

# Configuration Manual

MSc Research Project

Cybersecurity

Regin Raghavan Nair

Student ID: X21173281

School of Computing

National College of Ireland

Supervisor: Evgeniia Jayasekera

**National College of Ireland**  
**MSc Project Submission Sheet**



**School of Computing**

**Student Name:** Regin Raghavan Nair  
**Student ID:** X21173281  
**Programme:** MSc Cybersecurity **Year:** 2023  
**Module:** MSc Research Project  
**Supervisor:** Evgeniia Jayasekera  
**Submission Due Date:** 14 August 2023  
**Project Title:** Data Security at Cloud Storage using PGP in conjunction with IPsec VPN  
**Word Count:** 1595 **Page Count:** 13

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** Regin Raghavan Nair

**Date:** 12 August 2023

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission,</b> to each project (including multiple copies).	<input type="checkbox"/>
<b>You must ensure that you retain a HARD COPY of the project,</b> both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# Configuration Manual

Regin Raghavan Nair

Student ID: 21173281

## Configuration Manual

This Document provide detailed instructions about the components that are needed , an the respective configuration that needs to me done in order to recreate the project environment in another machine . The project has two major software components called the GNS3 Application that helps simulating the project environment using the GNS3VM. The GNS3 VM is hosted on VMware Workstation Pro 16. The Detailed descriptions will be given in the following sections.

### Physical Machine Configurations.

The physical machine on which the entire set up was built is a HP Gaming Machine with the following Configuration.

System Configuration	
Operating system	Microsoft Windows 11 Home Single Language/64bit
Processor	AMD Ryzen 5 3550H- 2100 Mhz, 4 Core(s), 8 Logical Processor(s)
Ram	16 GB
Virtual Memory	9.45 GB
Graphics card	4GB
Virtualization	Enabled at Bios

The following stages discuss about installation and configuration of software components needed for this project.

### GNS3:

GNS3 tools is used to simulate the devices such as routers, firewalls, server and other infrastructure devices , to be tested and evaluated in a sandbox environment. The latest version of GNS3 2.2.41 is installed on the machine.

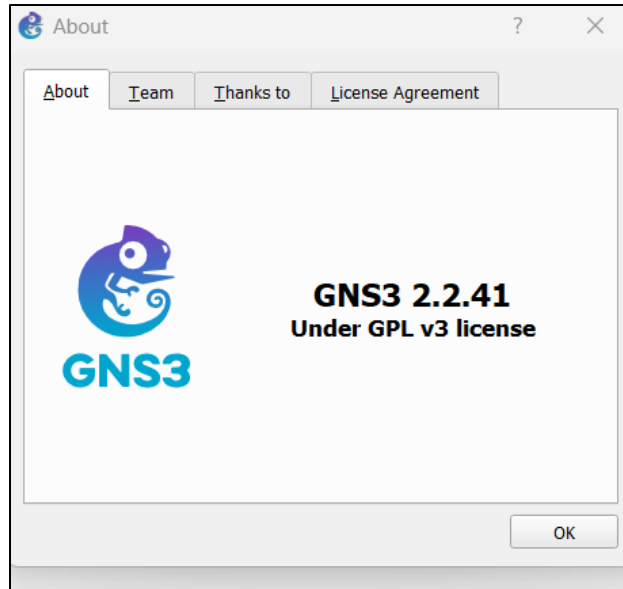


Figure 1 GNS3 version

[Gns3 installation guide](#) form the GNS3 can be found in the official gns3 website(*GNS3 Windows Install | GNS3 Documentation*, no date).

### VMware Workstation Pro:

VMware Workstation Pro, developed by VMware, Inc., empowers users to generate and oversee numerous virtual machines (VMs) on a solitary physical computer. The version used here is the 16.2.4.

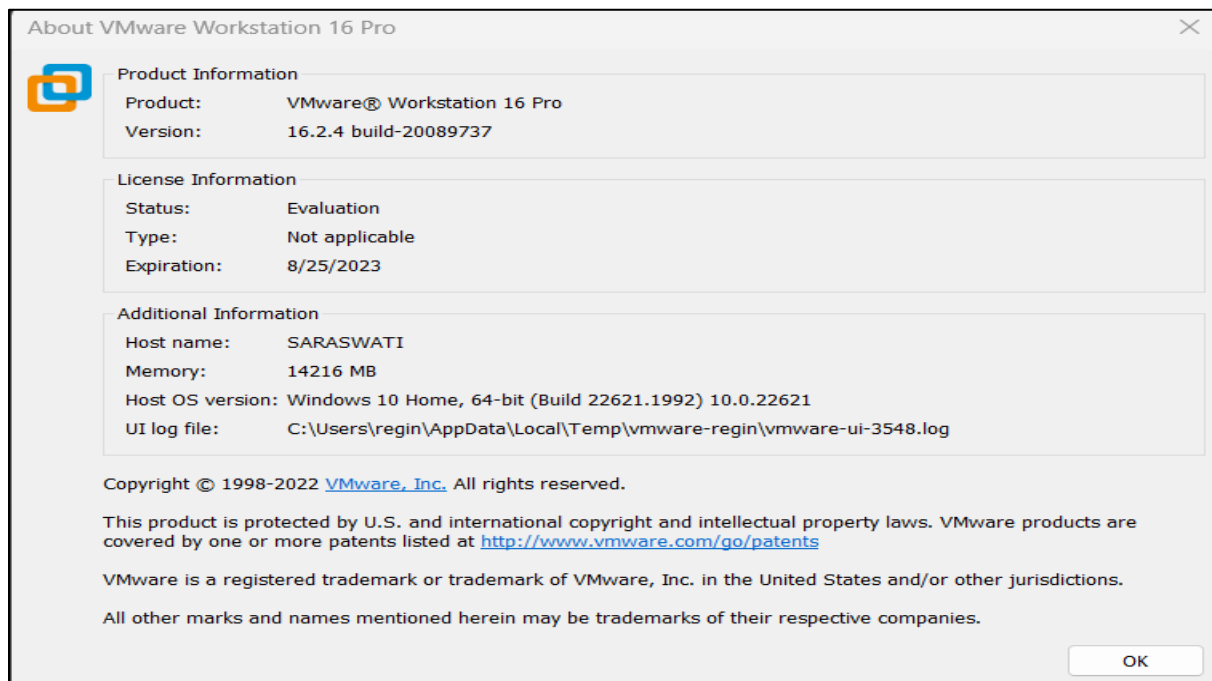


Figure 2 VMware Workstation Version.

The installation guide for VMware workstation pro can be found in the official website(*Install Workstation Pro on a Windows Host*, no date) [[Guide](#)].

## GNS3 VM installation:

### Step 1:

Download the GNS3 VM from the GNS3 official website's download section. Once you click on the download VM option at the bottom of the page, select the hypervisor for which the VM needs to be downloaded, which in our case is a the VMware workstation. This would down load a ".OVA " file.

### Step 2:

Utilizing VMware Workstation as your hypervisor, move forward with importing the previously downloaded GNS3 VM image. Launch VMware Workstation, access the "File" menu, proceed to "Open," and opt for the downloaded GNS3 VM OVA file. Subsequently, adhere to the instructions displayed on-screen to effortlessly finalize the import procedure. The final screen after installation is as shown below(*GNS3 Windows Install | GNS3 Documentation*, no date).

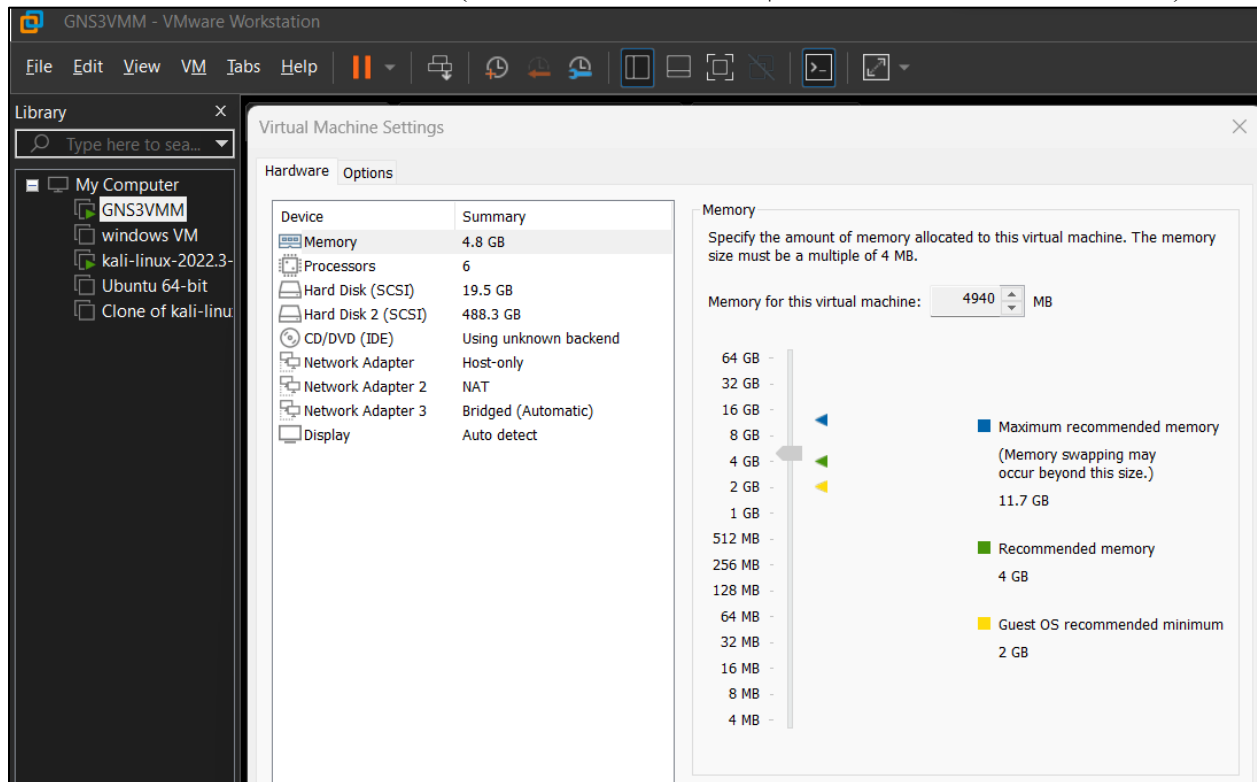


Figure 3 GNSVM installation

### Step 3:

Once the GNS3 application and the GNS3 VM is installed, the next step is to link the GNS3 Application with GNS3VM. Upon launching GNS3 for the first time, you'll encounter the GNS3 Setup Wizard. Alternatively, you can manually initiate the Setup Wizard by clicking Help > Setup Wizard within the GNS3 application. In the Wizard, opt for 'Run appliances in a Virtual machines' and proceed by clicking 'Next':

### Step 4:

Prior to advancing with the remaining GNS3-VM configuration steps, it is imperative to set up the local server settings in GNS3. Confirm the accuracy of the gns3server executable path (typically C:\Program Files\GNS3 in a default installation) and select a Host binding and Port. Opting for the 127.0.0.1 local loopback address generally proves to be the most seamless host binding option.

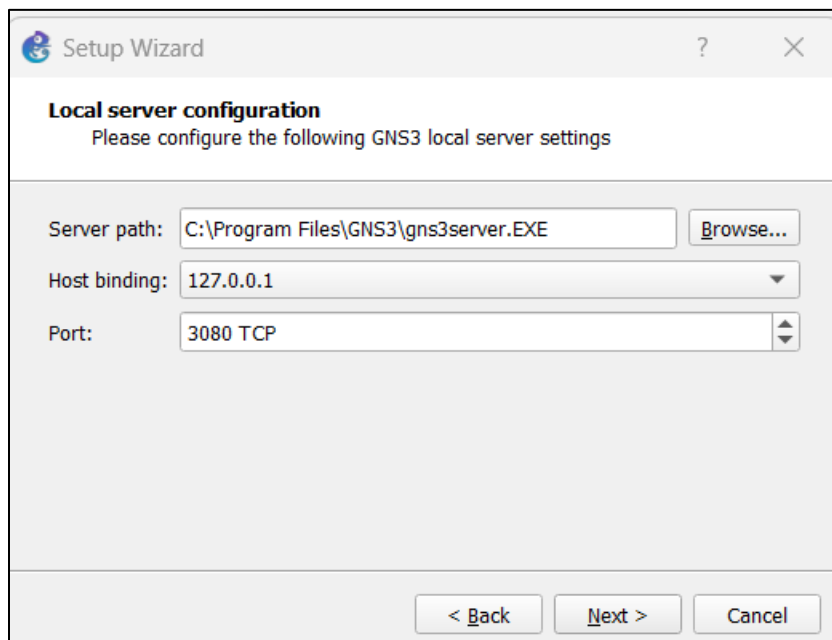


Figure 4 GNS3 Set up wizard 1

### Step 5:

The Setup Wizard will automatically detect the presence of the GNS3 VM within VMware Workstation. If the GNS3 VM doesn't appear, utilize the 'Refresh' button and double-check the accurate import of the VM into VMware Workstation. Modify the vCPU cores and RAM values based on your computer's capacity, and then proceed by clicking 'Next'.

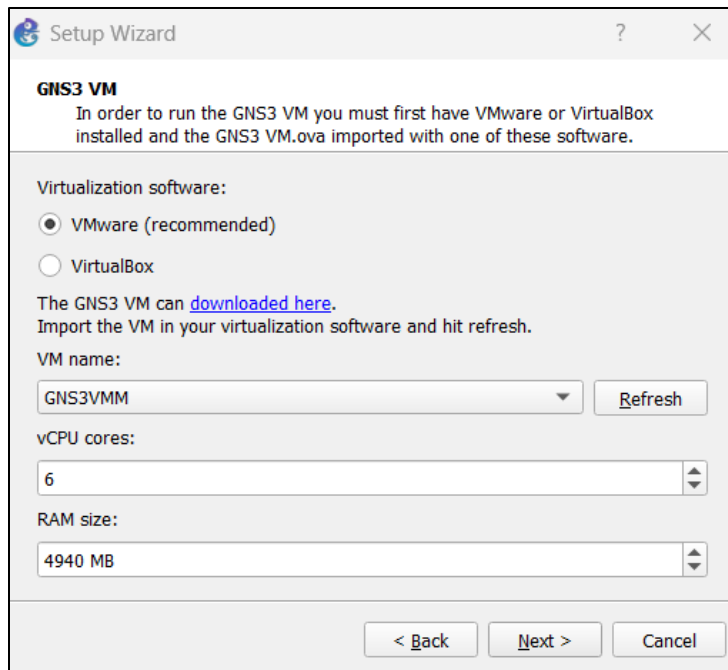


Figure 5 GNS3 setup wizard 2

## Step 6:

The following page will present a summary of the chosen settings for the GNS3 VM. It's possible that a "Please Wait" notification may pop up. This occurrence is entirely normal, as GNS3 is in the process of initializing the GNS3 VM. The subsequent page will reiterate the summary of the selected GNS3 VM settings. Should you observe a "Please Wait" pop-up, it is customary, reflecting GNS3's process of launching the GNS3 VM. Post installation the tool looks as shown below(*GNS3 integration with GNS3 VM | GNS3 Documentation, no date*).

```
GNS3 server version: 2.2.41
Release channel: 2.2
VM version: 0.15.0
Ubuntu version: focal
Qemu version: 4.2.1
Virtualization: vmware
KVM support available: True
Uptime: up 0 minutes

IP: 192.168.159.128 PORT: 80

To log in using SSH: ssh gns3@192.168.159.128
Password: gns3

To launch the Web-Ui: http://192.168.159.128

Images and projects are stored in '/opt/gns3'
```

Figure 6 GNS3 VM successful integration

## Import Appliance to GNS3 (Router)

Navigate to Edit > Preferences > IOS Routers to access the appropriate section. In the New IOS router template window, opt for running the IOS router on the GNS3 VM and proceed by clicking 'Next'.

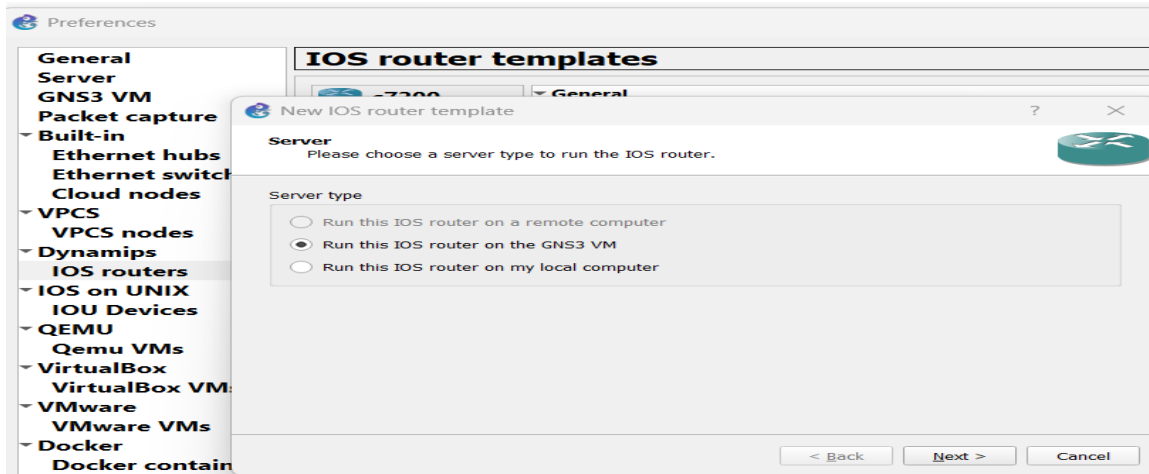


Figure 7 Adding IOS image

Locate the directory where your Cisco IOS images are stored. Select the desired image and press 'Open'. This is recommended for an improved user experience, as decompressing the IOS image can take a few minutes, even on physical hardware. Click 'Yes' to initiate image decompression.

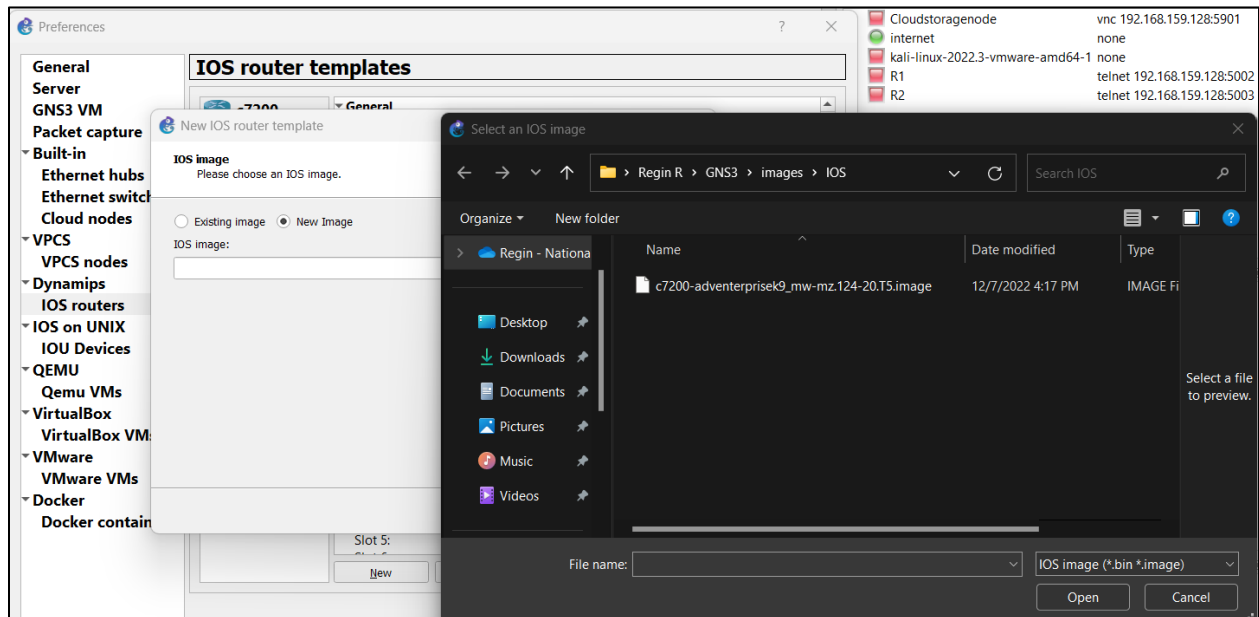


Figure 8 Image import 2

The Name and platform window will emerge. Verify the Platform choice, define the router Name as needed, and then click 'Next'. A Default RAM setting will be displayed. Ensure you review your Router's minimum memory prerequisites using the Vendor website.



opt for your preferred Network adapters and proceed to the next step. It's crucial for optimal GNS3 performance to select an Idle-PC value. If a valid green Idle-PC value isn't shown, click the 'Idle-PC finder' button to identify one. Once the Idle-PC value is generated, click 'Finish' to conclude the GNS3 Setup Wizard.

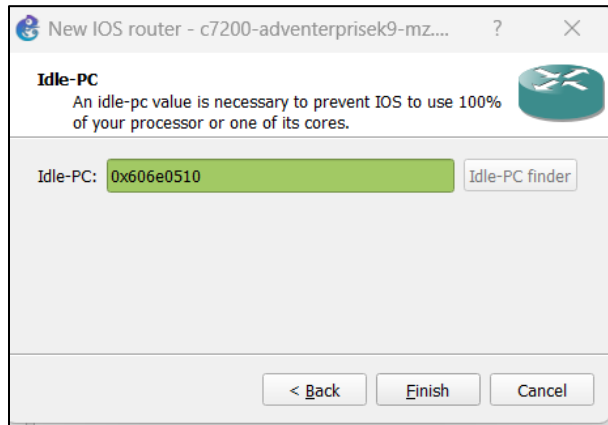


Figure 9 Idle PC value

The newly added device is now accessible within the GNS3 Dynamips Section(*GNS3 integration with GNS3 VM | GNS3 Documentation*, no date).

### **Kali VM import.**

Import kali VM into the VMware workstation using the Guide provided by kali.org (*Import Pre-Made Kali VMware VM | Kali Linux Documentation*, no date). Steps are similar to ones performed to import the GNS3 “.OVA” file. Once successfully imported configure Ram , network interfaces, and CPU cores for the VM. The configuration on kali VM used for this project is as shown below.

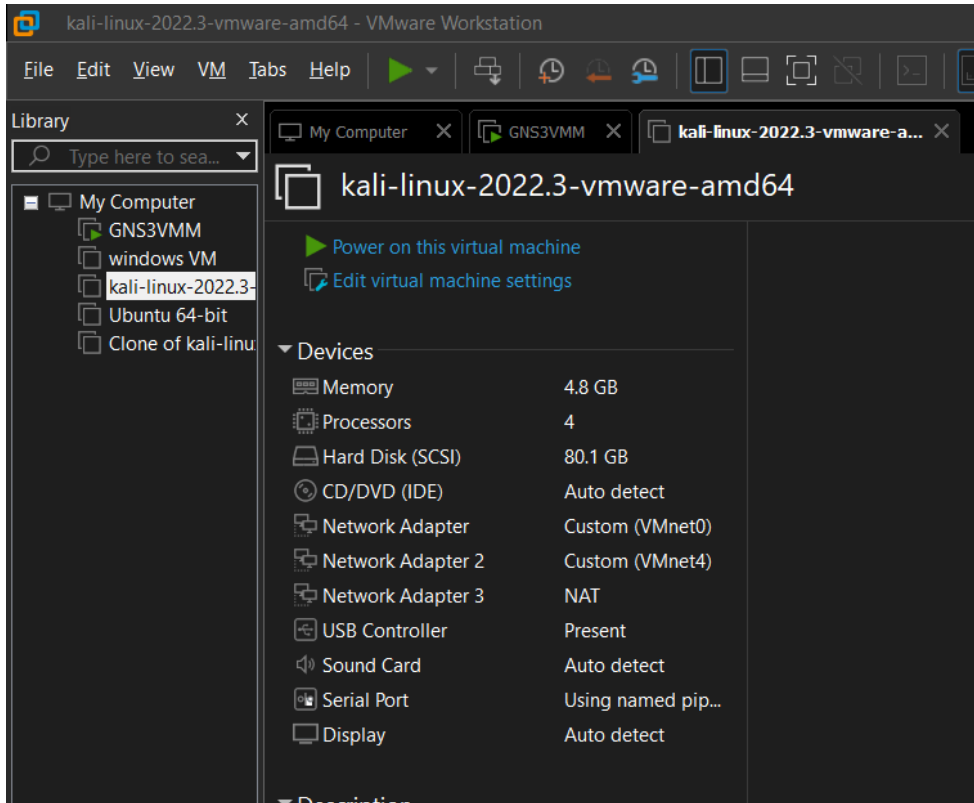


Figure 10 Kali VM Configuration

Import the Kali VM and into GNS3 following the steps similar to how the GNS3VM was integrated with GNS3 application. Post which kali VM should be available for use as in figure below.

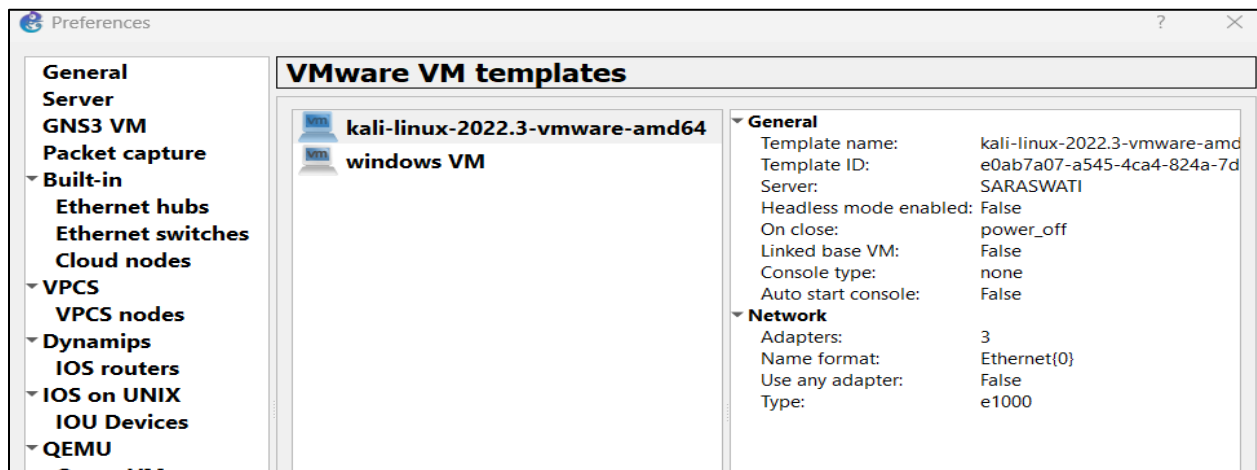


Figure 11 Kali VM in GNS3

Once all the nodes are imported and start the GNS3 application, the application show a green notification showing the utilization on resources on physical machine and the VM, this is the proof of successful installation of all the software components.

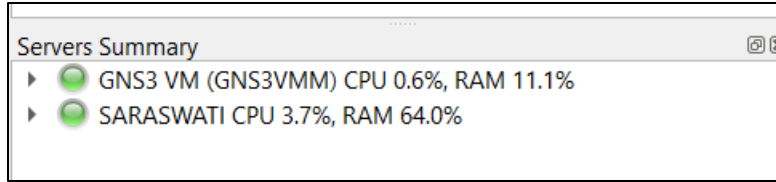


Figure 12 Successful installation

Once all the devices are imported and the nodes are connected to appropriate interface as shown in the figure, the Ip addresses need to be configured to each node as shown in the table below.

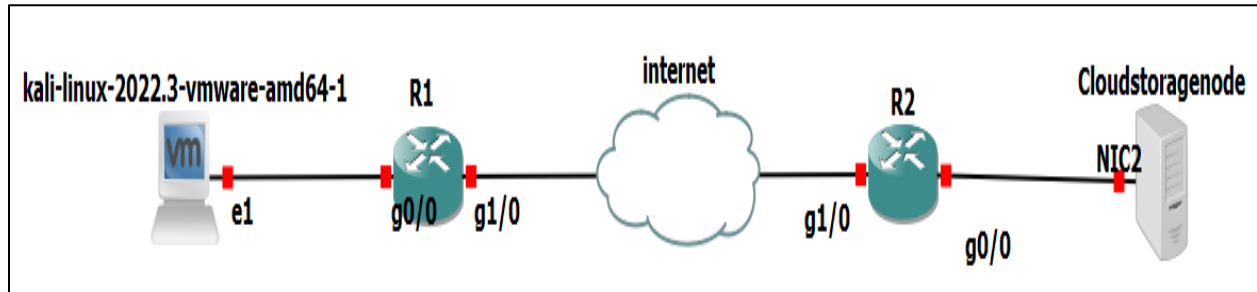


Figure 13 Infrastructure design

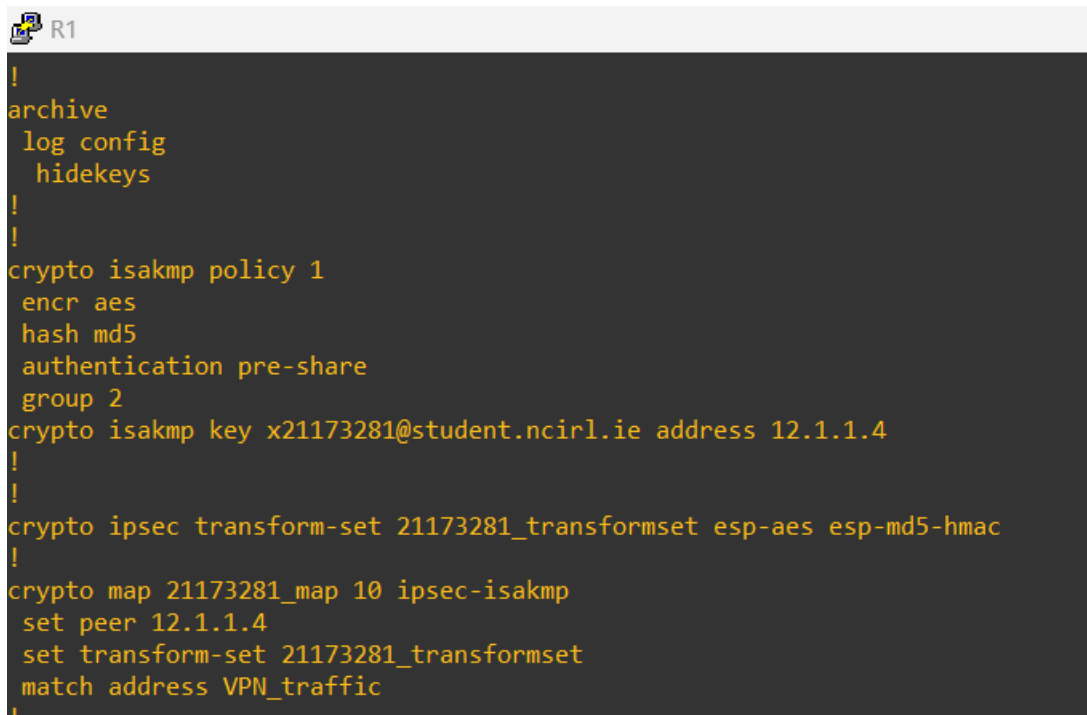
The IP address allocation to each node is as shown below.

Table 1 Ip address Details

kali-linux-2022.3-vmware-amd64-1(FOG node)Eth1 :	12.10.1.2/24
Gigabit ethernet 0/0,on router R1 connecting to linux machine(FOG).	12.10.1.2/24
Gigabit ethernet 1/0,on router R1 connecting to Gigabit ethernet 1/0,on router R2 of cloud network:	12.1.1.2/24
Gigabit ethernet 1/0,on router R2 connecting to Gigabit ethernet 1/0,on router R1 of FOG network:	12.1.1.4/24
Gigabit ethernet 0/0,on router R2 connecting to Windows machine(Cloud Storage).	12.10.2.4/24
Windows Cloudstoragenode (Nic2) :	12.10.2.2/24

Once all the running configuration for R1 and R2 provided in the artifacts are imported into R1 and R2 are imported and after configuring the IP details on the Kali Linux node and Windows VM network interfaces, we should be able to ping successfully to each node from both directions verifying connectivity and routing to be in place. The Configuration of VPN is also included in the configurations.

The devices were fully configured during the building phase of the project and running configuration were exported so that it can be imported easily into another devices if needs to be tested on another machine. the scree shot of configuration from the device is as shown below.

A screenshot of a terminal window titled 'R1' showing the configuration of a VPN on a Cisco router. The configuration includes enabling logging for configuration and keys, setting an ISAKMP policy with AES encryption, MD5 hashing, and pre-share authentication, generating an ISAKMP key, creating an IPsec transform set with AES and MD5-HMAC, and finally creating a crypto map to apply the IPsec transform set to VPN traffic.

```
R1
!
archive
 log config
  hidekeys
!
!
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
crypto isakmp key x21173281@student.ncirl.ie address 12.1.1.4
!
!
crypto ipsec transform-set 21173281_transformset esp-aes esp-md5-hmac
!
crypto map 21173281_map 10 ipsec-isakmp
 set peer 12.1.1.4
 set transform-set 21173281_transformset
 match address VPN_traffic
!
```

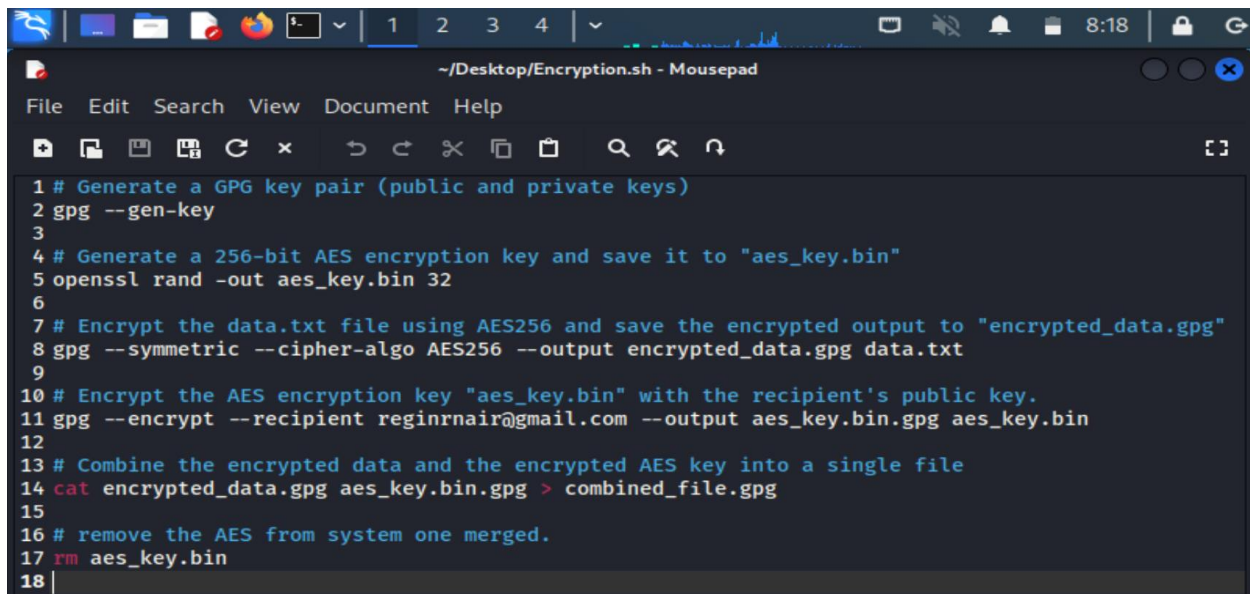
Figure 14 Section of VPN configuration on router R1.

Once all configuration and end to end connection is verified, we can proceed with testing the environment. The first step begins with taking plaintext data and perform hybrid encryption.

The commands that was followed to perform encryption is as shown in the figure below. Steps take a sequence of

- AES key generation,
- Public and Private key generation,
- Encryption of data by AES,
- Encryption of AES key by using RSA
- Merging of both encrypted data and certificate.

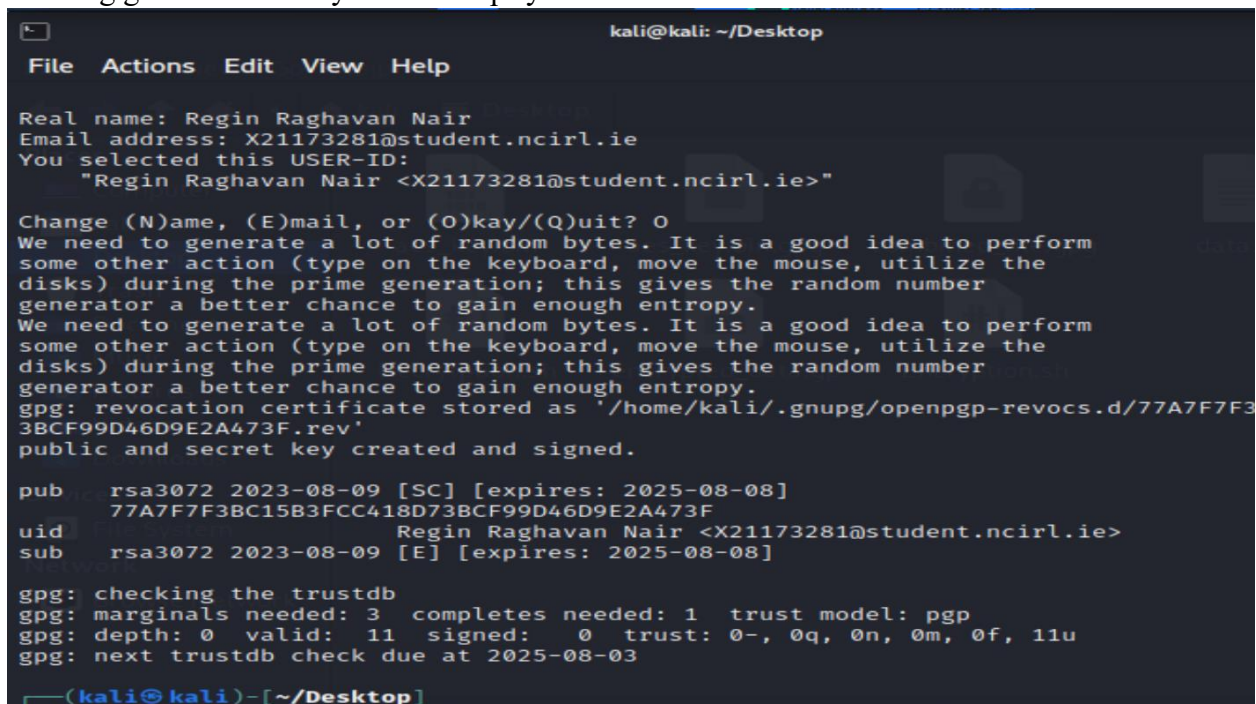
**Note:** During the process of key generation the GNUPG would prompt to enter a passphrase for additional security, this password is used to protect the private key which will be used to decrypt the data.



```
~/Desktop/Encryption.sh - Mousepad
File Edit Search View Document Help
1 # Generate a GPG key pair (public and private keys)
2 gpg --gen-key
3
4 # Generate a 256-bit AES encryption key and save it to "aes_key.bin"
5 openssl rand -out aes_key.bin 32
6
7 # Encrypt the data.txt file using AES256 and save the encrypted output to "encrypted_data.gpg"
8 gpg --symmetric --cipher-algo AES256 --output encrypted_data.gpg data.txt
9
10 # Encrypt the AES encryption key "aes_key.bin" with the recipient's public key.
11 gpg --encrypt --recipient reginrnair@gmail.com --output aes_key.bin.gpg aes_key.bin
12
13 # Combine the encrypted data and the encrypted AES key into a single file
14 cat encrypted_data.gpg aes_key.bin.gpg > combined_file.gpg
15
16 # remove the AES from system one merged.
17 rm aes_key.bin
18 |
```

Figure 15 Encryption Configuration

Once encryption is done, we can see that the AES key, private and public keys are generated, along with the encrypted files. Below screenshot shows logs on the kali terminal windows showing generation of keys and its expiry.



```
kali@kali: ~/Desktop
File Actions Edit View Help
Real name: Regin Raghavan Nair
Email address: X21173281@student.ncirl.ie
You selected this USER-ID:
  "Regin Raghavan Nair <X21173281@student.ncirl.ie>"
Change (N)ame, (E)mail, or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/77A7F7F3
3BCF99D46D9E2A473F.rev'
public and secret key created and signed.

pub   rsa3072 2023-08-09 [SC] [expires: 2025-08-08]
      77A7F7F3BC15B3FCC418D73BCF99D46D9E2A473F
uid           Regin Raghavan Nair <X21173281@student.ncirl.ie>
sub   rsa3072 2023-08-09 [E] [expires: 2025-08-08]

gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid: 11  signed: 0  trust: 0-, 0q, 0n, 0m, 0f, 11u
gpg: next trustdb check due at 2025-08-03

(kali@kali)-[~/Desktop]
```

Figure 16 encryption logs

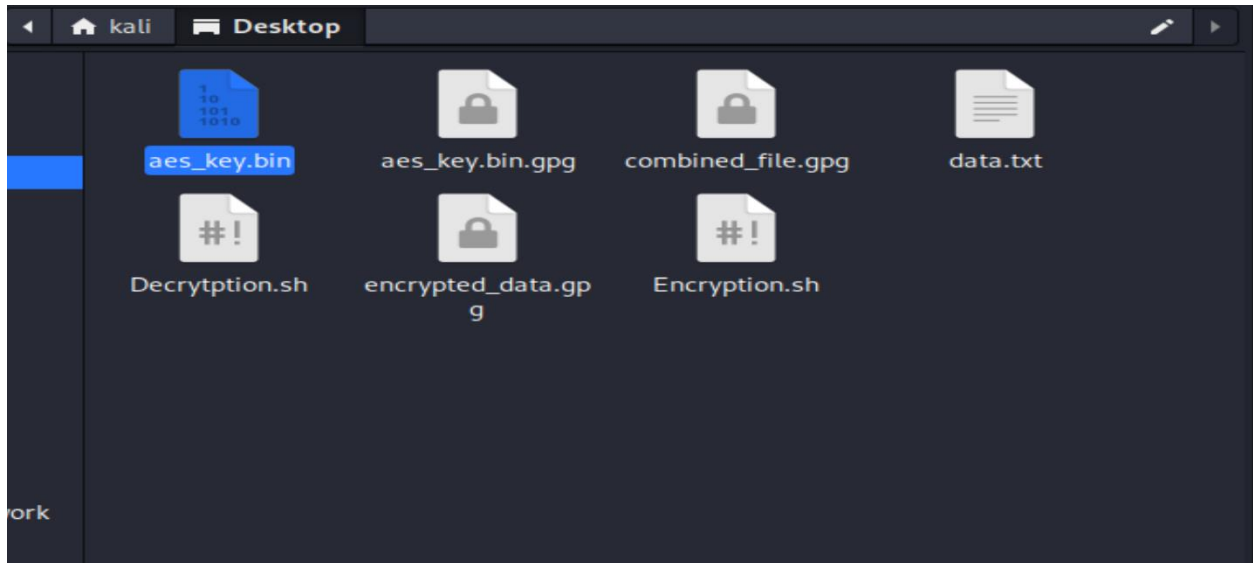


Figure 17 encrypted files and keys

The screen shot below shows the scrambled content when we try opening the encrypted file using “cat” command in liux.

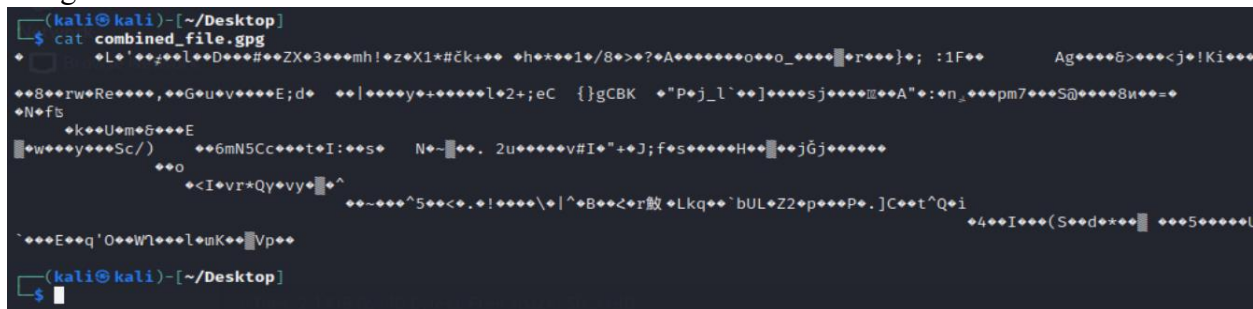


Figure 18 Encrypted data

Once the file is encrypted, we can send the file to the cloud storage system using FTP or SFTP .

Similarly, the decryption process can be carried out by using the commands below. The GNUPG will prompt for password during the decryption process, use the password that was used to secure the private key to decrypt data.

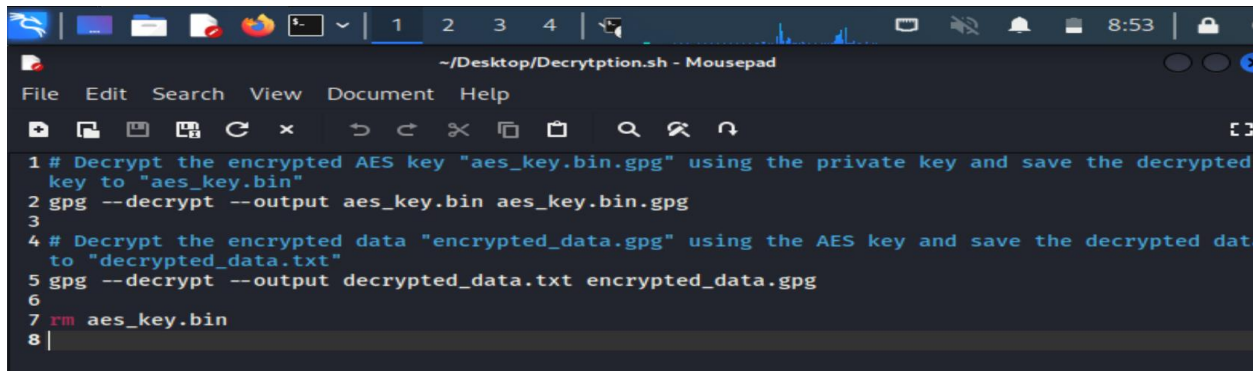


Figure 19 Decryption steps

```
(kali@kali)-[~/Desktop]
└─$ ./Decryption.sh
gpg: encrypted with 3072-bit RSA key, ID 01E769F8958E5A4D, created 2023-08-09
"regin <reginrnair@gmail.com>"
File 'aes_key.bin' exists. Overwrite? (y/N) y
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase

(kali@kali)-[~/Desktop]
└─$ cat decrypted_data.txt
Name Regin Raghavan nair
Student id: 21173281
ph: 123456789
pps: 12345pps1

(kali@kali)-[~/Desktop]
└─$
```

Figure 20 Decrypted data

## References.

*GNS3 integration with GNS3 VM | GNS3 Documentation* (no date). Available at: <https://docs.gns3.com/docs/getting-started/setup-wizard-gns3-vm/> (Accessed: 8 August 2023).

*GNS3 Windows Install | GNS3 Documentation* (no date). Available at: <https://docs.gns3.com/docs/getting-started/installation/windows/> (Accessed: 8 August 2023).

*Import Pre-Made Kali VMware VM | Kali Linux Documentation* (no date). Available at: <https://www.kali.org/docs/virtualization/import-premade-vmware/> (Accessed: 9 August 2023).

*Install Workstation Pro on a Windows Host* (no date). Available at: <https://docs.vmware.com/en/VMware-Workstation-Pro/17/com.vmware.ws.using.doc/GUID-F5A7B3CB-9141-458B-A256-E0C3EA805AAA.html> (Accessed: 8 August 2023).