Linux Administration, Network Services, and System Analysis Guide

By Pomod Dissanayake.

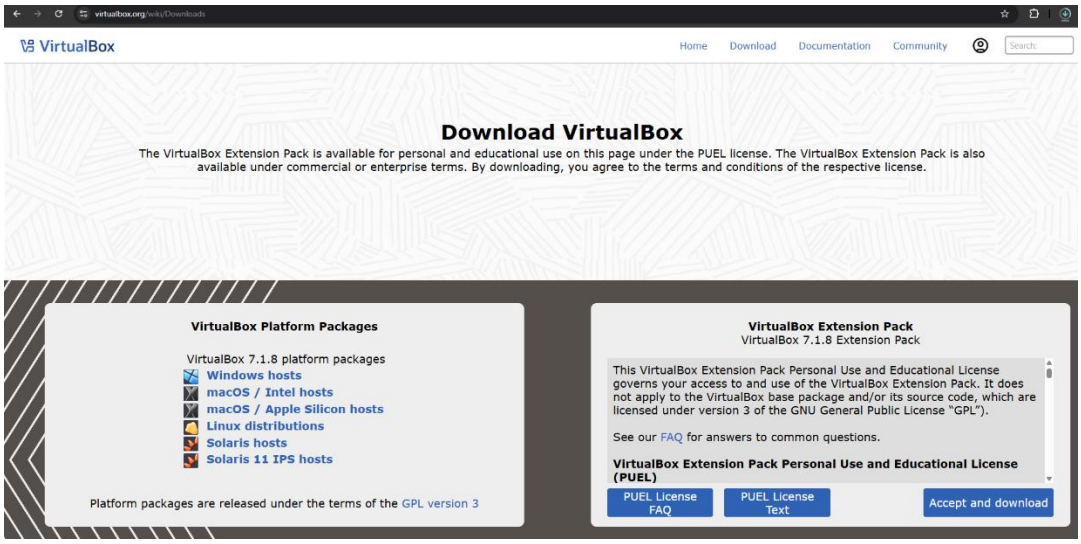
Contents

Basic of Linux Environments

Setting Up

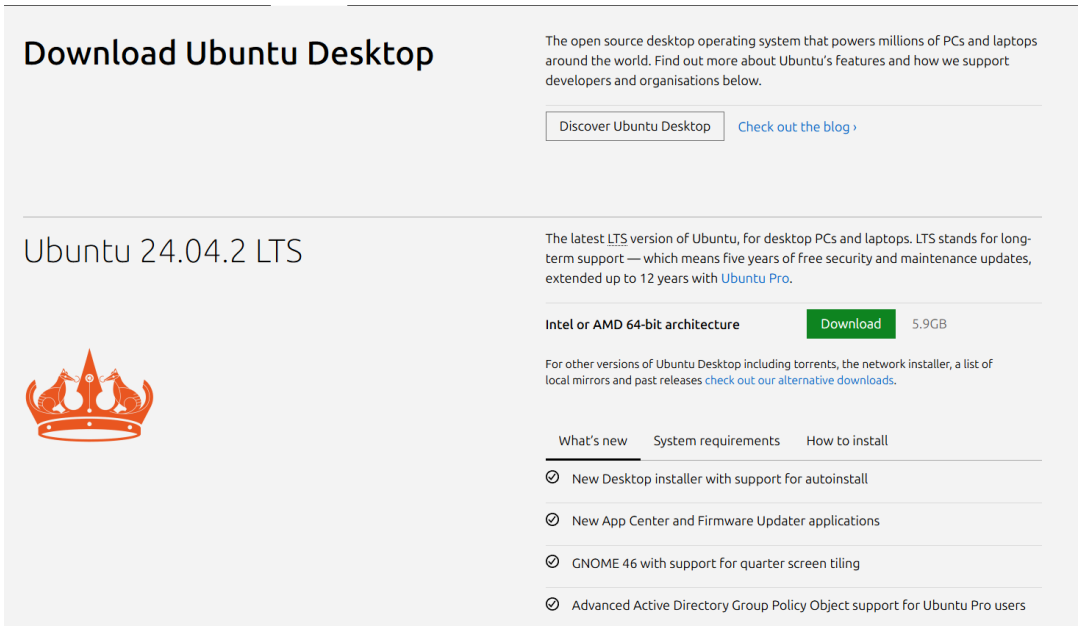
First step was to download a VM manager. Oracle VM manager was chosen for this project.

https://www.virtualbox.org/wiki/Downloads

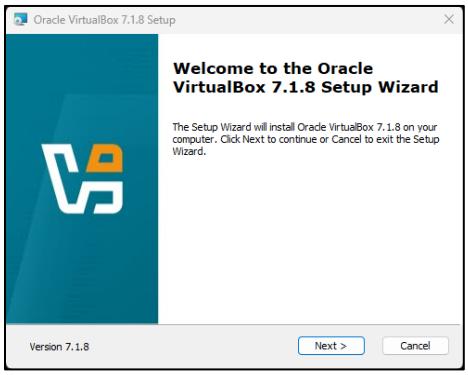


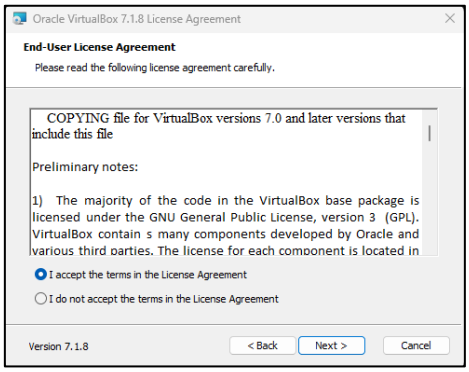
Then a Linux distribution was downloaded. Ubuntu was chosen as the distribution.

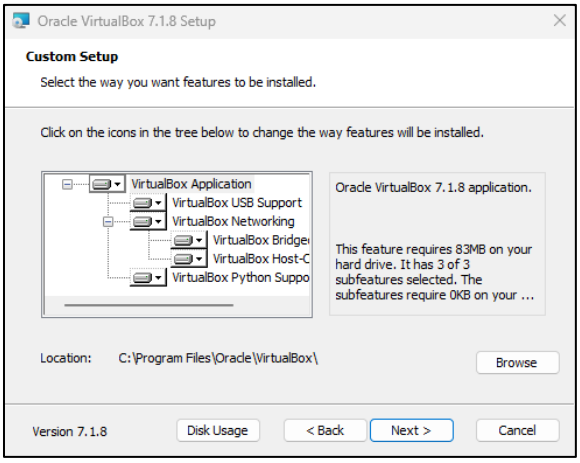
https:/ubuntu.com/download/desktop



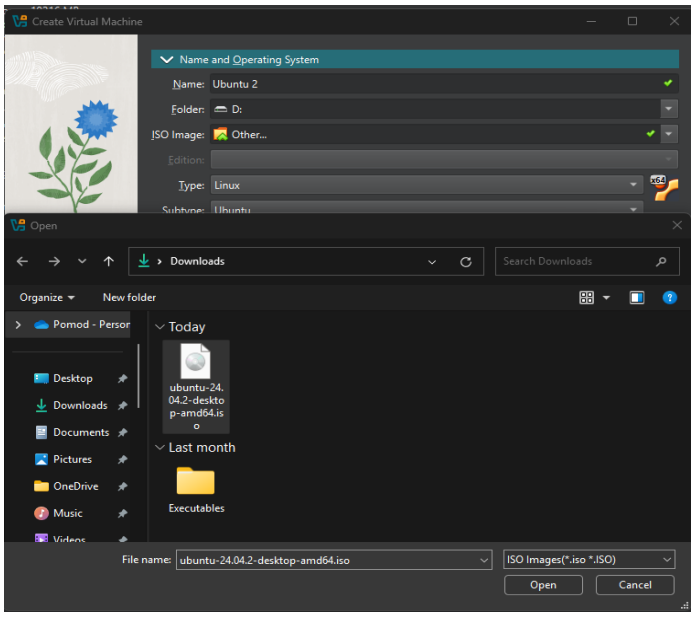
Next step was installing the VM manager.



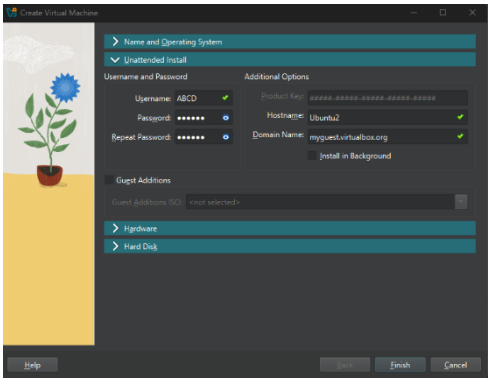


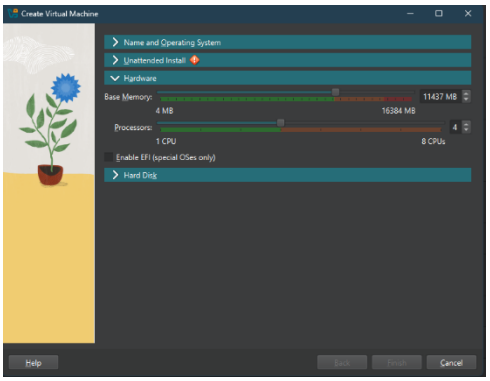


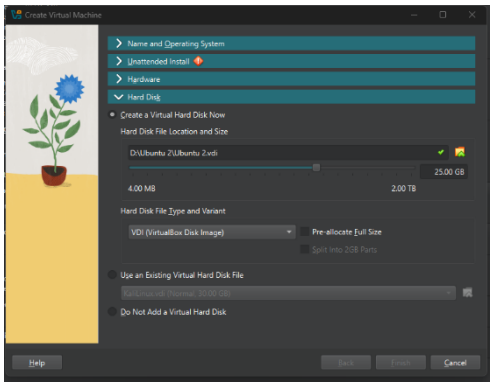
After that, In the oracle manager, selected new and in the following window, selected a name for the virtual machine, selected it's path and chose the ISO image that was downloaded earlier.



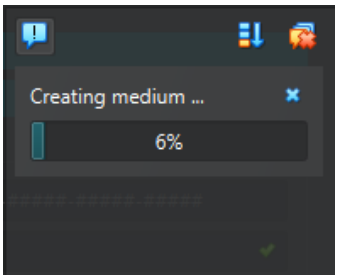
Next steps were to assign a username and password, allocate memory size and processors, and allocate storage space in the chosen storage location.

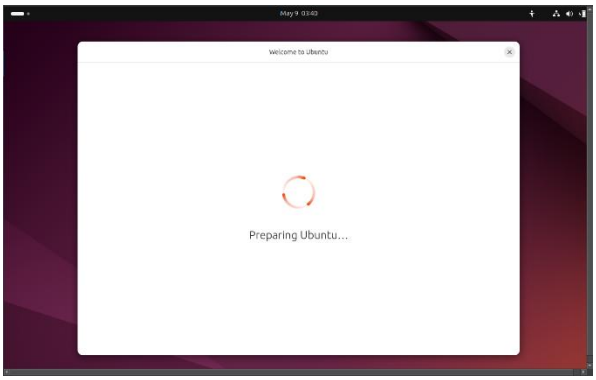


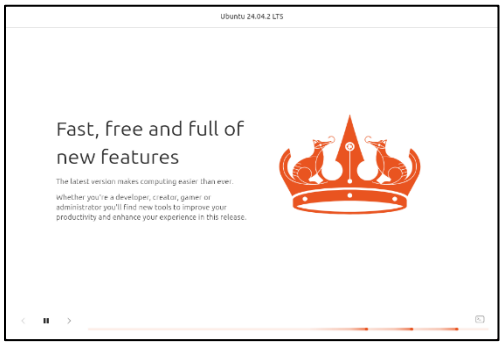




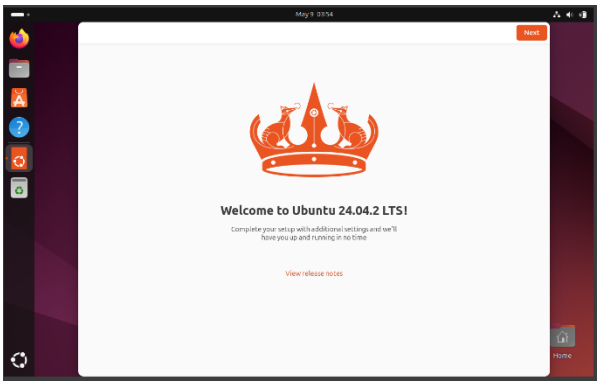
After that, the Oracle VM manager started the installation of the Ubuntu operating system.







When the installation was over, the OS asked for the username and password. After the login part, the Ubuntu operating system was ready to use.



Linux Commands

- "whoami"

  Retrieve the active user name.

```
pomod@pomod-VirtualBox:~$ whoami
pomod
```

- "pwd"

  Print the current working directory.

```
pomod@pomod-VirtualBox:~$ pwd
/home/pomod
```

- "who"

  Retrieve the information about users who are currently logged in.

```
pomod@pomod-VirtualBox:~$ who
pomod    seat0        2025-04-15 09:34 (login screen)
pomod    tty2         2025-04-15 09:34 (tty2)
```

- "ls"

  Lists all files and folders in the current directory.

```
pomod@pomod-VirtualBox:~$ ls
Desktop  Documents  Downloads  Lab1  Music  Pictures  Public  snap
```

- "ls -al"

  List all files and directories with size, permission, date.

```
pomod@pomod-VirtualBox:~/Documents$ ls -al
total 64
drwxr-xr-x  6 pomod pomod  4096 Apr 15 10:13 .
drwxr-x--- 16 pomod pomod  4096 Apr 15 09:41 ..
-rwxrwxr-x  1 pomod pomod 16088 Feb 27 21:50 displaytime
-rw-rw-r--  1 pomod pomod   266 Feb 27 21:50 displaytime.c
-rwxrwxr-x  1 pomod pomod 15960 Feb 28 11:08 hi
-rw-rw-r--  1 pomod pomod    64 Feb 28 11:09 hi.c
drwxrwxr-x  2 pomod pomod  4096 Mar  5 12:28 Lab2
drwxrwxr-x  2 pomod pomod  4096 Mar 12 12:13 Lab3
drwxrwxr-x  2 pomod pomod  4096 Apr 14 06:49 Lab4
-rw-rw-r--  1 pomod pomod     0 Apr 15 10:11 newfile.txt
drwxrwxr-x  4 pomod pomod  4096 Mar 26 14:29 SOS
```

- "cd"

  Used to move between directories.

```
pomod@pomod-VirtualBox:~$ cd Downloads
pomod@pomod-VirtualBox:~/Downloads$
```

- "mkdir"

  Creates a new folder (directory).

```
pomod@pomod-VirtualBox:~/Downloads$ mkdir New_Folder
pomod@pomod-VirtualBox:~/Downloads$ cd New_Folder
pomod@pomod-VirtualBox:~/Downloads/New_Folder$
```

- "rmdir"

  Remove an empty folder (directory).

```
pomod@pomod-VirtualBox:~/Downloads/New_Folder$ cd -
/home/pomod/Downloads
pomod@pomod-VirtualBox:~/Downloads$ rmdir New_Folder
pomod@pomod-VirtualBox:~/Downloads$ ls
2022-S2-IE2050-LabSheet-05.pdf  2023-S2-IE2050-LabSheet-04.pdf
pomod@pomod-VirtualBox:~/Downloads$
```

- "rm"

  Remove files or folders.

```
pomod@pomod-VirtualBox:~/Downloads$ ls
2022-S2-IE2050-LabSheet-05.pdf  2023-S2-IE2050-LabSheet-04.pdf
pomod@pomod-VirtualBox:~/Downloads$ rm 2022-S2-IE2050-LabSheet-05.pdf
pomod@pomod-VirtualBox:~/Downloads$ ls
2023-S2-IE2050-LabSheet-04.pdf
```

- "touch"

  Creates a new empty file.

```
pomod@pomod-VirtualBox:~/Downloads$ touch newfile.txt
pomod@pomod-VirtualBox:~/Downloads$ ls
2023-S2-IE2050-LabSheet-04.pdf  newfile.txt
pomod@pomod-VirtualBox:~/Downloads$
```

- “cp”

  Copy files or directories to another location.

```
pomod@pomod-VirtualBox:~/Documents$ ls
displaytime  displaytime.c  hi  hi.c  Lab2  Lab3  Lab4  newfile.txt  SOS
pomod@pomod-VirtualBox:~/Documents$ cp newfile.txt /home/pomod/Downloads
pomod@pomod-VirtualBox:~/Documents$ cd --
pomod@pomod-VirtualBox:~$ cd Downloads
pomod@pomod-VirtualBox:~/Downloads$ ls
2023-S2-IE2050-LabSheet-04.pdf  newfile.txt
```

- “mv”

  Moves or renames files/directories.

```
pomod@pomod-VirtualBox:~/Downloads$ ls
2023-S2-IE2050-LabSheet-04.pdf  newfile.txt
pomod@pomod-VirtualBox:~/Downloads$ mv newfile.txt /home/pomod/Documents
pomod@pomod-VirtualBox:~/Downloads$ cd --
pomod@pomod-VirtualBox:~$ cd Documents
pomod@pomod-VirtualBox:~/Documents$ ls
displaytime  displaytime.c  hi  hi.c  Lab2  Lab3  Lab4  newfile.txt  SOS
```

- “echo”

  Print text or variables to the terminal.

```
pomod@pomod-VirtualBox:~$ echo "Secure Network Programming"
Secure Network Programming
```

- “df -h”

  Shows available disk space in human-readable format.

```
pomod@pomod-VirtualBox:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           993M  1.5M  991M   1% /run
/dev/sda2        25G   12G   12G  51% /
tmpfs           4.9G     0  4.9G   0% /dev/shm
tmpfs           5.0M  8.0K  5.0M   1% /run/lock
tmpfs           993M  116K  993M   1% /run/user/1000
```

- “free -m”

Display used and free memory in megabytes.

```
pomod@pomod-VirtualBox:~$ free -m
               total        used        free      shared  buff/cache   available
Mem:            9921        1433        7831          49         947        8487
Swap:           4095           0        4095
```

- “uname -a”

  Display all system information.

```
pomod@pomod-VirtualBox:~$ uname -a
Linux pomod-VirtualBox 6.8.0-52-generic #53-Ubuntu SMP PREEMPT_DYNAMIC Sat Jan 11 00:06:25 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
```

DHCP, DNS and NTP Services.

DHCP- Dynamic Host Configuration Protocol.

DHCP is a network management protocol that simplifies the process of assigning IP addresses and related network configuration information to devices on a network. It can assign IP addresses dynamically or statically depending on the requirements. This protocol also assigns other settings like subnet mask, default gateway and DNS.

The range of IP addresses that a DHCP server can hand out is called the DHCP scope. When a computer obtains an IP address, the Server assigns the IP address as a lease. This lease means the amount of time that is valid.

Installation and Configuration

First step would be to install using sudo apt command.

```
pomod@pomod-VirtualBox:~$ sudo apt install isc-dhcp-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  isc-dhcp-common
Suggested packages:
  isc-dhcp-server-ldap policycoreutils
The following NEW packages will be installed:
  isc-dhcp-common isc-dhcp-server
0 upgraded, 2 newly installed, 0 to remove and 316 not upgraded.
Need to get 1,281 kB of archives.
After this operation, 4,281 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-server amd64 4.4.3-P1-4ubuntu2 [1,236 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-common amd64 4.4.3-P1-4ubuntu2 [45.8 kB]
Fetched 1,281 kB in 3s (429 kB/s)
Preconfiguring packages ...
Selecting previously unselected package isc-dhcp-server.
(Reading database ... 189965 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-server_4.4.3-P1-4ubuntu2_amd64.deb ...
Unpacking isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Selecting previously unselected package isc-dhcp-common.
Preparing to unpack .../isc-dhcp-common_4.4.3-P1-4ubuntu2_amd64.deb ...
Unpacking isc-dhcp-common (4.4.3-P1-4ubuntu2) ...
Setting up isc-dhcp-server (4.4.3-P1-4ubuntu2) ...
Generating /etc/default/isc-dhcp-server...
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server.service → /usr/lib/systemd/system/isc-dhcp-server.servi
ce.
Created symlink /etc/systemd/system/multi-user.target.wants/isc-dhcp-server6.service → /usr/lib/systemd/system/isc-dhcp-server6.ser
vice.
Setting up isc-dhcp-common (4.4.3-P1-4ubuntu2) ...
Processing triggers for man-db (2.12.0-4build2) ...
```

Second step would be to edit the configuration file to simulate a small network

```
pomod@pomod-VirtualBox:~$ sudo nano /etc/dhcp/dhcpd.conf
```

```
#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}

subnet 192.168.56.0 netmask 255.255.255.0 {
        range 192.168.56.20 192.168.56.100;
        option routers 192.168.56.1;
        option subnet-mask 255.255.255.0;
        option domain-name-servers 8.8.8.8;
        default-lease-time 600;
        max-lease-time 7200;
}
```

The subnet 192.168.56.0 netmask 255.255.255.0 Defines the network block.

Range defines the IP range the DHCP server will assign to clients.

Option routers define the gateway/router IP address for clients.

Option domain name server point to the Google DNS server.

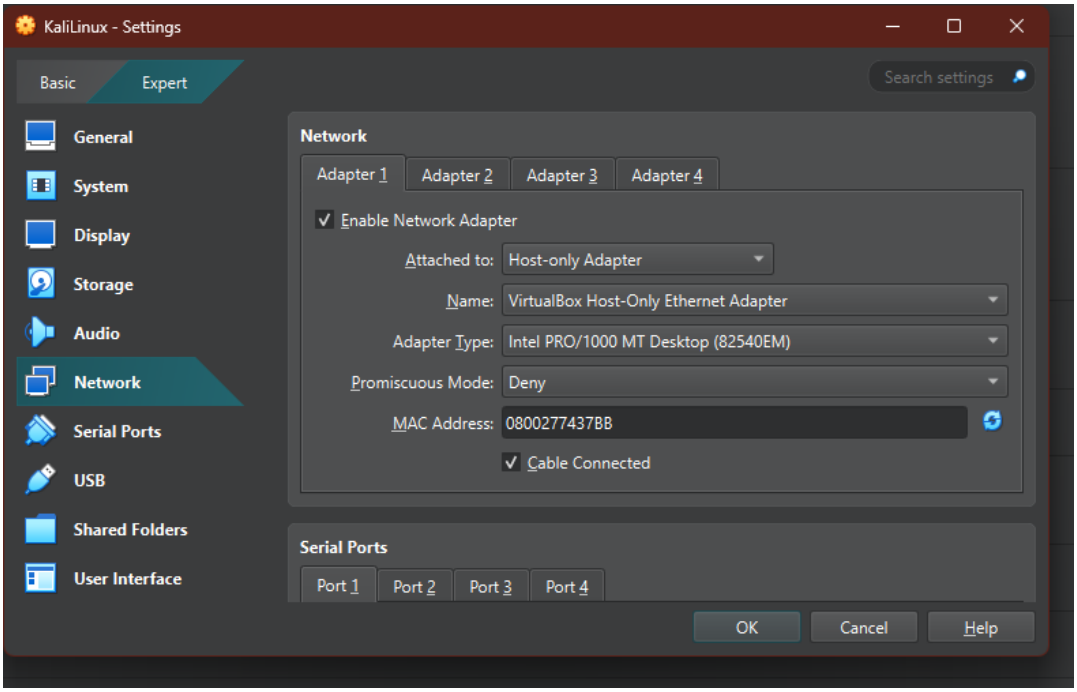
Defualt and max lease time refer to the time duration for each IP address.

The next step would be to configure the network interface.

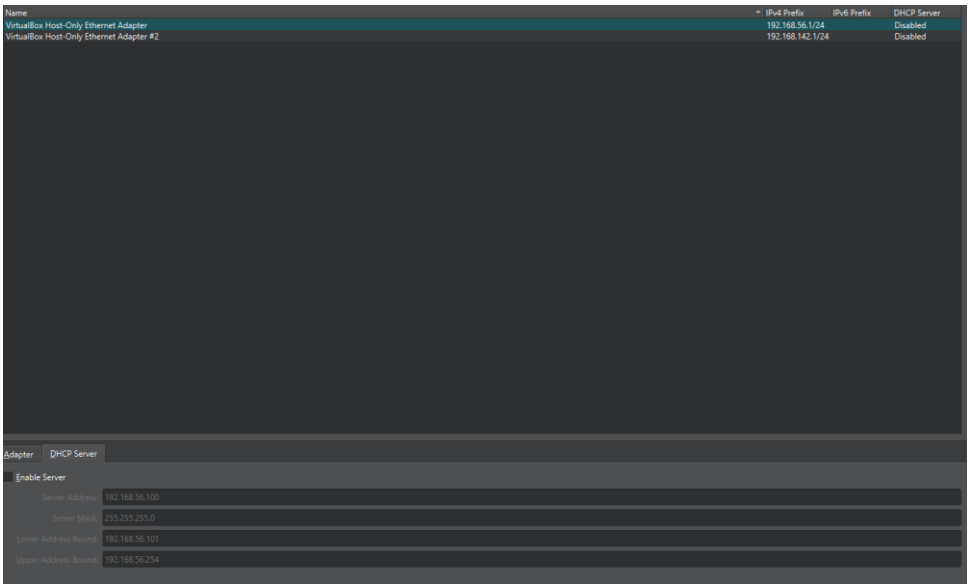
```
  GNU nano 7.2                                          /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="enp0s3"
INTERFACESv6=""
```

The network interface in the device is “enp0s3”.

The network of both VMs that need to be connected must be configured next. Using a host-only adapter lets the VMs talk to each other.



Then, the default DHCP server in the VM manager was disabled to receive an IP from the client.



Then the Ubuntu VM was restarted. After this step, an IP address needed to be assigned manually to the Ubuntu client because it did not have an IP address after the network configuration. Then, the DHCP was restarted and its status was checked.

```
pomod@pomod-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:f5:32:d9 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fef5:32d9/64 scope link
       valid_lft forever preferred_lft forever
pomod@pomod-VirtualBox:~$
```

```
pomod@pomod-VirtualBox:~$ sudo ip addr add 192.168.56.1 dev enp0s3
pomod@pomod-VirtualBox:~$ sudo ip link set enp0s3 up
pomod@pomod-VirtualBox:~$ ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:f5:32:d9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.1/32 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef5:32d9/64 scope link
       valid_lft forever preferred_lft forever
pomod@pomod-VirtualBox:~$ sudo systemctl restart isc-dhcp-server
pomod@pomod-VirtualBox:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-05-06 22:31:09 +0530; 6s ago
       Docs: man:dhcpd(8)
   Main PID: 3602 (dhcpd)
      Tasks: 1 (limit: 11816)
     Memory: 3.8M (peak: 4.0M)
        CPU: 25ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─3602 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf enp0s3

May 06 22:31:09 pomod-VirtualBox dhcpd[3602]: PID file: /run/dhcp-server/dhcpd.pid
May 06 22:31:09 pomod-VirtualBox dhcpd[3602]: Wrote 0 leases to leases file.
May 06 22:31:09 pomod-VirtualBox dhcpd[3602]: Listening on LPF/enp0s3/08:00:27:f5:32:d9/192.168.56.0/24
May 06 22:31:09 pomod-VirtualBox sh[3602]: Listening on LPF/enp0s3/08:00:27:f5:32:d9/192.168.56.0/24
May 06 22:31:09 pomod-VirtualBox sh[3602]: Sending on   LPF/enp0s3/08:00:27:f5:32:d9/192.168.56.0/24
May 06 22:31:09 pomod-VirtualBox sh[3602]: Sending on   Socket/fallback/fallback-net
May 06 22:31:09 pomod-VirtualBox dhcpd[3602]: Sending on   LPF/enp0s3/08:00:27:f5:32:d9/192.168.56.0/24
May 06 22:31:09 pomod-VirtualBox dhcpd[3602]: Sending on   Socket/fallback/fallback-net
May 06 22:31:09 pomod-VirtualBox dhcpd[3602]: Server starting service.
May 06 22:31:13 pomod-VirtualBox dhcpd[3602]: DHCPREQUEST for 10.0.2.15 from 08:00:27:f5:32:d9 via enp0s3: ignored (not authoritative).
```

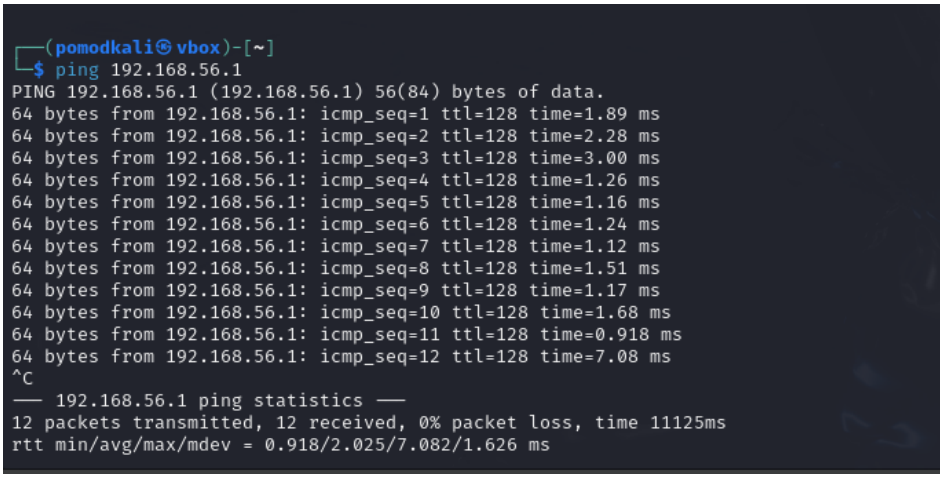
Since the server was active and running, Kali VM was initiated and discarded the current IP that was leased by **dhclient -r** command. After that, using **dhclient -v,** I requested an IP address from an available DHCP server. Since the default one was disabled. The DHCP server in Ubuntu provided the 192.168.56.22 to the Kali VM.

```
┌──(pomodkali㉿vbox)-[~]
└─$ sudo dhclient -r eth0
[sudo] password for pomodkali:

┌──(pomodkali㉿vbox)-[~]
└─$ sudo dhclient -v eth0
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/08:00:27:74:37:bb
Sending on   LPF/eth0/08:00:27:74:37:bb
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 192.168.56.22 from 192.168.56.1
DHCPREQUEST for 192.168.56.22 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.56.22 from 192.168.56.1
bound to 192.168.56.22 -- renewal in 228 seconds.

┌──(pomodkali㉿vbox)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:74:37:bb brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.22/24 brd 192.168.56.255 scope global dynamic eth0
       valid_lft 536sec preferred_lft 536sec
    inet6 fe80::a00:27ff:fe74:37bb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

The provision of the 192.168.56.22 IP address was recorded in the Ubuntu interface as well.

```
pomod@pomod-VirtualBox:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-05-06 22:31:09 +0530; 4min 39s ago
       Docs: man:dhcpd(8)
   Main PID: 3602 (dhcpd)
      Tasks: 1 (limit: 11816)
     Memory: 3.8M (peak: 4.3M)
        CPU: 39ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─3602 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf enp0s3

May 06 22:34:01 pomod-VirtualBox dhcpd[3602]: DHCPDISCOVER from 08:00:27:74:37:bb via enp0s3
May 06 22:34:01 pomod-VirtualBox dhcpd[3602]: icmp_echorequest 192.168.56.21: Network is unreachable
May 06 22:34:02 pomod-VirtualBox dhcpd[3602]: DHCPOFFER on 192.168.56.21 to 08:00:27:74:37:bb (vbox) via enp0s3
May 06 22:34:02 pomod-VirtualBox dhcpd[3602]: DHCPREQUEST for 192.168.56.21 (192.168.56.1) from 08:00:27:74:37:bb (vbox) via enp0s3
May 06 22:34:02 pomod-VirtualBox dhcpd[3602]: DHCPACK on 192.168.56.21 to 08:00:27:74:37:bb (vbox) via enp0s3
May 06 22:35:30 pomod-VirtualBox dhcpd[3602]: DHCPDISCOVER from 08:00:27:74:37:bb via enp0s3
May 06 22:35:30 pomod-VirtualBox dhcpd[3602]: icmp_echorequest 192.168.56.22: Network is unreachable
May 06 22:35:31 pomod-VirtualBox dhcpd[3602]: DHCPOFFER on 192.168.56.22 to 08:00:27:74:37:bb (vbox) via enp0s3
May 06 22:35:31 pomod-VirtualBox dhcpd[3602]: DHCPREQUEST for 192.168.56.22 (192.168.56.1) from 08:00:27:74:37:bb (vbox) via enp0s3
May 06 22:35:31 pomod-VirtualBox dhcpd[3602]: DHCPACK on 192.168.56.22 to 08:00:27:74:37:bb (vbox) via enp0s3
pomod@pomod-VirtualBox:~$
```

For more clarification, the DHCP server was pinged and received successful data packets.



DNS -Domain Name System.

The Domain Name System (DNS) is the phonebook of the Internet. It converts the human-readable domain names, such as google.com, into the machine-readable IP addresses. Every Internet-connected device has a unique IP address that other computers can use to locate it. DNS servers make it unnecessary for people to commit IP addresses like 192.168.1.1 (in IPv4) or, more complicated, recent alphanumeric IP addresses like 2400:cb00:2048:1::c629:d7a2 (in IPv6) to memory.

The following are the steps for configuring a DNS server using BIND on the Ubuntu VM.

The first step was to download BIND9

```
pomod@pomod-VirtualBox:~$ sudo apt install bind9 bind9utils bind9-doc dnsutils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-utils
Suggested packages:
  bind-doc
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils dnsutils
0 upgraded, 5 newly installed, 0 to remove and 316 not upgraded.
Need to get 3,673 kB of archives.
After this operation, 9,274 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

After the installation, a domain was created for testing by editing the named.conf.local file.

```
pomod@pomod-VirtualBox:~$ sudo nano /etc/bind/named.conf.local
  GNU nano 7.2                                  /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "mytest.local" {
        type master;
        file "/etc/bind/db.mytest.local";
};
```

This defines a DNS zone called mytest.local.

A zone represents a domain or subdomain that the DNS server is responsible for.

The type of this zone is set to master.

This means this server is the primary/master DNS server for mytest.local.

Then a copy of the default zone file (db.local)was created and named it db.mytest.local so that it can used for domain mytest.local.

```
pomod@pomod-VirtualBox:~$ sudo cp /etc/bind/db.local /etc/bind/db.mytest.local
```

Then db.mytest.local file was configured to specify the authoritative server and to map hostnames to IP addresses.

```
pomod@pomod-VirtualBox:~$ sudo nano /etc/bind/db.mytest.local
```

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.mytest.local. admin.mytest.local (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.mytest.local.
ns1     IN      A       127.0.0.1
@       IN      A       127.0.0.1
www     IN      A       10.0.2.15
```

Then used the command **sudo systemctl restart bind9** to restart the DNS server and **sudo systemctl status bind9** to find the status of the server.

```
● named.service - BIND Domain Name Server
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-05-08 21:01:34 +0530; 2s ago
       Docs: man:named(8)
   Main PID: 3681 (named)
     Status: "running"
      Tasks: 10 (limit: 11816)
     Memory: 6.7M (peak: 7.3M)
        CPU: 436ms
     CGroup: /system.slice/named.service
             └─3681 /usr/sbin/named -f -u bind

May 08 21:01:33 pomod-VirtualBox named[3681]: zone 0.in-addr.arpa/IN: loaded serial 1
May 08 21:01:33 pomod-VirtualBox named[3681]: zone 127.in-addr.arpa/IN: loaded serial 1
May 08 21:01:34 pomod-VirtualBox named[3681]: zone 255.in-addr.arpa/IN: loaded serial 1
May 08 21:01:34 pomod-VirtualBox named[3681]: zone mytest.local/IN: loaded serial 2
May 08 21:01:34 pomod-VirtualBox named[3681]: zone localhost/IN: loaded serial 2
May 08 21:01:34 pomod-VirtualBox named[3681]: all zones loaded
May 08 21:01:34 pomod-VirtualBox named[3681]: running
May 08 21:01:34 pomod-VirtualBox systemd[1]: Started named.service - BIND Domain Name Server.
May 08 21:01:34 pomod-VirtualBox named[3681]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
May 08 21:01:34 pomod-VirtualBox named[3681]: managed-keys-zone: Key 38696 for zone . is now trusted (acceptance timer complete)
pomod@pomod-VirtualBox:~$
```

Then updated the resolve.conf to add the nameserver 127.0.0.1 so that the system uses the DNS server that was created.

```
pomod@pomod-VirtualBox:~$ sudo nano /etc/resolv.conf
[sudo] password for pomod:
```

```
  GNU nano 7.2                                                    /etc/resolv.conf *
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.1
options edns0 trust-ad
search .
```

Then it was tested with the **dig** command to verify whether it was working.

```
pomod@pomod-VirtualBox:~$ dig @127.0.0.1 www.mytest.local

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @127.0.0.1 www.mytest.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48044
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: fe92e96b166082dd01000000681cce8a017f7c97274660ac (good)
;; QUESTION SECTION:
;www.mytest.local.              IN      A

;; ANSWER SECTION:
www.mytest.local.       604800  IN      A       10.0.2.15

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu May 08 21:02:26 +0530 2025
;; MSG SIZE  rcvd: 89
```

Instead of the local server, it is possible to use a public DNS such as Google DNS. By using 8.8.8.8 rather than the local nameserver IP in the resolve.conf file, Google DNS was accessed.

```
nameserver 8.8.8.8
options edns0 trust-ad
search .
```

```
pomod@pomod-VirtualBox:~$ ping google.com
PING google.com (142.251.42.110) 56(84) bytes of data.
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=1 ttl=255 time=110 ms
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=2 ttl=255 time=104 ms
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=3 ttl=255 time=110 ms
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=4 ttl=255 time=108 ms
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=5 ttl=255 time=108 ms
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=6 ttl=255 time=109 ms
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=7 ttl=255 time=109 ms
64 bytes from bom07s45-in-f14.1e100.net (142.251.42.110): icmp_seq=8 ttl=255 time=107 ms
^C
--- google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 11108ms
rtt min/avg/max/mdev = 104.332/108.223/109.600/1.631 ms
pomod@pomod-VirtualBox:~$ dig google.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45560
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             17      IN      A       142.251.42.110
```

NTP- Network Time Protocol

Network Time Protocol synchronizes time across all devices across a network. It ensures that all devices on a network agree on the current time. Allowing them to coordinate activities, log events accurately and maintain time-sensitive operations.

sudo apt install ntp command is used to download NTP service to the system.

```
pomod@pomod-VirtualBox:~$ sudo apt install ntp
```

By using the **ntpq -p** command, the NTP servers were shown and the server that the system was synchronized with was marked with a " * " sign.

```
pomod@pomod-VirtualBox:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
 0.ubuntu.pool.n .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 1.ubuntu.pool.n .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 2.ubuntu.pool.n .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 3.ubuntu.pool.n .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 alphyn.canonica 132.163.96.1     2 u    6   64    3 256.0047  -1.7351   8.5589
+time.cloudflare 10.111.8.4       3 u   59   64    1  12.4850  22.0162  12.0902
+time.cloudflare 10.111.8.4       3 u   59   64    1  12.6068  22.0821   2.1396
*ntp.sltidc.lk   216.239.35.8     2 u   59   64    1  11.0082   5.9167   0.9226
+time.cloudflare 10.111.8.4       3 u   11   64    3   8.6134  31.2097  12.2610
-time.cloudflare 10.111.8.4       3 u   30   64    3  19.6926  28.5153  17.4762
pomod@pomod-VirtualBox:~$
```

Security and other servers

Shell Scripting

```bash
#!/bin/bash

LOG_DIR="/var/log/custom_logs"
BACKUP_DIR="/backups"
TODAY=$(date +%Y%m%d)

mkdir -p "$LOG_DIR"
mkdir -p "$BACKUP_DIR"

# Delete old log files and count them
DELETED_FILES=$(find "$LOG_DIR" -name "*.log" -type f -mtime +7 -print -delete | wc -l)

# Find remaining log files
LOG_FILES=("$LOG_DIR"/*.log)
LOG_COUNT=${#LOG_FILES[@]}

if [ "$DELETED_FILES" -gt 0 ]; then
    echo "Deleted $DELETED_FILES old log files."
else
    echo "No old log files to delete."
fi

if [ -e "${LOG_FILES[0]}" ]; then
    cd "$LOG_DIR"
    tar -czf "$BACKUP_DIR/logs_${TODAY}.tar.gz" *.log
    ARCHIVED_FILES=$(tar -tzf "$BACKUP_DIR/logs_${TODAY}.tar.gz" | wc -l)
    echo "Archived $ARCHIVED_FILES log files to $BACKUP_DIR/logs_${TODAY}.tar.gz"
    cd -
else
    echo "No log files to archive."
fi
```

Code

```
#!/bin/bash
LOG_DIR="/var/log/custom_logs"
BACKUP_DIR="/backups"
TODAY=$(date +%Y%m%d)

mkdir -p "$LOG_DIR"
mkdir -p "$BACKUP_DIR"

# Delete old log files and count them
DELETED_FILES=$(find "$LOG_DIR" -name "*.log" -type f -mtime +7 -print -delete | wc -l)

# Find remaining log files
LOG_FILES=("$LOG_DIR"/*.log)
LOG_COUNT=${#LOG_FILES[@]}
if [ "$DELETED_FILES" -gt 0 ]; then
    echo "Deleted $DELETED_FILES old log files."
else
    echo "No old log files to delete."
fi
if [ -e "${LOG_FILES[0]}" ]; then
    cd "$LOG_DIR"
    tar -czf "$BACKUP_DIR/logs_${TODAY}.tar.gz" *.log
    ARCHIVED_FILES=$(tar -tzf "$BACKUP_DIR/logs_${TODAY}.tar.gz" | wc -l)
    echo "Archived $ARCHIVED_FILES log files to $BACKUP_DIR/logs_${TODAY}.tar.gz"
    cd -
else
    echo "No log files to archive."
fi
```

Result

```
pomod@pomod-VirtualBox:~/Documents$ bash ./log_cleanup.sh
No old log files to delete.
Archived 5 log files to /backups/logs_20250508.tar.gz
/home/pomod/Documents
pomod@pomod-VirtualBox:~/Documents$
```

Cron Job

```
pomod@pomod-VirtualBox:~/Documents$ sudo crontab -e
no crontab for root - using an empty one
crontab: installing new crontab
```

```
  GNU nano 7.2                                  /tmp/crontab.A0vU3n/crontab *
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

0 0 * * 0 /home/pomod/Documents/log_cleanup.sh
```

code

0 0 * * 0 /home/pomod/Documents/log_cleanup.sh

SSH -Secure Shell

SSH (Secure Shell) is a secure network protocol used to access and manage remote computers safely. It encrypts the connection, protecting data and passwords from being intercepted. SSH is commonly used by system administrators to log in, run commands, and transfer files securely over the internet.

First step was to download OpenSSH to the system.

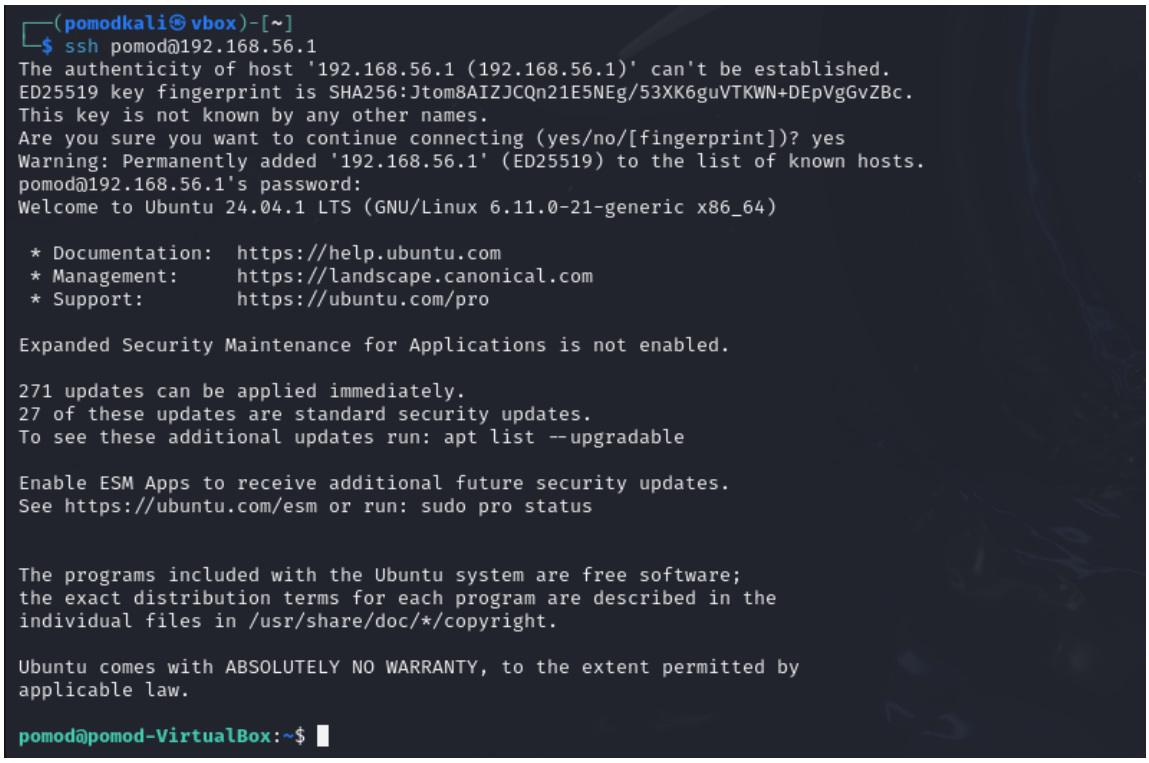
```
pomod@pomod-VirtualBox:~$ sudo apt install openssh-server -y
[sudo] password for pomod:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
```

This requres the same network configuration as in the DHCP server setup to connect both VMs.The next step was to start the SSH service and check its status.

```
pomod@pomod-VirtualBox:~$ sudo systemctl enable --now ssh
```

```
pomod@pomod-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>
     Active: active (running) since Tue 2025-05-06 22:53:54 +0530; 27s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3370 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3372 (sshd)
      Tasks: 1 (limit: 11816)
     Memory: 2.1M (peak: 2.4M)
        CPU: 72ms
     CGroup: /system.slice/ssh.service
             └─3372 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 06 22:53:53 pomod-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Sec>
May 06 22:53:54 pomod-VirtualBox sshd[3372]: Server listening on :: port 22.
May 06 22:53:54 pomod-VirtualBox systemd[1]: Started ssh.service - OpenBSD Secu>
```

After that, Using the Ubuntu's host-only IP, Access to the Ubuntu system through Kali Linux was possible.



iptabels and ACL

iptables is a Linux-based firewall tool that lets administrators set up rules to control incoming and outgoing network traffic, enhancing server security by filtering packets based on criteria like IP address, port, and protocol.

Access Control Lists (ACLs) are sets of rules used to permit or deny access to system resources or network traffic. ACLs can be used on files and directories to manage user permissions, or on network devices to filter traffic and improve security by specifying which users or systems can access certain resources.

In order to limit access to Facebook, Instagram and Twitter, IP addresses of these sites are needed. nslookup was used for this task.

```
pomod@pomod-VirtualBox:~$ nslookup facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   facebook.com
Address: 57.144.144.1
Name:   facebook.com
Address: 2a03:2880:f348:1:face:b00c:0:25de

pomod@pomod-VirtualBox:~$ nslookup instagram.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   instagram.com
Address: 157.240.15.174
Name:   instagram.com
Address: 2a03:2880:f20c:1e5:face:b00c:0:4420

pomod@pomod-VirtualBox:~$ nslookup twitter.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   twitter.com
Address: 162.159.140.229
```

After that, using those IPs, the rules were created that block access to these sites. The rules are given below.

```
pomod@pomod-VirtualBox:~$ sudo iptables -A OUTPUT -d 57.144.144.1 -j REJECT
pomod@pomod-VirtualBox:~$ sudo iptables -A OUTPUT -d 157.240.15.174 -j REJECT
pomod@pomod-VirtualBox:~$ sudo iptables -A OUTPUT -d 162.159.140.229 -j REJECT
```

To block all unencrypted HTTP traffic (port 80) and allow only HTTPS (port 443) to ensure secure browsing for all users, the following rules were implemented and updated.

```
pomod@pomod-VirtualBox:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -j REJECT
pomod@pomod-VirtualBox:~$ sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
```

iptables Rules

sudo iptables -A OUTPUT -d 57.144.144.1 -j REJECT

sudo iptables -A OUTPUT -d 157.240.15.174 -j REJECT

sudo iptables -A OUTPUT -d 162.159.140.229 -j REJECT

sudo iptables -A OUTPUT -p tcp –dport 80 -j REJECT

sudo iptables -A OUTPUT -p tcp –dport 443 -j ACCEPT

Web Server

A web server is a computer system, consisting of hardware and software, that stores, processes, and delivers web content such as web pages, images, and videos to users over the internet using the HTTP or HTTPS protocols. When a user requests a web page through a browser, the web server processes the request, retrieves the necessary files, and sends them back to the browser to display. Web servers can host multiple websites, support dynamic content generation, and handle various services like web hosting, email, and media streaming. Popular web server software includes Apache, Nginx, and LiteSpeed

To download Apache server to the system, **sudo apt install apache2** was used.

```
pomod@pomod-VirtualBox:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
0 upgraded, 8 newly installed, 0 to remove and 266 not upgraded.
Need to get 1,900 kB of archives.
After this operation, 7,455 kB of additional disk space will be used.
```

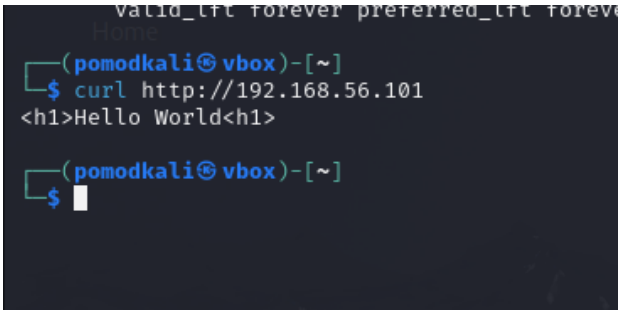
The next step was the enabling and status check of the system.

```
pomod@pomod-VirtualBox:~$ sudo systemctl status apache2
[sudo] password for pomod:
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-05-08 21:58:42 +0530; 51min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1239 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1323 (apache2)
      Tasks: 55 (limit: 11816)
     Memory: 7.6M (peak: 8.2M)
        CPU: 790ms
     CGroup: /system.slice/apache2.service
             ├─1323 /usr/sbin/apache2 -k start
             ├─1325 /usr/sbin/apache2 -k start
             └─1326 /usr/sbin/apache2 -k start

May 08 21:58:38 pomod-VirtualBox systemd[1]: Starting apache2.service - The Apache HTTP Server...
May 08 21:58:42 pomod-VirtualBox apachectl[1277]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' direct
May 08 21:58:42 pomod-VirtualBox systemd[1]: Started apache2.service - The Apache HTTP Server.
```

After starting the server, a small sample web page was created.

```
pomod@pomod-VirtualBox:~$ echo '<h1>Hello World<h1>' | sudo tee /var/www/html/index.html
[sudo] password for pomod:
<h1>Hello World<h1>
pomod@pomod-VirtualBox:~$
```

Then, using the Kali VM and Ubuntu IP, the web page was accessed over the network successfully.

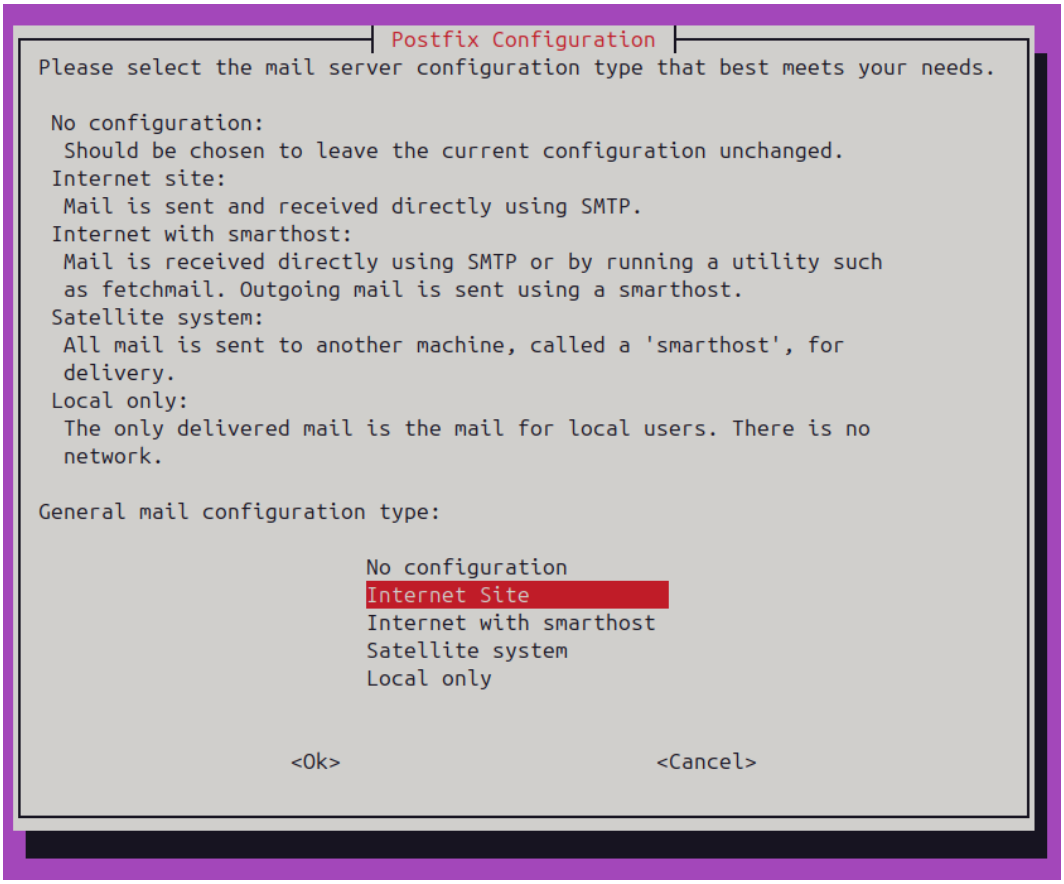


Email Server

An email server is a computer system that sends, receives, and stores emails by managing the flow of messages between senders and recipients. It uses protocols like SMTP to send outgoing mail and POP3 or IMAP to receive incoming mail. Acting like a digital post office, the email server ensures emails are properly routed, authenticated, and secured, often filtering spam and protecting sensitive information. It works behind the scenes while users interact with email clients like Gmail or Outlook to access their messages

Postfix was installed as the first step.

```
pomod@pomod-VirtualBox:~$ sudo apt install postfix mailutils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gsasl-common guile-3.0-libs libgc1 libgsasl18 libgssglue1 libmailutils9t64 libmysqlclient21 libnsl2 libntlm0 libpq5 mailutils-common mysql-common
Suggested packages:
  mailutils-mh mailutils-doc postfix-cdb postfix-doc postfix-ldap postfix-lmdb postfix-mta-sts-resolver postfix-mysql postfix-pcre postfix-pgsql postfix-sqlite procmail sasl2-bin
  | dovecot-common
The following NEW packages will be installed:
  gsasl-common guile-3.0-libs libgc1 libgsasl18 libgssglue1 libmailutils9t64 libmysqlclient21 libnsl2 libntlm0 libpq5 mailutils mailutils-common mysql-common postfix
0 upgraded, 14 newly installed, 0 to remove and 266 not upgraded.
Need to get 11.6 MB of archives.
After this operation, 71.9 MB of additional disk space will be used.
```



Then, a test email was sent to the server. After that, the mail was discovered by the **mail** command.

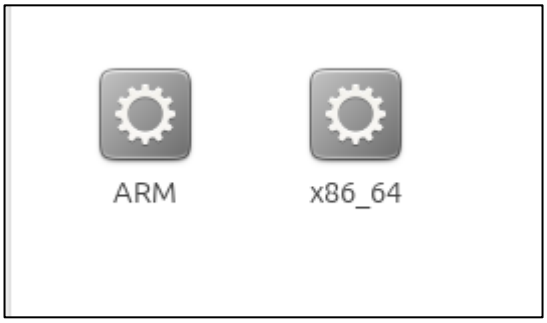
```
pomod@pomod-VirtualBox:~$ echo 'Test mail' | mail -s 'Test Subject' pomod
pomod@pomod-VirtualBox:~$ mail
"/var/mail/pomod": 1 message 1 new
>N   1 Pomod              Tue May  6 23:59  13/440   Test Subject
?
```

```
Return-Path: <pomod@pomod-VirtualBox>
X-Original-To: pomod
Delivered-To: pomod@pomod-VirtualBox
Received: by pomod-VirtualBox (Postfix, from userid 1000)
        id 5DA64A463D; Tue,  6 May 2025 23:59:44 +0530 (+0530)
Subject: Test Subject
To: pomod@pomod-VirtualBox
User-Agent: mail (GNU Mailutils 3.17)
Date: Tue,  6 May 2025 23:59:44 +0530
Message-Id: <20250506182944.5DA64A463D@pomod-VirtualBox>
From: Pomod <pomod@pomod-VirtualBox>
```

Linux GDB

Execution Process

The executable file contained two files that are meant for two different system architectures.




```
pomod@pomod-VirtualBox:~$ uname -m
x86_64
pomod@pomod-VirtualBox:~$
```

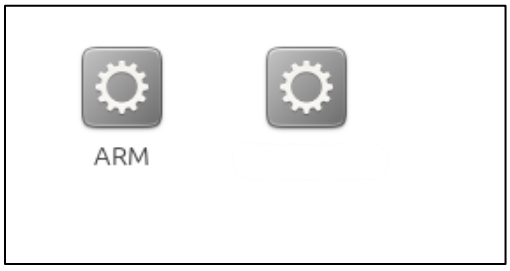
The x86_64 was chosen as it matched the system architecture. After granting permission, the program was executed.

```
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$ ./x86_64
bash: ./x86_64: Permission denied
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$
```

```
ables$ chmod +x x86_64
ables$
```

```
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$ ./x86_64
Enter the student IT number:
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$
```

The program asked for the registration number, and when provided, the program renamed it as the registration number.



The program, now renamed, was executed again. This created a text file.

```
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$ ./[redacted]
[sudo] password for pomod:
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$
```


```
total 104
drwxr-xr-x 2 pomod pomod  4096 May  8 15:48 .
drwxrwxr-x 4 pomod pomod  4096 May  8 15:45 ..
-rw-rw-r-- 1 pomod pomod 70824 Mar 17 06:26 ARM
-rwx------ 1 pomod pomod    36 May  8 15:51 data.txt
-rwxrwxr-x 1 pomod pomod 20368 May  8 15:46 [redacted]
```

The creation time confirms that it was created after the execution of the aforementioned program.

Debugging Process

The first step was to open GDB with the executable file. -q was used for smoother output.

```
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$ gdb -q ./[redacted]
Warning: 'set logging on', an alias for the command 'set logging enabled', is deprecated.
Use 'set logging enabled on'.

Warning: 'set logging off', an alias for the command 'set logging enabled', is deprecated.
Use 'set logging enabled off'.

Reading symbols from ./[redacted]...
```

The **info functions** command was used to identify the functions in this particular program.

```
gdb$ info functions
All defined functions:

File [redacted].c:
13:     int main();
5:      void xor_encrypt_decrypt(char *, const char *);
```

This shows that there are two functions in the program. The first one was the common main function, but the second one was named as “xor_encrypt_decrypt”. This means the operation in this program is encryption. There are two parameters that are being passed. Both of them are passing as characters, and one parameter is set as a constant. This might be a key that is used for encryption.

Now the disassembled language was set to Intel because by default it is set to AT&T, and Intel is more user-friendly.

```
gdb$ set disassembly-flavor intel
```

Next, the disassembled code was taken from both functions to get a rough idea of the program.

```
gdb$ disas main
Dump of assembler code for function main:
   0x00000000000012f0 <+0>:     endbr64
   0x00000000000012f4 <+4>:     push   rbp
   0x00000000000012f5 <+5>:     mov    rbp,rsp
   0x00000000000012f8 <+8>:     sub    rsp,0x60
   0x00000000000012fc <+12>:    mov    rax,QWORD PTR fs:0x28
   0x0000000000001305 <+21>:    mov    QWORD PTR [rbp-0x8],rax
   0x0000000000001309 <+25>:    xor    eax,eax
   0x000000000000130b <+27>:    lea    rax,[rip+0xcf6]        # 0x2008
   0x0000000000001312 <+34>:    mov    rsi,rax
   0x0000000000001315 <+37>:    lea    rax,[rip+0xcf4]        # 0x2010
   0x000000000000131c <+44>:    mov    rdi,rax
   0x000000000000131f <+47>:    call   0x1160 <popen@plt>
   0x0000000000001324 <+52>:    mov    QWORD PTR [rbp-0x58],rax
   0x0000000000001328 <+56>:    cmp    QWORD PTR [rbp-0x58],0x0
   0x000000000000132d <+61>:    jne    0x1348 <main+88>
   0x000000000000132f <+63>:    lea    rax,[rip+0xd02]        # 0x2038
   0x0000000000001336 <+70>:    mov    rdi,rax
   0x0000000000001339 <+73>:    call   0x10e0 <puts@plt>
   0x000000000000133e <+78>:    mov    eax,0x1
   0x0000000000001343 <+83>:    jmp    0x1400 <main+272>
   0x0000000000001348 <+88>:    mov    rdx,QWORD PTR [rbp-0x58]
   0x000000000000134c <+92>:    lea    rax,[rbp-0x40]
   0x0000000000001350 <+96>:    mov    esi,0x32
   0x0000000000001355 <+101>:   mov    rdi,rax
   0x0000000000001358 <+104>:   call   0x1150 <fgets@plt>
   0x000000000000135d <+109>:   mov    rax,QWORD PTR [rbp-0x58]
   0x0000000000001361 <+113>:   mov    rdi,rax
   0x0000000000001364 <+116>:   call   0x1120 <pclose@plt>
   0x0000000000001369 <+121>:   lea    rax,[rbp-0x40]
   0x000000000000136d <+125>:   lea    rdx,[rip+0xcda]        # 0x204e
   0x0000000000001374 <+132>:   mov    rsi,rdx
   0x0000000000001377 <+135>:   mov    rdi,rax
   0x000000000000137a <+138>:   call   0x1140 <strcspn@plt>
   0x000000000000137f <+143>:   mov    BYTE PTR [rbp+rax*1-0x40],0x0
   0x0000000000001384 <+148>:   lea    rax,[rip+0xcc5]        # 0x2050
   0x000000000000138b <+155>:   mov    QWORD PTR [rbp-0x50],rax
   0x000000000000138f <+159>:   mov    rdx,QWORD PTR [rbp-0x50]
   0x0000000000001393 <+163>:   lea    rax,[rbp-0x40]
   0x0000000000001397 <+167>:   mov    rsi,rdx
   0x000000000000139a <+170>:   mov    rdi,rax
   0x000000000000139d <+173>:   call   0x1269 <xor_encrypt_decrypt>
   0x00000000000013a2 <+178>:   lea    rax,[rip+0xcab]        # 0x2054
   0x00000000000013a9 <+185>:   mov    rsi,rax
   0x00000000000013ac <+188>:   lea    rax,[rip+0xca3]        # 0x2056
   0x00000000000013b3 <+195>:   mov    rdi,rax
   0x00000000000013b6 <+198>:   call   0x1170 <fopen@plt>
   0x00000000000013bb <+203>:   mov    QWORD PTR [rbp-0x48],rax
   0x00000000000013bf <+207>:   cmp    QWORD PTR [rbp-0x48],0x0
   0x00000000000013c4 <+212>:   jne    0x13dc <main+236>
   0x00000000000013c6 <+214>:   lea    rax,[rip+0xc92]        # 0x205f
   0x00000000000013cd <+221>:   mov    rdi,rax
   0x00000000000013d0 <+224>:   call   0x10e0 <puts@plt>
   0x00000000000013d5 <+229>:   mov    eax,0x1
   0x00000000000013da <+234>:   jmp    0x1400 <main+272>
   0x00000000000013dc <+236>:   mov    rdx,QWORD PTR [rbp-0x48]
   0x00000000000013e0 <+240>:   lea    rax,[rbp-0x40]
   0x00000000000013e4 <+244>:   mov    rsi,rdx
   0x00000000000013e7 <+247>:   mov    rdi,rax
   0x00000000000013ea <+250>:   call   0x1130 <fputs@plt>
   0x00000000000013ef <+255>:   mov    rax,QWORD PTR [rbp-0x48]
   0x00000000000013f3 <+259>:   mov    rdi,rax
   0x00000000000013f6 <+262>:   call   0x10f0 <fclose@plt>
   0x00000000000013fb <+267>:   mov    eax,0x0
   0x0000000000001400 <+272>:   mov    rdx,QWORD PTR [rbp-0x8]
   0x0000000000001404 <+276>:   sub    rdx,QWORD PTR fs:0x28
   0x000000000000140d <+285>:   je     0x1414 <main+292>
   0x000000000000140f <+287>:   call   0x1110 <__stack_chk_fail@plt>
   0x0000000000001414 <+292>:   leave
   0x0000000000001415 <+293>:   ret
End of assembler dump.
```

```
gdb$ disas xor_encrypt_decrypt
Dump of assembler code for function xor_encrypt_decrypt:
   0x0000000000001269 <+0>:     endbr64
   0x000000000000126d <+4>:     push   rbp
   0x000000000000126e <+5>:     mov    rbp,rsp
   0x0000000000001271 <+8>:     sub    rsp,0x30
   0x0000000000001275 <+12>:    mov    QWORD PTR [rbp-0x28],rdi
   0x0000000000001279 <+16>:    mov    QWORD PTR [rbp-0x30],rsi
   0x000000000000127d <+20>:    mov    rax,QWORD PTR [rbp-0x28]
   0x0000000000001281 <+24>:    mov    rdi,rax
   0x0000000000001284 <+27>:    call   0x1100 <strlen@plt>
   0x0000000000001289 <+32>:    mov    QWORD PTR [rbp-0x10],rax
   0x000000000000128d <+36>:    mov    rax,QWORD PTR [rbp-0x30]
   0x0000000000001291 <+40>:    mov    rdi,rax
   0x0000000000001294 <+43>:    call   0x1100 <strlen@plt>
   0x0000000000001299 <+48>:    mov    QWORD PTR [rbp-0x8],rax
   0x000000000000129d <+52>:    mov    QWORD PTR [rbp-0x18],0x0
   0x00000000000012a5 <+60>:    jmp    0x12e2 <xor_encrypt_decrypt+121>
   0x00000000000012a7 <+62>:    mov    rdx,QWORD PTR [rbp-0x28]
   0x00000000000012ab <+66>:    mov    rax,QWORD PTR [rbp-0x18]
   0x00000000000012af <+70>:    add    rax,rdx
   0x00000000000012b2 <+73>:    movzx  esi,BYTE PTR [rax]
   0x00000000000012b5 <+76>:    mov    rax,QWORD PTR [rbp-0x18]
   0x00000000000012b9 <+80>:    mov    edx,0x0
   0x00000000000012be <+85>:    div    QWORD PTR [rbp-0x8]
   0x00000000000012c2 <+89>:    mov    rax,QWORD PTR [rbp-0x30]
   0x00000000000012c6 <+93>:    add    rax,rdx
   0x00000000000012c9 <+96>:    movzx  ecx,BYTE PTR [rax]
   0x00000000000012cc <+99>:    mov    rdx,QWORD PTR [rbp-0x28]
   0x00000000000012d0 <+103>:   mov    rax,QWORD PTR [rbp-0x18]
   0x00000000000012d4 <+107>:   add    rax,rdx
   0x00000000000012d7 <+110>:   xor    esi,ecx
   0x00000000000012d9 <+112>:   mov    edx,esi
   0x00000000000012db <+114>:   mov    BYTE PTR [rax],dl
   0x00000000000012dd <+116>:   add    QWORD PTR [rbp-0x18],0x1
   0x00000000000012e2 <+121>:   mov    rax,QWORD PTR [rbp-0x18]
   0x00000000000012e6 <+125>:   cmp    rax,QWORD PTR [rbp-0x10]
   0x00000000000012ea <+129>:   jb     0x12a7 <xor_encrypt_decrypt+62>
   0x00000000000012ec <+131>:   nop
   0x00000000000012ed <+132>:   nop
   0x00000000000012ee <+133>:   leave
   0x00000000000012ef <+134>:   ret
End of assembler dump.
gdb$
```

In summary,

- The main program calls popen() with a command and captures its output,
- Reads a line from the output into a buffer,
- Calls strcspn() to trim newline characters,
- Calls xor_encrypt_decrypt() function on the buffer,
- Opens a file for writing (fopen),
- Writes the buffer into this file using fputs.
- Then closes the program.

It was assumed that the file being created was the data.txt file that was created earlier. Which means it must contain whatever data was encrypted.

Then, breakpoints were set for both functions to analyze their behaviors.

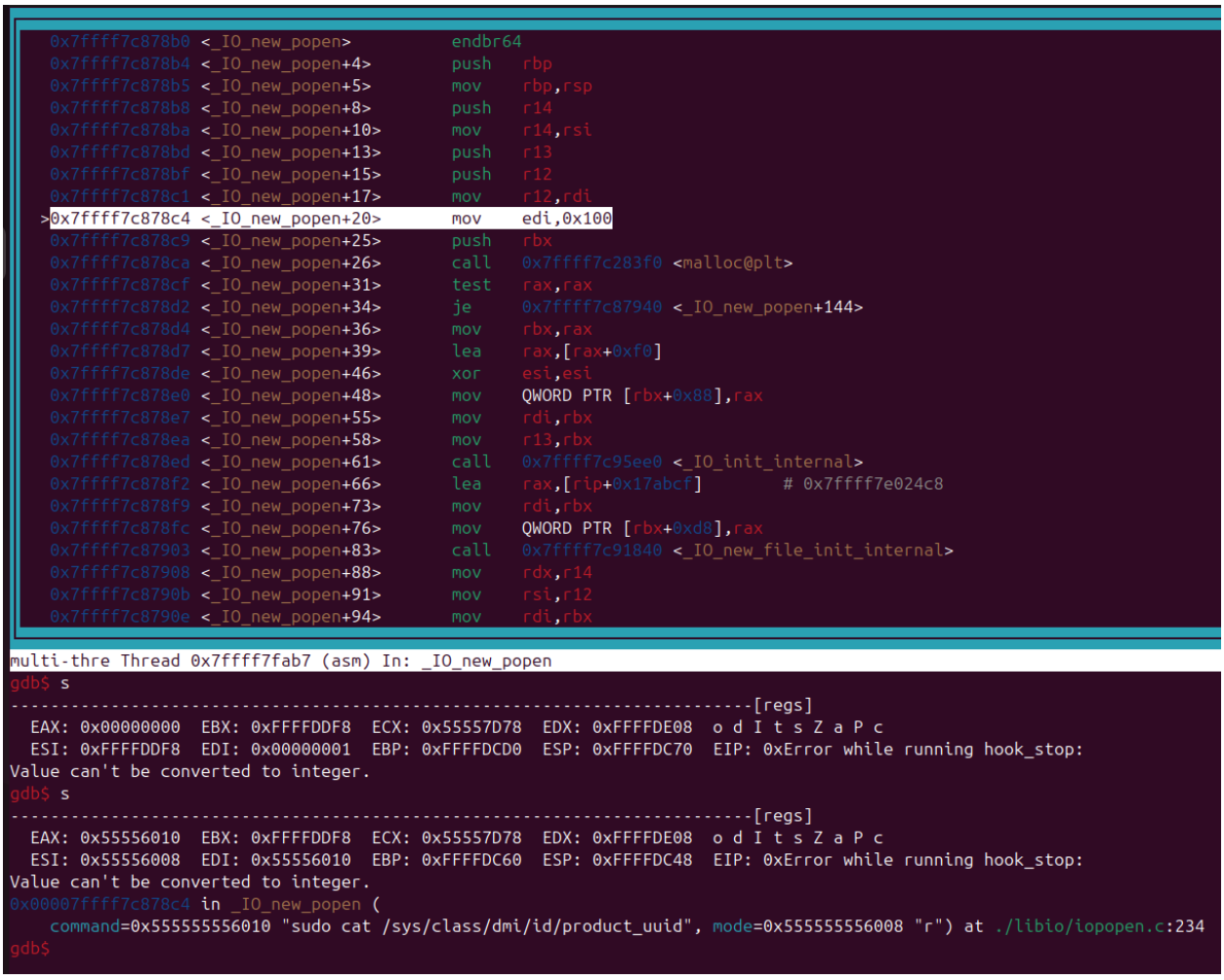
```
gdb$ break main

This GDB supports auto-downloading debuginfo from the following URLs:
  <https://debuginfod.ubuntu.com>
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.
Breakpoint 1 at 0x12fc: file [redacted].c, line 13.
gdb$ break xor_encrypt_decrypt
Breakpoint 2 at 0x127d: file [redacted].c, line 6.
gdb$
```

Then, the program was executed with the run command. As set it was stopped at the main function.

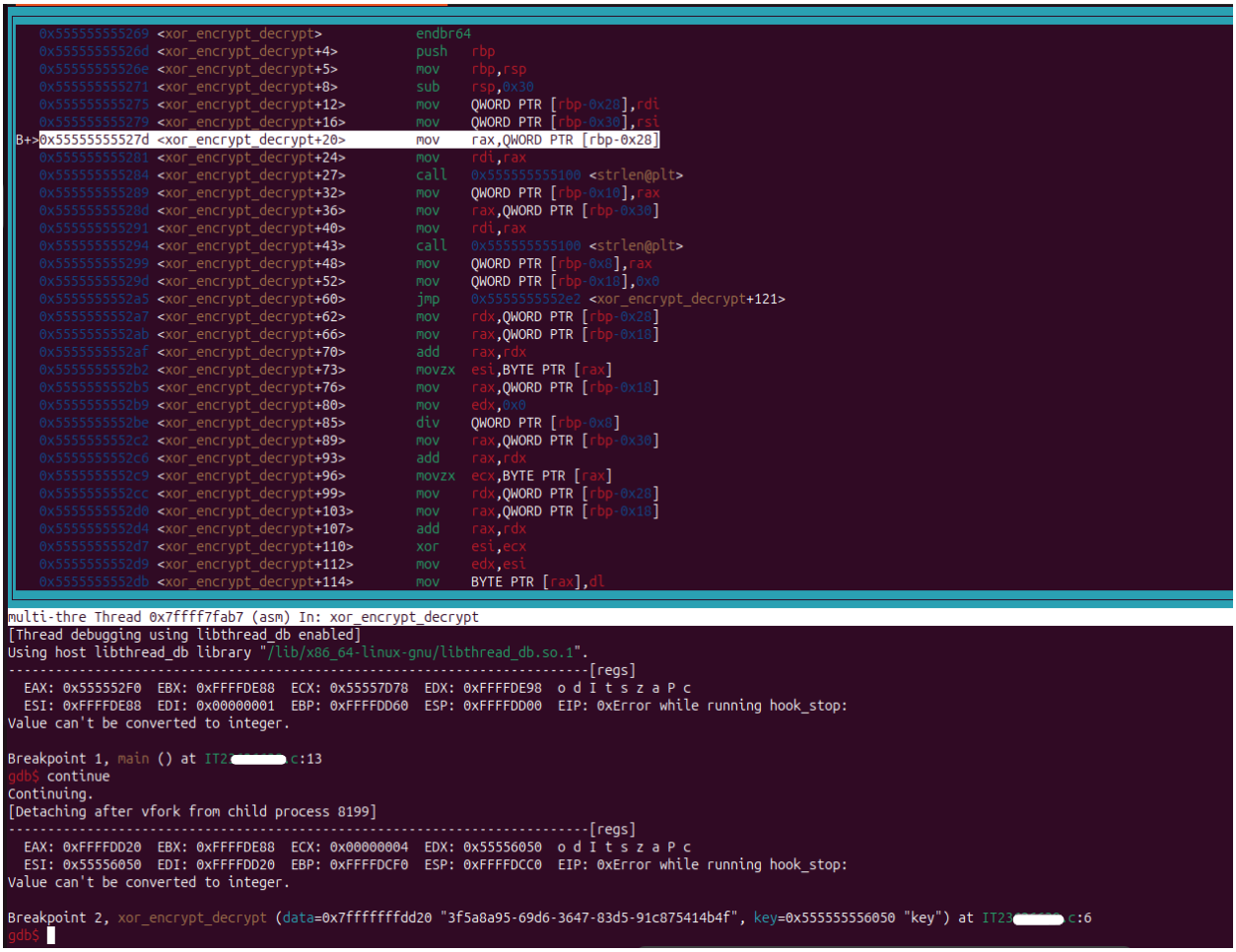
```
gdb$ run
Starting program: /home/pomod/Downloads/Executables/Executables/IT[redacted]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
--------------------------------------------------------------------------[regs]
  EAX: 0x555552F0  EBX: 0xFFFFDDD8  ECX: 0x55557D78  EDX: 0xFFFFDDE8  o d I t s z a P c
  ESI: 0xFFFFDDD8  EDI: 0x00000001  EBP: 0xFFFFDCB0  ESP: 0xFFFFDC50  EIP: 0xError while running hook_stop:
Value can't be converted to integer.

Breakpoint 1, main () at [redacted].c:13
warning: 13     [redacted].c: No such file or directory
gdb$ layout asm
```

Then **layout asm** was used to see the assembly code while the program was running.

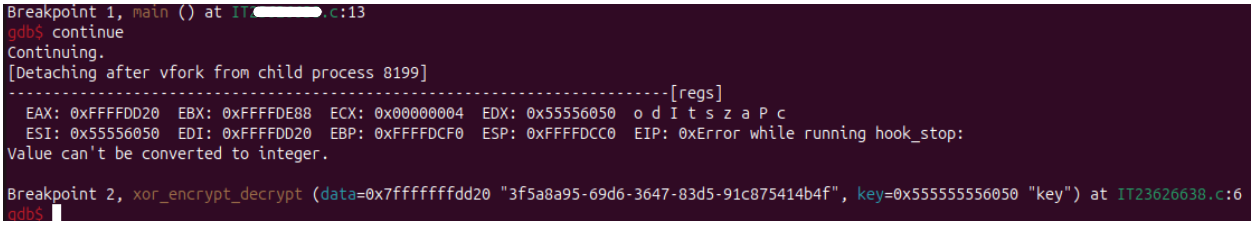
While using the **step** command, a command was shown to read a file. The program is about to execute the command "**sudo cat /sys/class/dmi/id/product_uuid**" using **popen**() in read mode. The assembly is part of the C library's implementation of popen, handling memory allocation.



After that **continue** command was given to continue the program until the next break point. The program stopped at the second breakpoint point which was set at the XOR function.

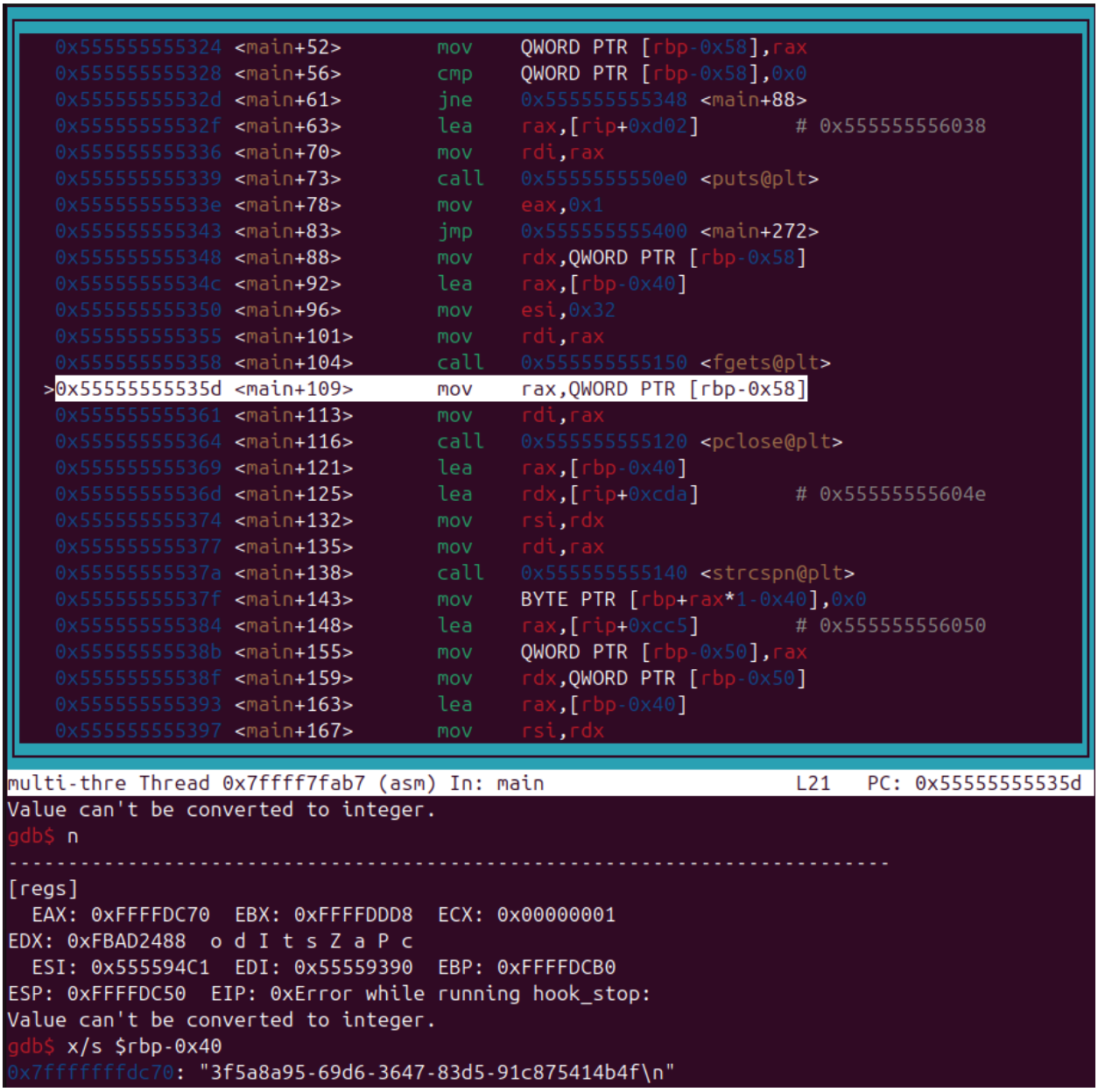


At the second breakpoint, it was noticed that two values were passed as parameters.



“3f5a8a95-69d6-3647-83d5-91c875414b4f ” value was passed as the first parameter and “key” was passed as the second parameter. Which means the first value must be encrypted by the “key” keyword and the result must be the output of the .txt file. It is safe to assume that the first value was taken from the file shown before, with the path.

The value was also caught while it was loading into the buffer.



So to conclude, the program reads a value from the discovered command, and then uses the value that is returned and a keyword to encrypt this value using the XOR function, and outputs the encrypted value to the data.txt file.

File System Analysis

The data.txt file was created because of the execution of the executable process. To ensure this **inotifywait** tool was used. By setting up a watch for the file and running the program a few times, it shows that the file was being modified by the program.

```
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$ inotifywait -m -e create,modify,delete  data.txt
Setting up watches.
Watches established.
data.txt MODIFY
data.txt MODIFY
```

Using the file command the type of content the file stores was discovered.

```
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$ file data.txt
data.txt: data
pomod@pomod-VirtualBox:~/Downloads/Executables/Executables$
```

The next step was to see the inside of the file using a text editor. To do that, the file needed a permission change.

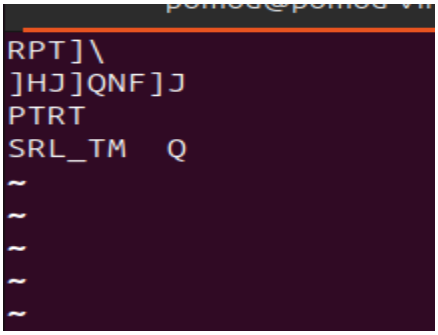
```
ecutables$ chmod 700 data.txt
ecutables$
```

Using the text editor nano, the file was opened.

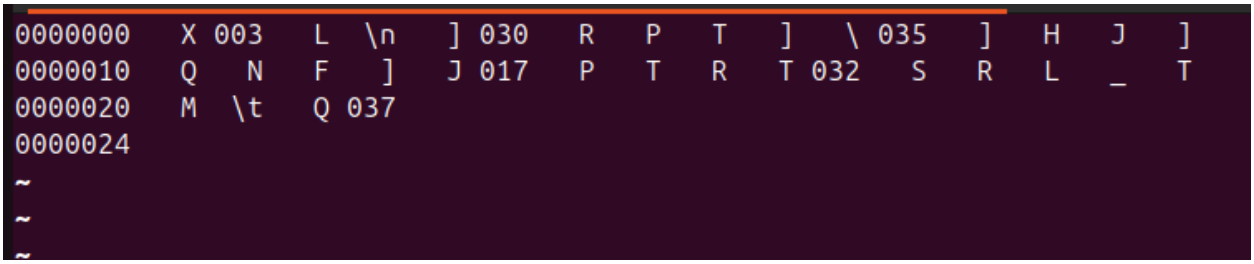
```
  GNU nano 7.2                                    data.txt
X^CL
]^XRPT]\^]]HJ]QNF]J^OPTRT^ZSRL_TM       Q^_
```

It was shown as some random data. Probably encrypted, since in the debugging part, it was discovered that the file might hold encrypted data. After a few executions of the IT numbered program, the values stayed the same.

The **string** command was also used to find any strings in the file. No hopeful result in that.



The **hexdump** command was also used to find meaningful content. But it displays the file byte-by-byte in ASCII, using escape sequences for non-printable characters.



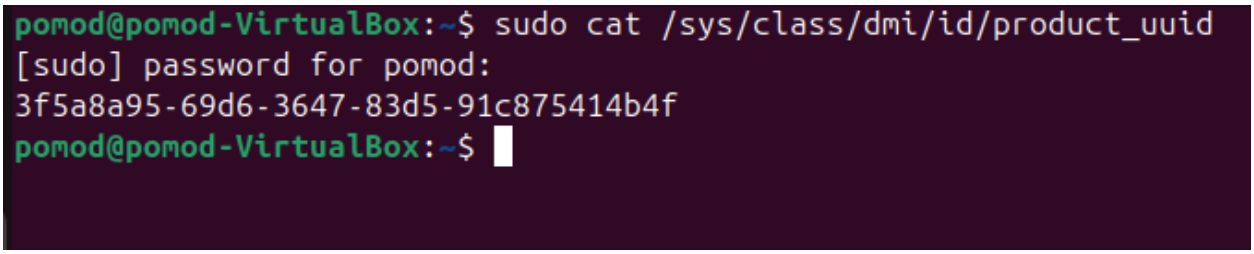
In the current state. It was impossible to get an idea about the content of the data.txt file. A decryption method was suggested to check whether it provided the original value that was discovered in the debugging part.

So, a C language program and a copy of the .txt file were used to decrypt the data.txt file.

```
  GNU nano 7.2
#include <stdio.h>
#include <stdlib.h>

void xor_encrypt_decrypt(unsigned char *data, size_t data_len, const unsigned char *key, size_t key_len) {
    for (size_t i = 0; i < data_len; i++) {
        data[i] ^= key[i % key_len];
    }
}

int main() {
    const char *filename = "data.txt";
    const char *output_filename = "decrypted.txt";
    const unsigned char key[] = "key";
    size_t key_len = sizeof(key) - 1; // exclude null terminator

    // Open input file in binary mode
    FILE *fp = fopen(filename, "rb");
    if (fp == NULL) {
        perror("Failed to open input file");
        return 1;
    }

    // Get file size
    fseek(fp, 0, SEEK_END);
    long file_size = ftell(fp);
    fseek(fp, 0, SEEK_SET);

    if (file_size <= 0) {
        fprintf(stderr, "Invalid file size\n");
        fclose(fp);
        return 1;
    }

    // Allocate buffer for file content
    unsigned char *buffer = malloc(file_size);
    if (buffer == NULL) {
        perror("Memory allocation failed");
        fclose(fp);
        return 1;
    }

    // Read file content
    if (fread(buffer, 1, file_size, fp) != file_size) {
        perror("Failed to read file");
        free(buffer);
        fclose(fp);
        return 1;
    }
    fclose(fp);

    // Decrypt data
    xor_encrypt_decrypt(buffer, file_size, key, key_len);

    // Write decrypted data to output file
    FILE *out_fp = fopen(output_filename, "wb");
    if (out_fp == NULL) {
        perror("Failed to open output file");
        free(buffer);
        return 1;
    }

    if (fwrite(buffer, 1, file_size, out_fp) != file_size) {
        perror("Failed to write output file");
        free(buffer);
        fclose(out_fp);
        return 1;
    }

    printf("Decryption completed. Output saved to '%s'\n", output_filename);

    free(buffer);
    fclose(out_fp);

    return 0;
}
```

The resulting decrypted.txt shows the following value.

This value matches with value that was discovered in the debugging part. To further assure that, the command that was found while debugging part was also executed to get the result.



This confirms that the data.txt file is the result of the executable program and that it contains the XOR-encrypted value of the discovered value.

END.