National College of Ireland

Enhancing Security Measures for Virtual Machine Monitor (VMM) Insertion in Virtualization Environments

MSc Research Project
Cyber Security

SIVA SANKAR SENTHIL KUMAR
Student ID: 22237640

School of Computing
National College of Ireland

Supervisor: Prof. Jawad Salahuddin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: SIVA SANKAR SENTHIL KUMAR

Student ID: 22237640

Programme: MSc in Cyber Security **Year:** 2023 - 2024

Module: MSc Research Project

Supervisor: Jawad Salahuddin

Submission Due Date: 12-08-2024

Project Title: Enhancing Security Measures for Virtual Machine Monitor (VMM) Insertion in Virtualization Environments

Word Count: 642 **Page Count**: 10

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: Siva Sankar S ...

Date: 12-08-2024 ...

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

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

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

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

SIVA SANKAR SENTHIL KUMAR

22237640

1. Introduction

This configuration manual will contain steps for implementing and deploying the project titled “Enhancing Security Measures for Virtual Machine Monitor (VMM) Insertion in Virtualization Environments”. Here are the guidelines for development and testing of the security measures featured in this report. It is intended to help users to identify the appropriate hardware and software components required in reproducing and verifying the outcomes of the report. The manual contains information on system and software requirements, configurations for virtual machine instances and security testing approaches.

2. System Specification

The following system specifications are required for the research,

- Processor: AMD Ryzen 5-5600H
- RAM: 16 GB
- Storage: 512 SSD
- System Type: 64-bit Operating System
- Operating System: Windows 11

3. Software Specifications

To implement the project, the following software components must be installed:

Virtualization Platform: Oracle VirtualBox - version 7.0.10

Operating Systems:

- Kali Linux - version 2024.2 (for hosting the virtualized environment and as the target VM also conducting phishing and rootkit attacks)

Security Tools and Utilities:

- Pyphisher (for phishing simulation)
- Social Engineering Toolkit (SET) (for phishing email generation)
- Diamorphine Rootkit (for rootkit demonstration)
- Python (for scripting and automation)

4. Steps for Configuration of Virtual Machines and Security Tools

4.1. Setting Up Virtual Machines

Download and Install Oracle VirtualBox:

- Visit the Oracle VirtualBox website and download the latest version compatible with your operating system.
- Follow the installation wizard to complete the setup.

Create Virtual Machines:

- Open Oracle VirtualBox and create two virtual machines: one for Host VM (attacker) and one for User VM (victim).

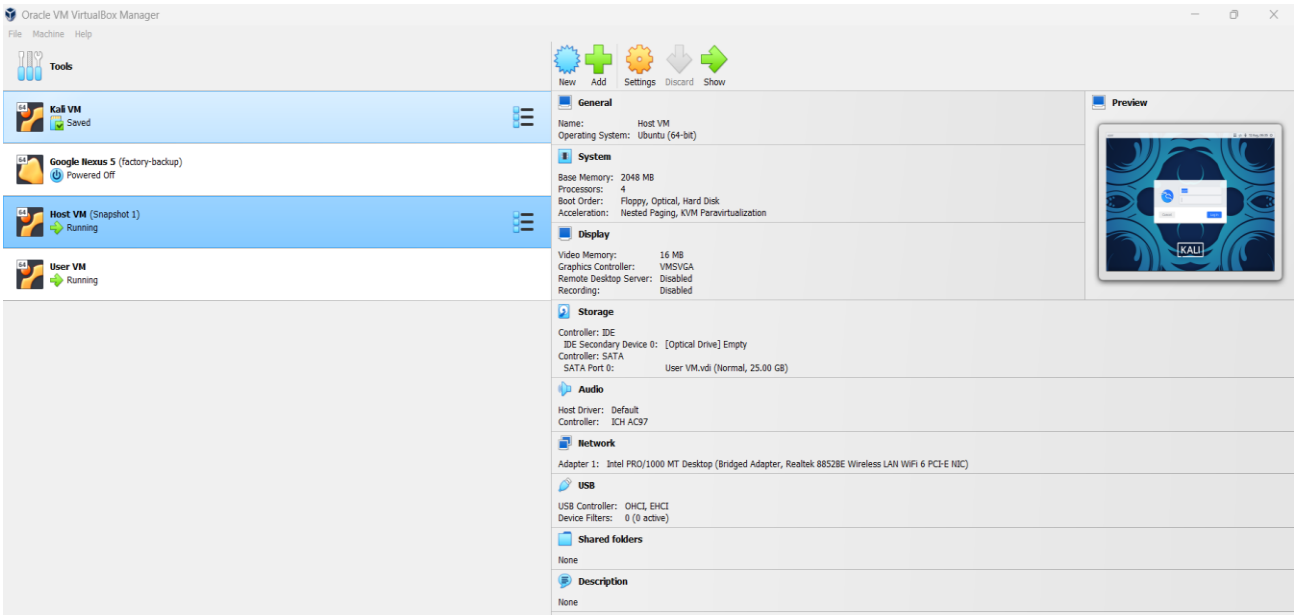

Figure 1: Oracle VirtualBox and VMs

- Configure both VMs to use a "Bridged Adapter" network setting to simulate a local network environment.

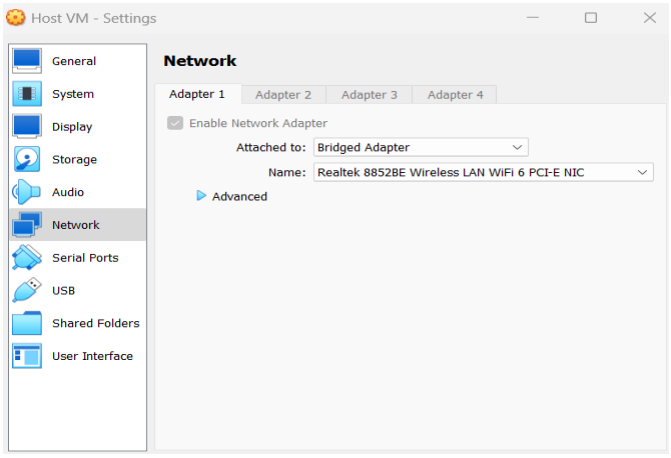

Figure 2: Host VM Network Settings

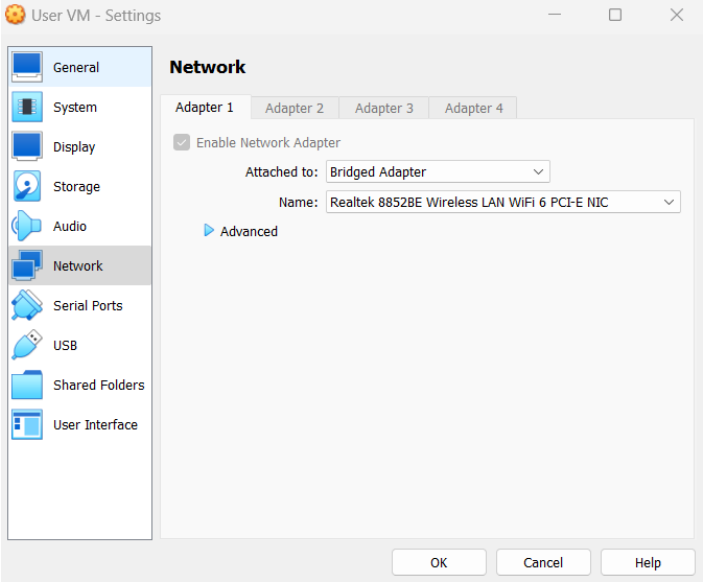

Figure 3: User VM Network Settings

Install Kali Linux Operating Systems:

- Download the Kali Linux ISO from the official website.
- Attach the ISO to the Kali VM and follow the installation instructions.

4.2. Configuring Security Tools

Phishing Simulation:

- Download the Pyphisher tool from its Github repository.
- Follow the setup instructions provided in the repository to install and configure Pyphisher.

Social Engineering Toolkit (SET):

- Use SET to craft and send phishing emails with fake login links.

Install Diamorphine Rootkit:

- Obtain the Diamorphine rootkit from a Github repository.
- Follow the installation guide provided with the rootkit to deploy it on the User VM.
- Use the rootkit to hide processes and files

Image Metadata Manipulation:

- Create a Python script using the PIL (Python Imaging Library) and ExifRead libraries to modify image metadata.
- Test the script on sample images to ensure it can modify data in metadata fields.

5. Procedure for Security Testing

5.1. Phishing Attack Simulation

- Run Pyphisher on the host VM and configure it with various fake website templates.

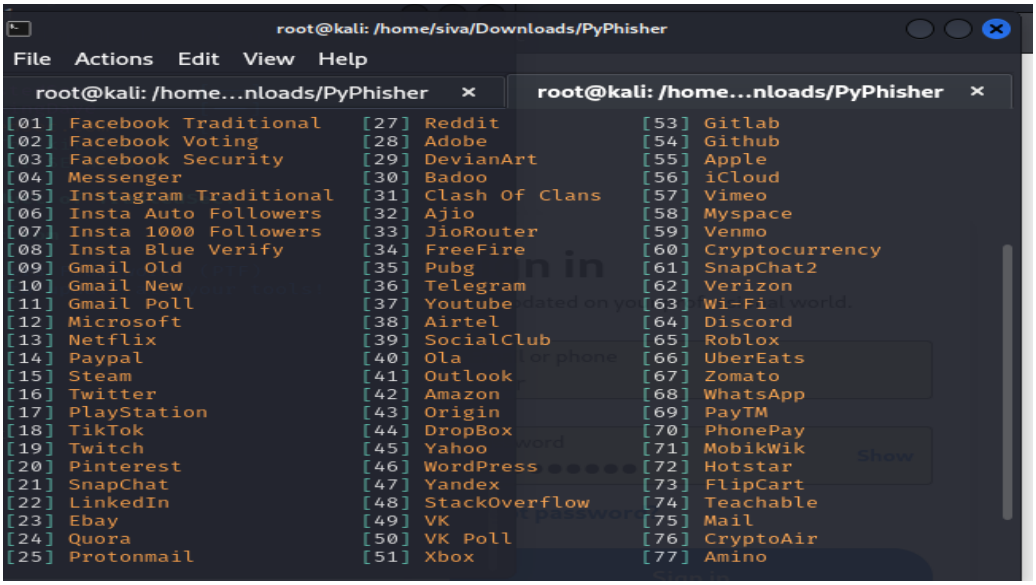

Figure 4: Pyphisher Fake Website Platforms

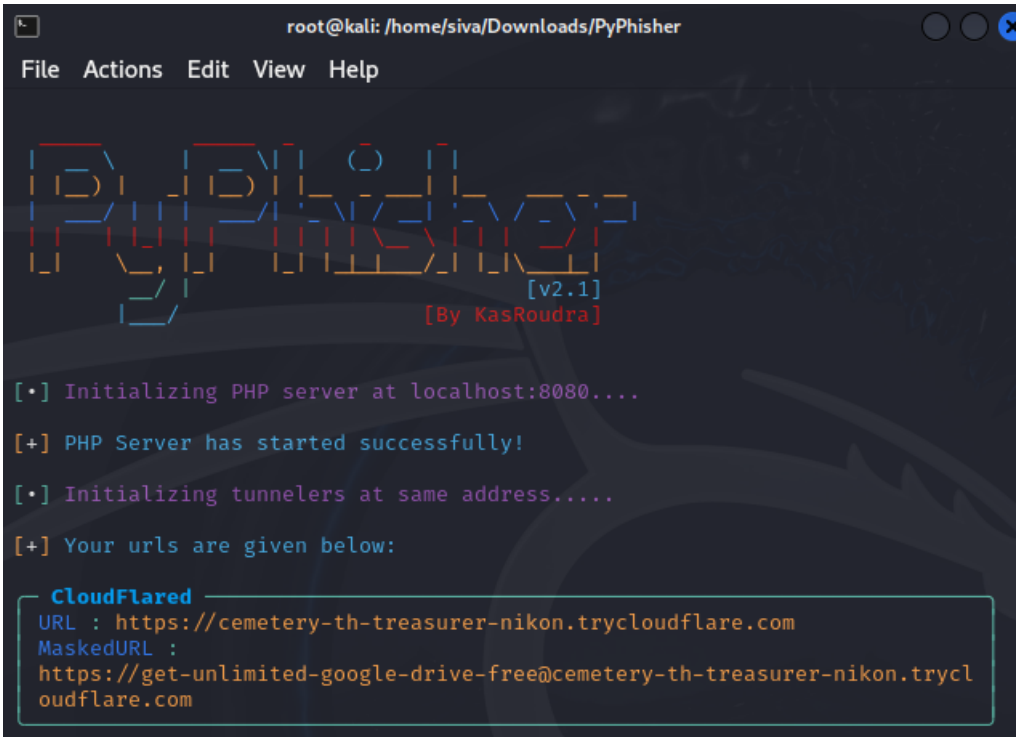

Figure 5: Fake URL link for Gmail website

- Use SET to create and send phishing emails containing links to the fake Gmail login page.

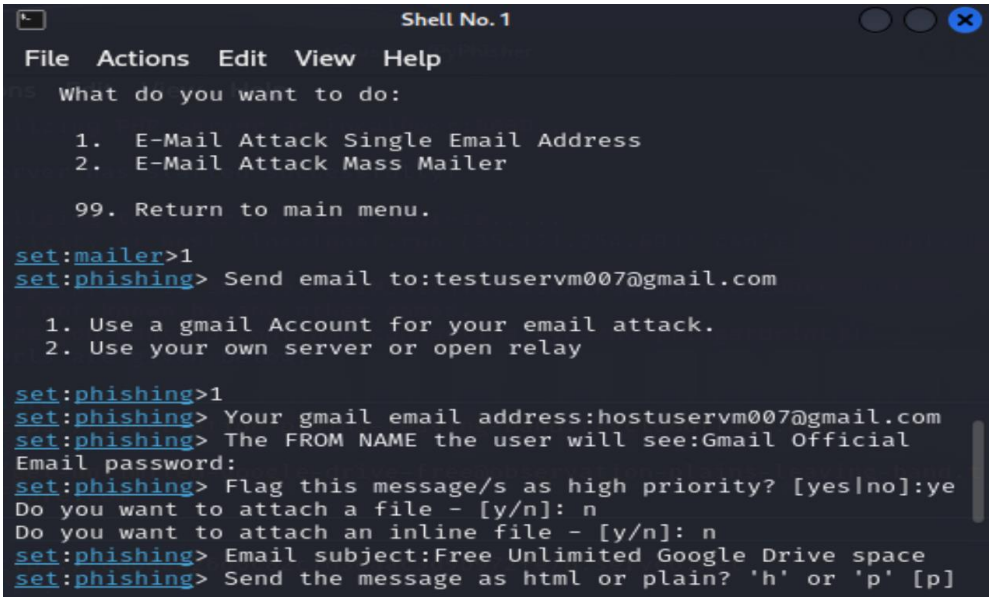

Figure 6: Enter the user account details to send a phishing mail

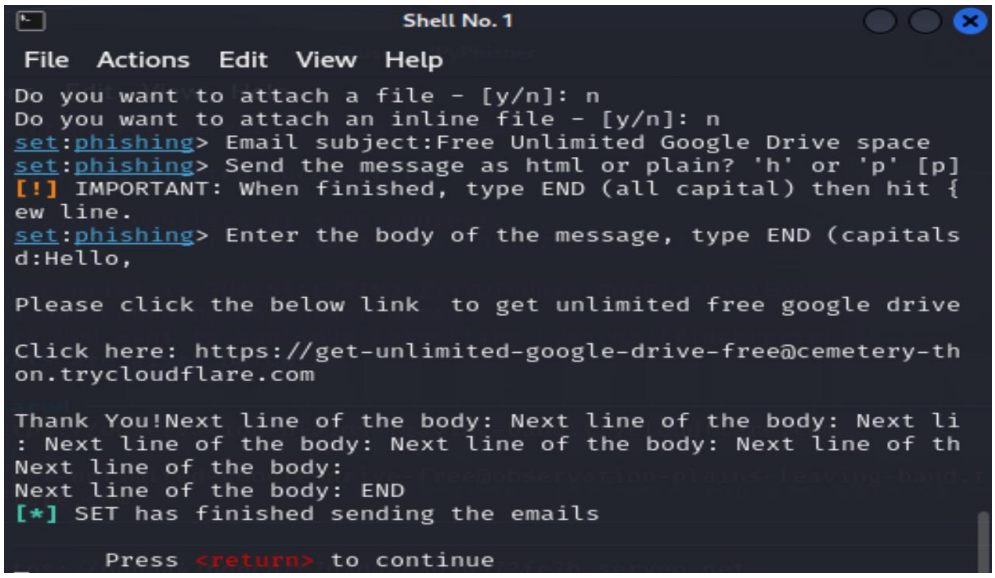

Figure 7: Body of the Phishing Mail

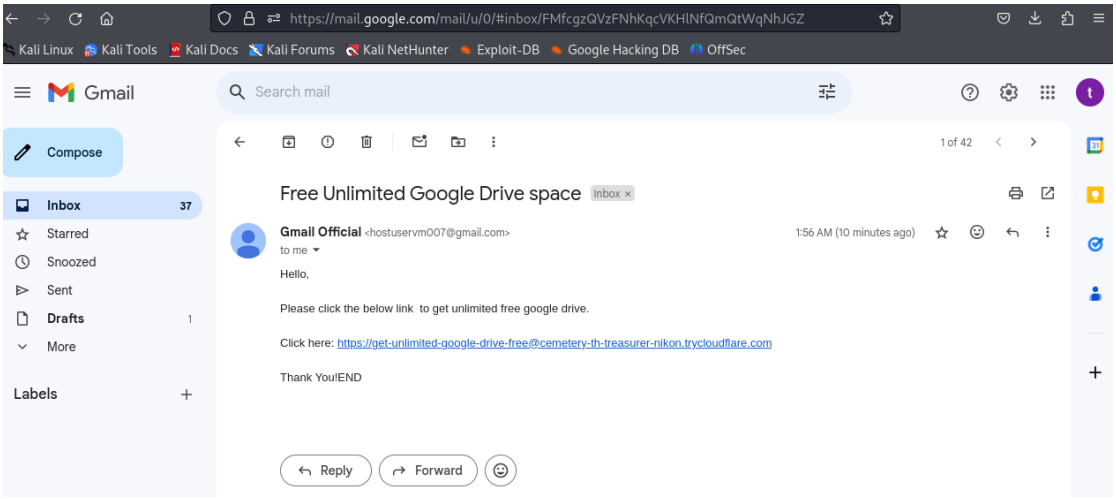

Figure 8: Phishing Mail received by the user with fake URL link

- Monitor the user VM for responses to the phishing email.

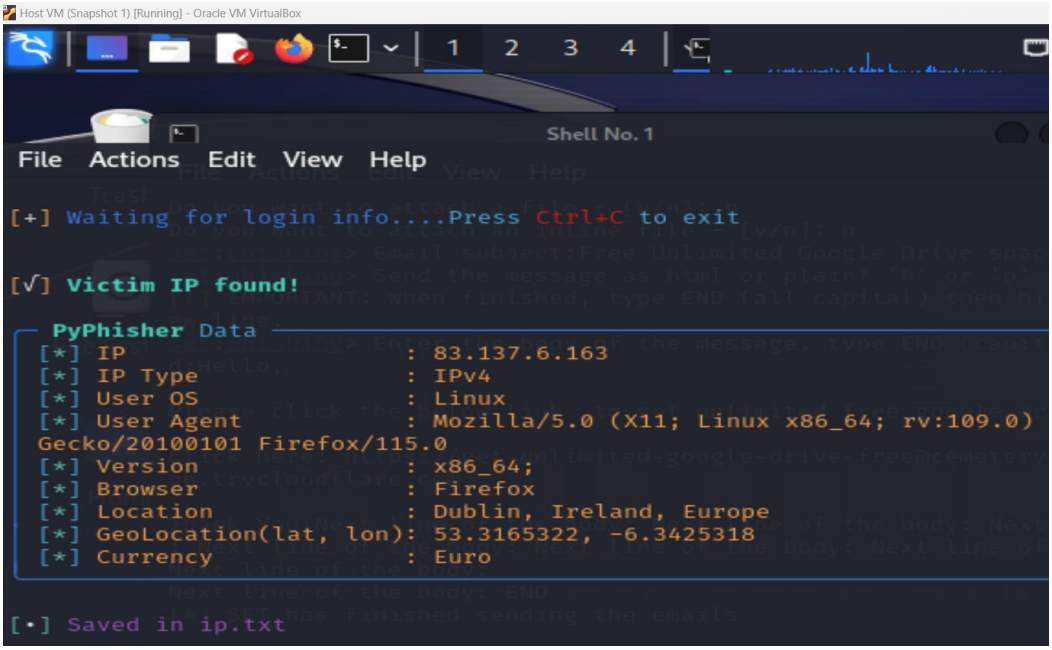

Figure 9: User IP and Location details received by Pyphisher Tool

- Verify if the phishing attempt successfully captures user credentials.

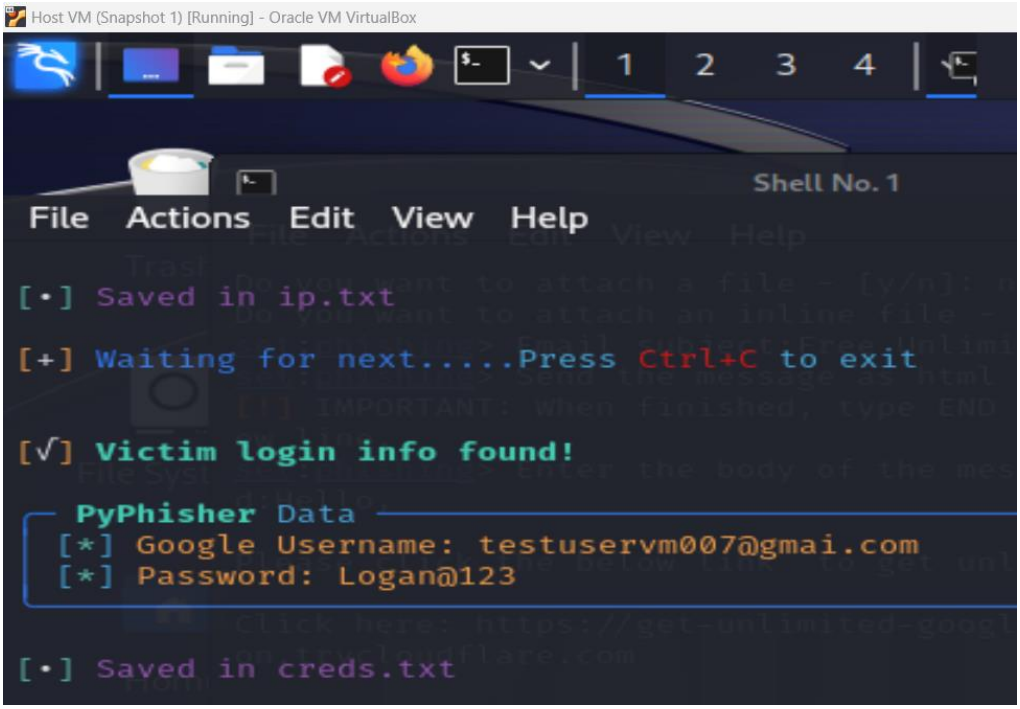

Figure 10: User credentials received successfully

5.2. Rootkit Installation and Detection

- Install Diamorphine rootkit on the User VM through SSH connection from the Host VM.

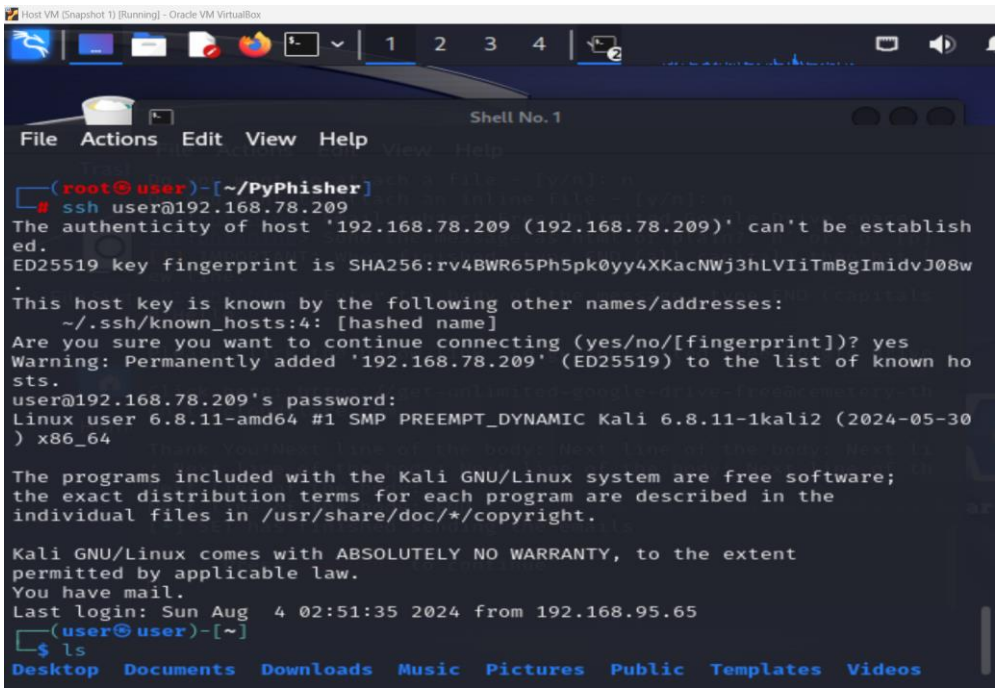

Figure 11: SSH connection established to the User VM

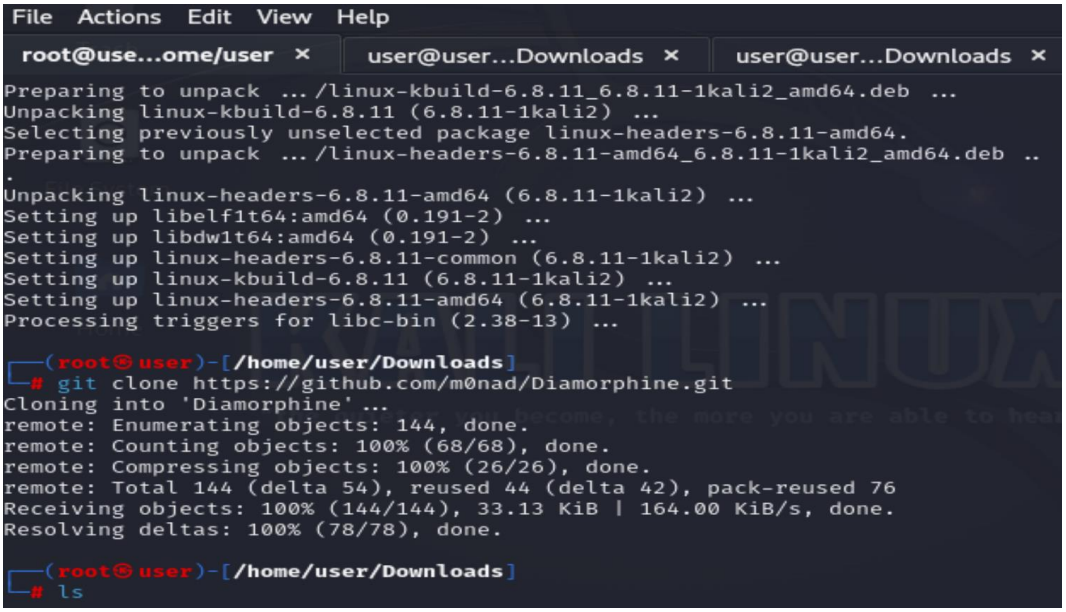

Figure 12: Diamorphine Rootkit Installation

5.3. Image Metadata Modification

- Execute the Python script with the '–preserve' option in order to retain the original image while altering the image metadata.

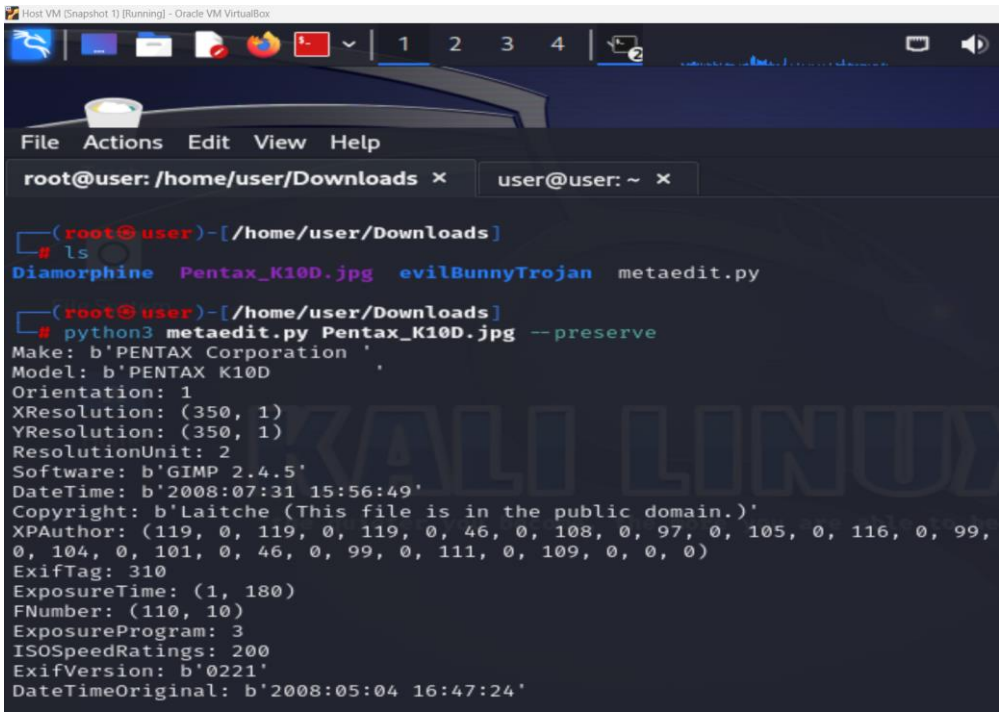

Figure 13: Executed the python script

- Enter the metadata field name and give the new value for the field.

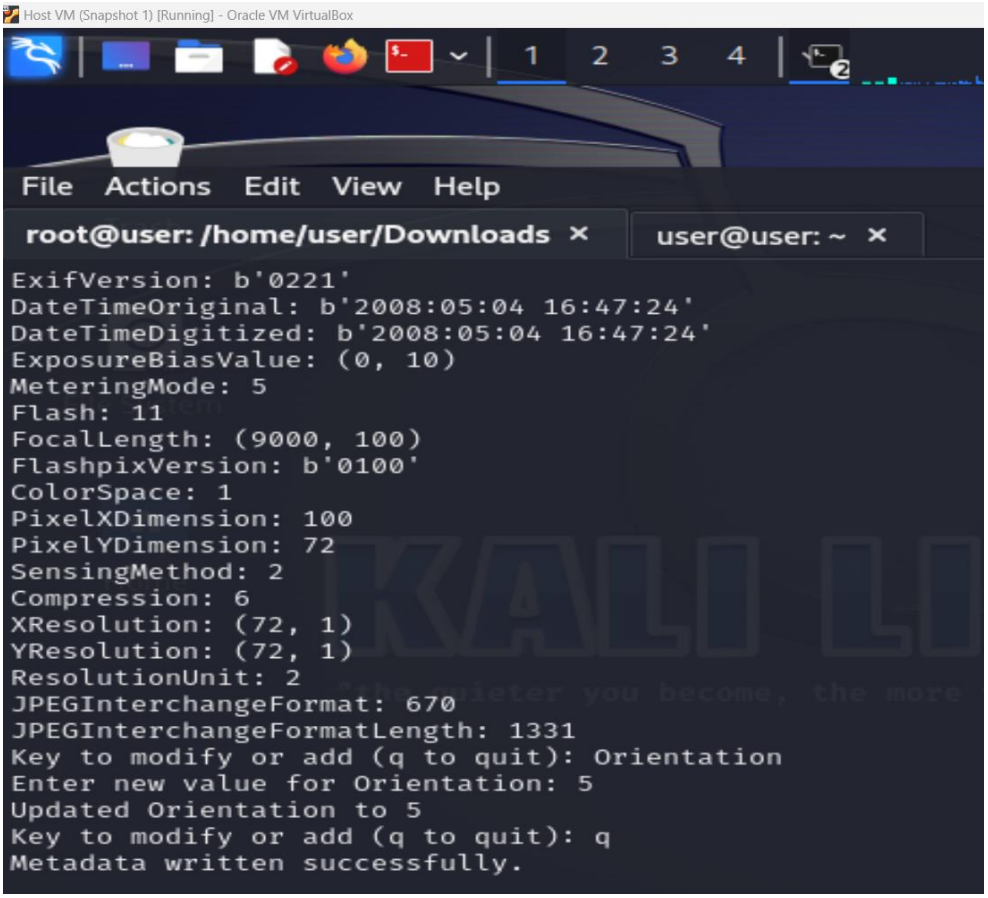

Figure 14: Editing the Image Metadata Value

- Modify the metadata value of the image.

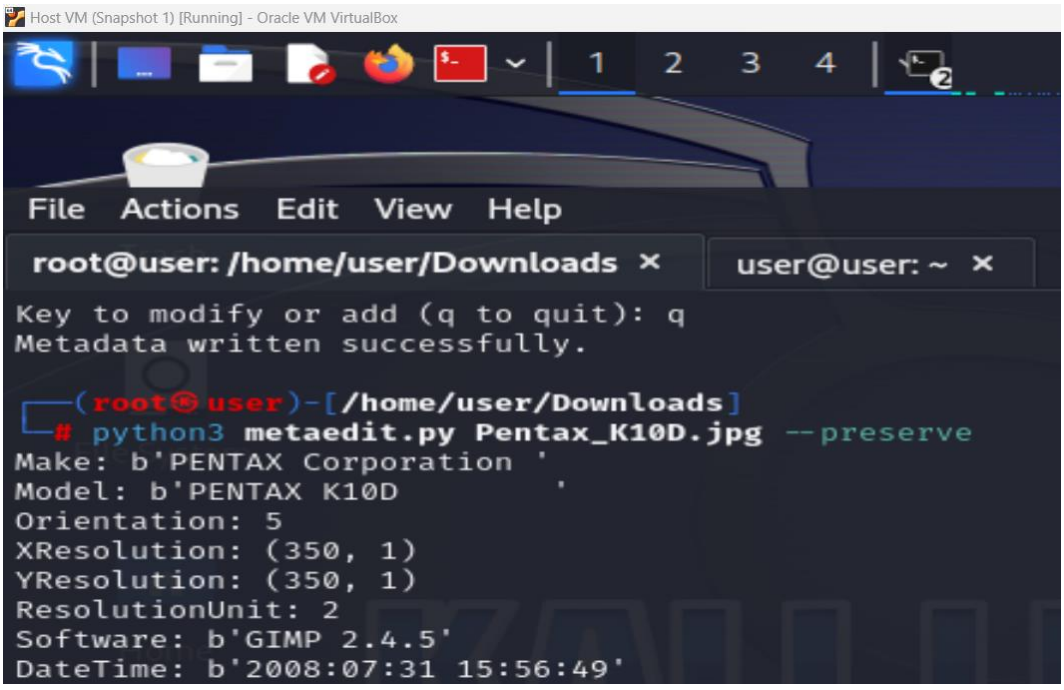

Figure 15: Modified the Image Metadata Value Successfully

6. References

[1] Downloads – Oracle VM VirtualBox (no date).
https://www.virtualbox.org/wiki/Downloads.

[2] Get Kali | Kali Linux (no date). https://www.kali.org/get-kali/#kali-platforms.

[3] Kas Roudra / PYPhisher · GitLab (no date). https://gitlab.com/KasRoudra/PyPhisher.

[4] M0nad (no date) GitHub - m0nad/Diamorphine: LKM rootkit for Linux Kernels
2.6.x/3.x/4.x/5.x/6.x (x86/x86_64 and ARM64). https://github.com/m0nad/Diamorphine.