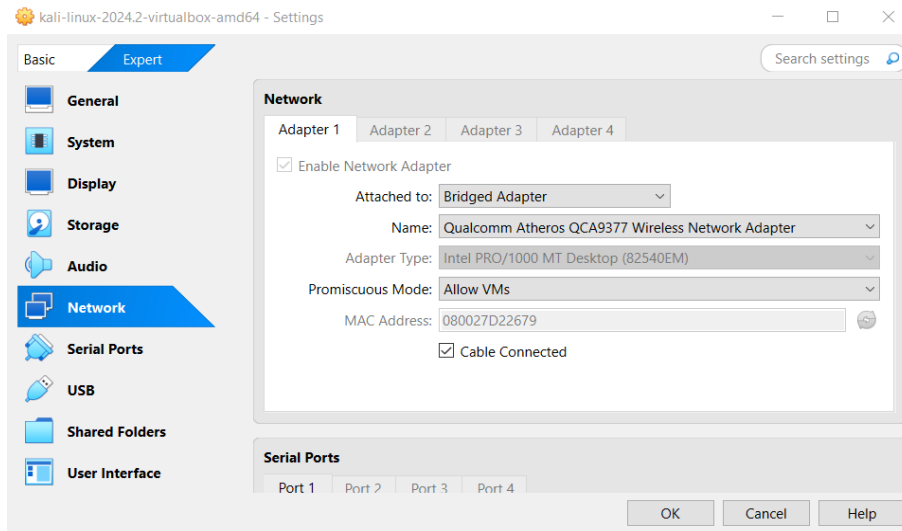
using **sudo apt install openssh-server**.

```
(kali㉿kali)-[~]  
$ sudo apt install openssh-server  
[sudo] password for kali:  
Upgrading:  
  openssh-client openssh-server openssh-sftp-server  
  
Summary:  
  Upgrading: 3, Installing: 0, Removing: 0, Not Upgrading: 987  
  Download size: 1,488 kB  
  Space needed: 1,024 B / 63.5 GB available  
  
Continue? [Y/n] y  
Get:1 http://kali.download/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:9.7p1-7 [65.1 kB]  
Get:2 http://mirror.aktkn.sg/kali kali-rolling/main amd64 openssh-server amd64 1:9.7p1-7 [458 kB]  
Get:3 http://kali.download/kali kali-rolling/main amd64 openssh-client amd64 1:9.7p1-7 [964 kB]  
Fetched 1,488 kB in 8s (190 kB/s)  
Preconfiguring packages ...  
(Reading database ... 391512 files and directories currently installed.)  
Preparing to unpack .../openssh-sftp-server_1%3a9.7p1-7_amd64.deb ...  
Unpacking openssh-sftp-server (1:9.7p1-7) over (1:9.7p1-5) ...  
Preparing to unpack .../openssh-server_1%3a9.7p1-7_amd64.deb ...  
Unpacking openssh-server (1:9.7p1-7) over (1:9.7p1-5) ...  
Preparing to unpack .../openssh-client_1%3a9.7p1-7_amd64.deb ...  
Unpacking openssh-client (1:9.7p1-7) over (1:9.7p1-5) ...  
Setting up openssh-client (1:9.7p1-7) ...  
Setting up openssh-sftp-server (1:9.7p1-7) ...  
Setting up openssh-server (1:9.7p1-7) ...  
Installing new version of config file /etc/pam.d/sshd ...  
ssh.service is a disabled or a static unit not running, not starting it.  
ssh.socket is a disabled or a static unit not running, not starting it.  
Processing triggers for kali-menu (2023.4.7) ...  
Processing triggers for man-db (2.12.1-1) ...
```

After installing we should start the SSH service. By default, the SSH server will listen for connections on **port 22**.

Connecting to my virtual machine remotely.

- Make sure our network adapter is attached to bridge adapter.



- Start the ssh server using **sudo systemctl start ssh**.
- To allow SSH traffic through the firewall (if we're using **ufw**).
We can use **sudo ufw allow ssh**.

```
(kali㉿kali)-[~]  
$ sudo ufw allow ssh  
sudo ufw enable  
Rules updated  
Rules updated (v6)  
Firewall is active and enabled on system startup
```

- Find the virtual machines ip address using the **ip a** command in the kali linux terminal.

```
(kali㉿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 08:00:27:d2:26:79 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0  
        valid_lft 80788sec preferred_lft 80788sec  
    inet 192.168.213.160/24 brd 192.168.213.255 scope global dynamic eth0  
        valid_lft 3593sec preferred_lft 3593sec  
    inet6 fd00::2062:370c:c3a8:2770/64 scope global dynamic noprefixroute  
        valid_lft 85138sec preferred_lft 13138sec  
    inet6 fe80::fe81:2669:b8b5:db7a/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

- In the terminal of the remote computer, we can connect using **ssh user@Ip_Address**.
- Replace **user** with our **Linux username** and **IP_Address** with the **IP address of our Linux machine**.
- In this case it is **ssh [kali@192.168.213.160](#)**.

```
C:\Users\Zayaf Ahamed>ssh kali@192.168.213.160
The authenticity of host '192.168.213.160 (192.168.213.160)' can't be established.
ECDSA key fingerprint is SHA256:ND4t1i4NrMPMzQf0ZSQTwDObRens/Nm/MDQ1H4c6UMw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.213.160' (ECDSA) to the list of known hosts.
kali@192.168.213.160's password: 
Linux kali 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
zsh: corrupt history file /home/kali/.zsh_history
❯(kali@ kali)-[~]
❯$ whoami
kali
❯(kali@ kali)-[~]
❯$
```

- Successfully connected.

3.3 iptables and ACLs

- we don't need to install iptables on Kali Linux because it comes pre-installed.
- Viewing the default iptables rules.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo iptables -L -v
[sudo] password for kali:
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

(kali㉿kali)-[~]
$
```

3.3.1 Web server security

Allow incoming traffic on port 80 (HTTP) and port 443 (HTTPS) and block all other incoming traffic.

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

```
sudo iptables -P INPUT DROP
```

```
(kali㉿kali)-[~]
$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
sudo iptables -P INPUT DROP
```

check if the rules were defined

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
    0    0 ACCEPT    tcp  --  any    any    anywhere                anywhere            tcp dpt:http
    0    0 ACCEPT    tcp  --  any    any    anywhere                anywhere            tcp dpt:https

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
```

This command helps to save and automatically restore iptables rules across reboots.

```
sudo apt install iptables-persistent
```

```
sudo netfilter-persistent save
```

3.3.2 Remote administration access

Allow SSH access from specific IP addresses:

include the trusted IP address.

sudo iptables -A INPUT -p tcp -s 192.168.213.64 --dport 22 -j ACCEPT

```
(kali㉿kali)-[~]  
$ sudo iptables -A INPUT -p tcp -s 192.168.213.64 --dport 22 -j ACCEPT  
[sudo] password for kali:
```

Block SSH from other sources.

sudo iptables -A INPUT -p tcp --dport 22 -j DROP.

```
(kali㉿kali)-[~]  
$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

3.3.3 Allow specific applications

Allow traffic for specific applications based on known port numbers.

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

```
(kali㉿kali)-[~]  
$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

3.3.4 Allow pings (ICMP echo requests)

create a rule using iptables to permit ICMP traffic.

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT.

```
(kali㉿kali)-[~]  
$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

3.3.5 printer server access

Allow printing traffic (port 9100) only from specific IP addresses on your local network, blocking all external access.

sudo iptables -A INPUT -p tcp -s 10.0.2.0/24 --dport 9100 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 9100 -j DROP

```
(kali㉿kali)-[~]  
$ sudo iptables -A INPUT -p tcp -s 10.0.2.0/24 --dport 9100 -j ACCEPT  
sudo iptables -A INPUT -p tcp --dport 9100 -j DROP
```

4. Best Practices

4.1 Disable root login over SSH

Allowing root login over SSH is risky because it gives full control of the system to anyone who accesses it. Disabling root login adds an extra layer of protection to keep our system more secure.

implementation:

step 1: Open the SSH configuration file.

sudo nano /etc/ssh/sshd_config

step2: disable root login

PermitRootLogin no

```
#LoginGraceTime 2m  
PermitRootLogin no  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10
```

step3: Restart the SSH service to apply the changes

sudo systemctl restart sshd

```
(kali㉿kali)-[~]  
$ sudo systemctl restart sshd
```

4.2 Regularly update and patch network-related software.

Keeping our network software up-to-date helps fix security issues and lowers the chances of our system being attacked.

Implementation:

step1: Regularly check for updates and apply them.

sudo apt update.

```
(kali㉿kali)-[~]  
$ sudo apt update  
[sudo] password for kali:  
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.1 MB]  
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [49.1 MB]  
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [110 kB]  
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [268 kB]  
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]  
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [875 kB]  
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]  
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [22.8 kB]  
Fetched 70.8 MB in 2min 43s (434 kB/s)  
1307 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

4.3 Use strong password.

- if we are planning Linux server security, one key practice is to set a powerful password.

Step 1: changing the password.

sudo passwd

Type the current password and after enter the new password.

```
(kali㉿kali)-[~]  
$ sudo passwd  
[sudo] password for kali:  
New password:  
Retype new password:  
passwd: password updated successfully
```

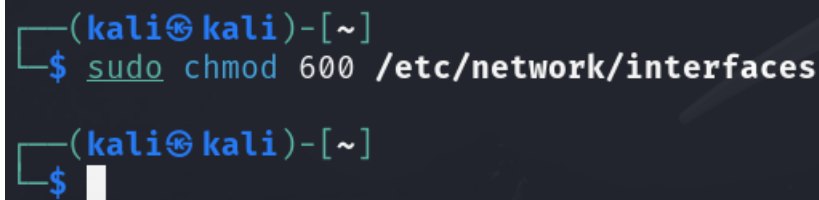
- Create passwords with at least ten characters, including special characters and a combination of uppercase and lowercase letters.
- It makes brute force attack impractical.

4.4 Restrict Access to Configuration Files.

- This is because network configuration files store valuable information, such as IP addresses, routing rules, and DNS settings. Improper access or editing may lead to network downtime or security breaches.

Step 1: Limit file permission.

Set permissions such that only the root user has access and can modify these files. This will prevent normal users or even harmful programs from making changes in the configurations.



```
(kali㉿kali)-[~]  
$ sudo chmod 600 /etc/network/interfaces  
  
(kali㉿kali)-[~]  
$
```

We are following one of the fundamental best practices in security-known as the **principle of least privilege-in** implementing restriction to configuration files.

4.5 Enable Logging and Monitoring.

Logging and monitoring of network interface configurations, when enabled, will help in the detection of unauthorized changes.

Step 1: Install rsyslog server.

```
(kali㉿kali)-[~]
└─$ sudo apt install rsyslog
The following packages were automatically installed and are no longer required:
 fonts-liberation2 libboost-thread1.83.0 libgfrpc0 libjsoncpp25 libpostproc57 libu2f-udev python3-mistune0
 ibverbs-providers libcephfs2 libgfxdr0 libndctl6 librados2 libusbmuxd6 python3-pendulum
 libassuan0 libdaxctl1 libglusterfs0 libplacebo338 librdmacm1t64 openjdk-17-jre python3-pytzdata
 libavfilter9 libgeos3.12.1t64 libibverbs1 libplist3 libre2-10 openjdk-17-jre-headless rwho
 libboost-iostreams1.83.0 libgfat0 libimobiledevice6 libpmem1 libroc0.3 python3-diskcache rwhod
Use 'sudo apt autoremove' to remove them.

Installing:
 rsyslog

Installing dependencies:
 libestr0 libfastjson4 liblognorm5

Suggested packages:
 rsyslog-mysql | rsyslog-pgsql rsyslog-mongodb rsyslog-doc rsyslog-openssl | rsyslog-gnutls rsyslog-gssapi rsyslog-relp

Summary:
 Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 187
 Download size: 848 kB
 Space needed: 2,317 kB / 62.1 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libestr0 amd64 0.1.11-1+b1 [9,236 B]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 liblognorm5 amd64 2.0.6-4+b1 [65.8 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libfastjson4 amd64 1.2304.0-1+b1 [29.0 kB]
Get:4 http://xsrv.moratelindo.io/kali kali-rolling/main amd64 rsyslog amd64 8.2406.0-1 [744 kB]
Fetched 848 kB in 13s (65.1 kB/s)
```

Step 2:

- Configure the server by adding the information about the file we want to monitor.
- I chose **/etc/network/interfaces**.

```
module(load="imfile")
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")
input(type="imfile"
       File="/etc/network/interfaces"
       Tag="net-config-change"
       Severity="warning")
```

Step 3:

- After the configuration we should restart the service.
Using **sudo systemctl restart rsyslog**.

Now the service should be running without errors.

```
—(kali@kali)-[~]
└─$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-10-01 11:31:54 EDT; 4s ago
     Invocation: e18a5117ea3a42b3849421e7ad50eec0
   TriggeredBy: ● syslog.socket
      Docs: man:rsyslogd(8)
            man:rsyslog.conf(5)
            https://www.rsyslog.com/doc/
    Main PID: 38959 (rsyslogd)
       Tasks: 5 (limit: 2221)
      Memory: 1.2M (peak: 2.2M)
         CPU: 93ms
    CGroup: /system.slice/rsyslog.service
            └─38959 /usr/sbin/rsyslogd -n -iNONE

Oct 01 11:31:53 kali systemd[1]: Starting rsyslog.service - System Logging Service...
Oct 01 11:31:54 kali rsyslogd[38959]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2406.0]
Oct 01 11:31:54 kali rsyslogd[38959]: [origin software="rsyslogd" swVersion="8.2406.0" x-pid="38959" x-info="https://www.rsyslog.com"] start
Oct 01 11:31:54 kali systemd[1]: Started rsyslog.service - System Logging Service.
```

Step 4: Verify logging

Make a change to the **/etc/network/interfaces** file and check the syslog to ensure it records changes: **sudo tail -f /var/log/syslog**.

```
—(kali@kali)-[~]
└─$ sudo tail -f /var/log/syslog
2024-10-01T11:31:53.942208-04:00 kali systemd[1]: Stopping rsyslog.service - System Logging Service...
2024-10-01T11:31:53.964224-04:00 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2406.0" x-pid="26908" x-info="https://www.rsyslog.com"] exiting on signal 15.
2024-10-01T11:31:53.965612-04:00 kali systemd[1]: rsyslog.service: Deactivated successfully.
2024-10-01T11:31:53.965858-04:00 kali systemd[1]: Stopped rsyslog.service - System Logging Service.
2024-10-01T11:31:53.972265-04:00 kali systemd[1]: Starting rsyslog.service - System Logging Service...
2024-10-01T11:31:54.085553-04:00 kali rsyslogd: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd. [v8.2406.0]
2024-10-01T11:31:54.085719-04:00 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2406.0" x-pid="38959" x-info="https://www.rsyslog.com"] start
2024-10-01T11:31:54.085788-04:00 kali systemd[1]: Started rsyslog.service - System Logging Service.
2024-10-01T11:33:29.763904-04:00 kali net-config-change new
2024-10-01T11:34:24.855660-04:00 kali net-config-change changes
```