Hands-On Android Penetration Testing Using PhoneSploit & ADB

Hacking Android using PhoneSploit

Setup: Installing and Running PhoneSploit on Kali Linux

1. **Open Kali Linux Terminal.**
2. **Install ADB**

- **sudo apt update**
- **sudo apt install adb**

3. Download PhoneSploit from GitHub:

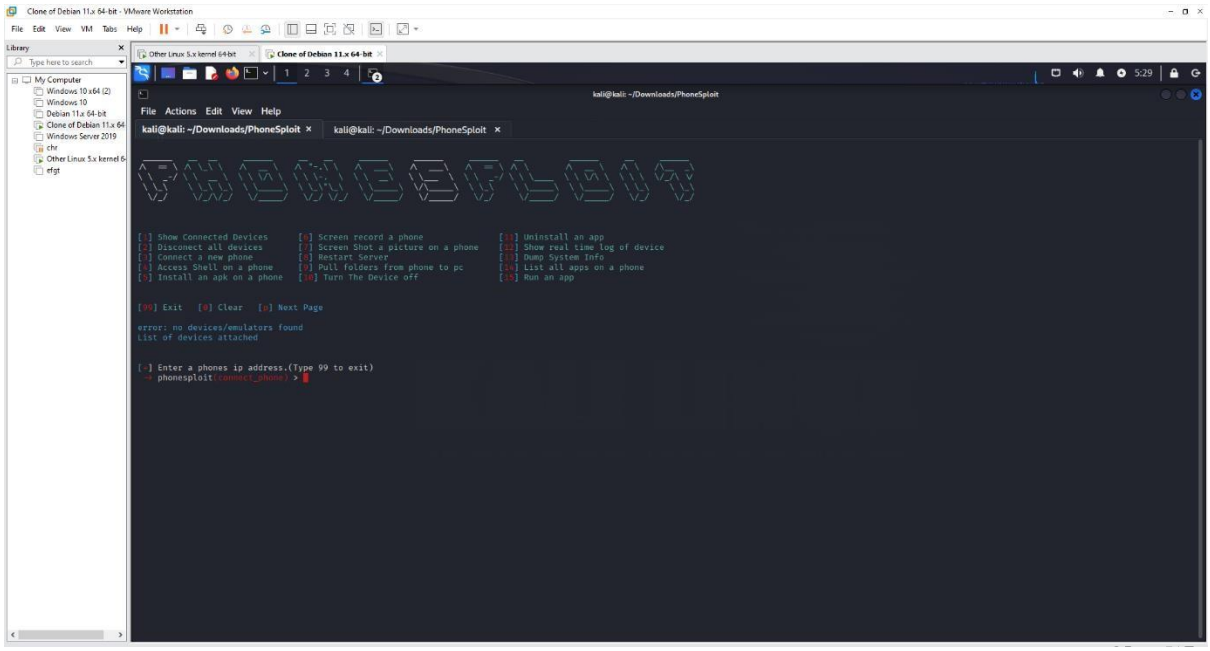
- **git clone https://github.com/prbhtkumr/PhoneSploit**
- **cd PhoneSploit**

4. Run PhoneSploit:

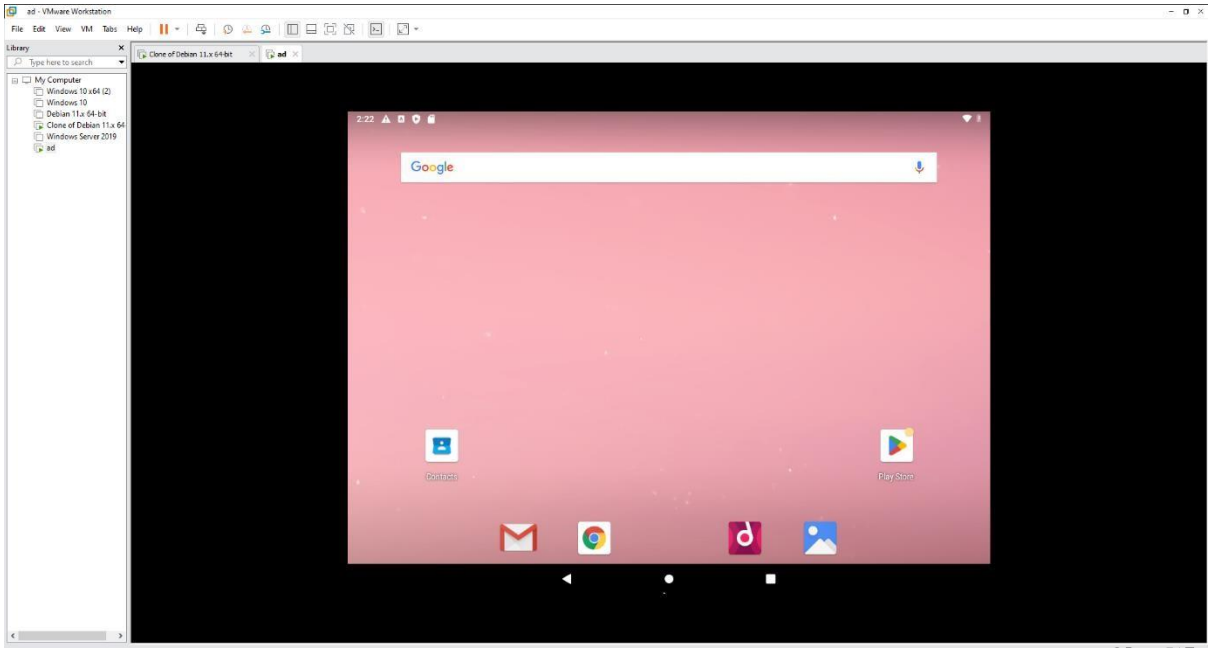
- python3 phonesploit.py

Verify Installation (Task 1):

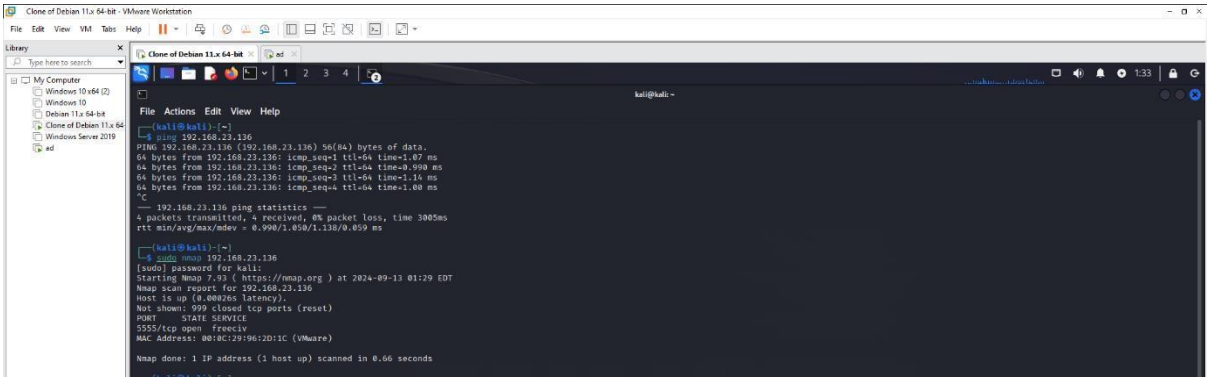
- Once PhoneSploit is running, it should display a menu of options.
- Take a screenshot of the tool running to fulfill **Task 1**



Android VM



I ping android vm and scane throught nmap to cheeck port

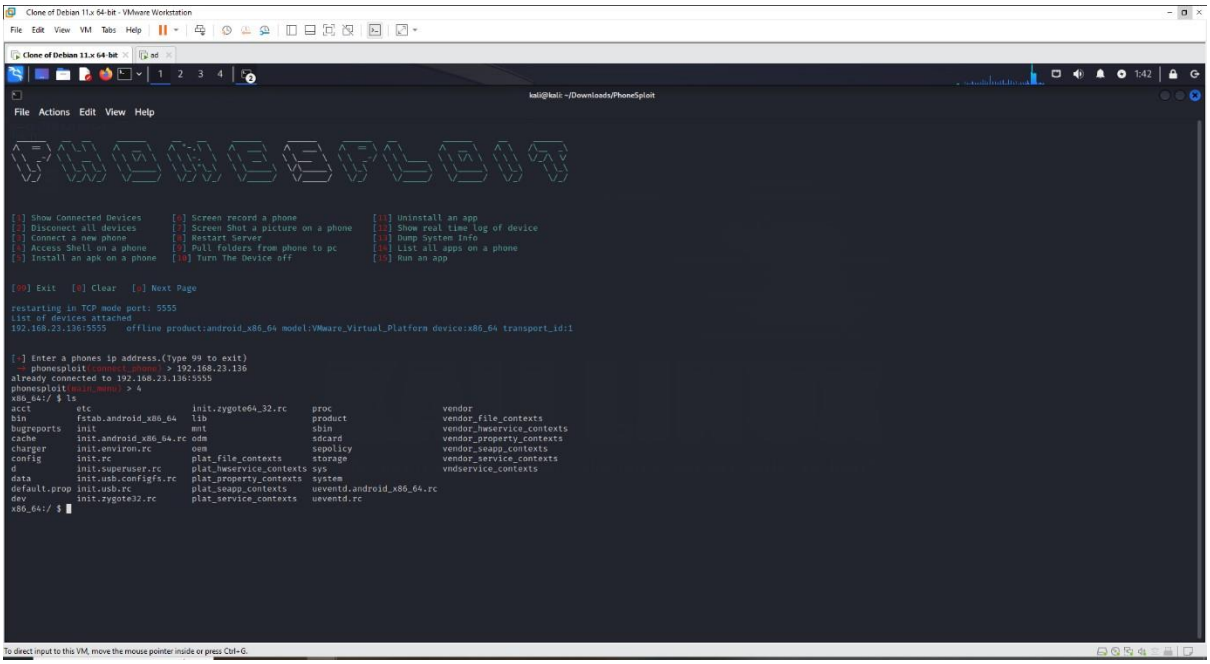


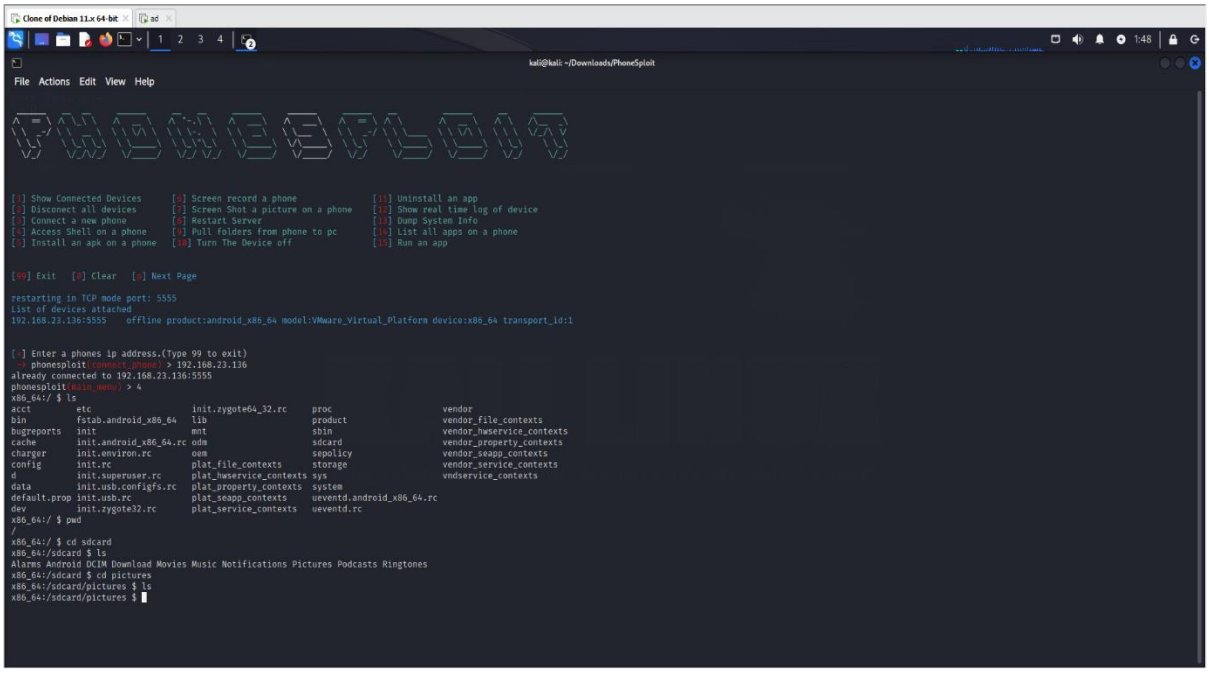
Task 2: Getting a Shell on Android VM & Running Commands

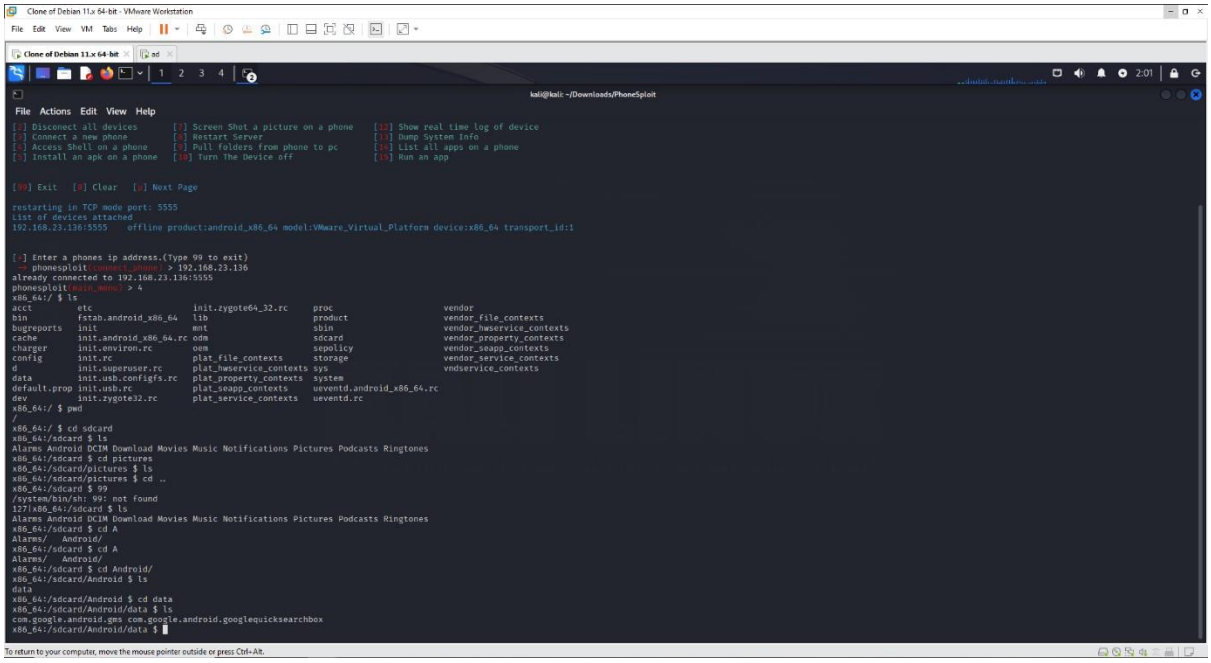
Steps to Get a Shell on the Android Device:

1. **Ensure ADB Debugging is Enabled on Android VM**:
    - Go to **Developer Options** on the Android VM and enable **USB Debugging**.
2. **Connect Your Kali Machine and Android VM to the Same Network**:
    - Obtain the IP address of your Android VM by going to **Settings > About Phone > Status > IP Address**.
3. **Connect to Android Device via ADB**:
    - In PhoneSploit, choose the option that connect to a device by IP.
4. **Get Shell Access:**
    - In PhoneSploit, select the option to access the shell of the Android device
5. **Screenshot for Task 2:**

- Take a screenshot showing the connection, command, and the output, and provide a brief explanation of how the shell command works and what information it returns.



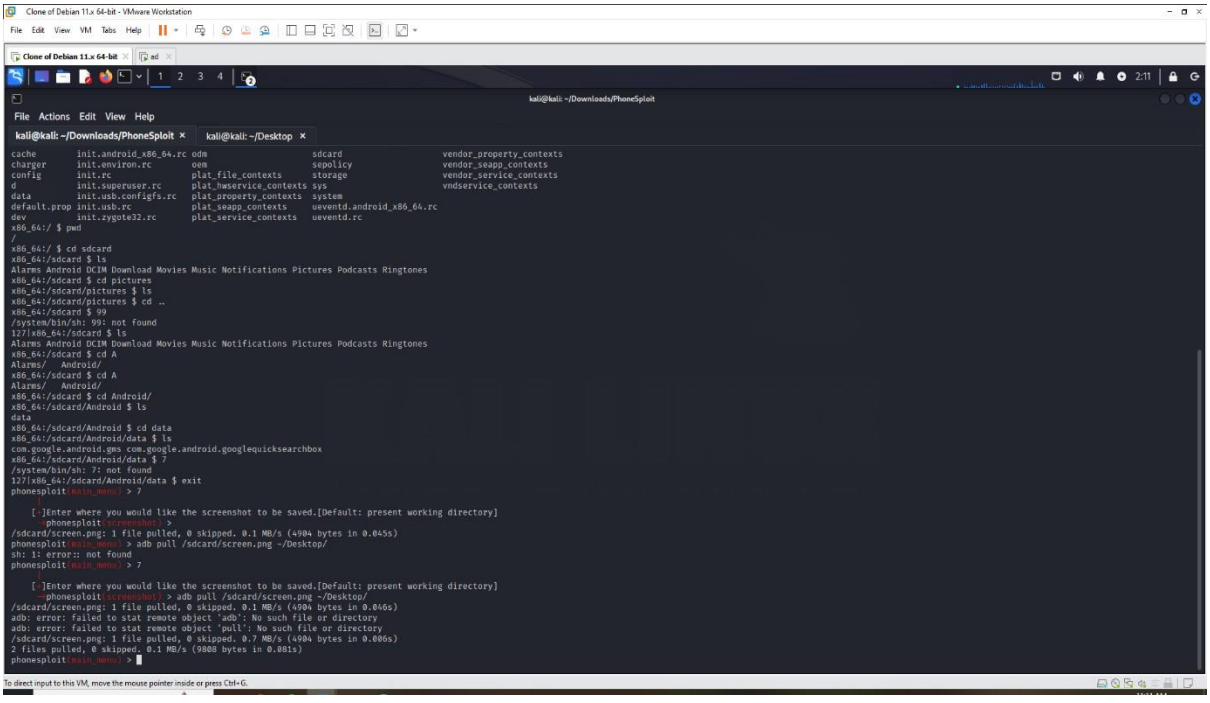




Task 3: Taking a Screenshot of the Android Device Screen

1. **Take a Screenshot**:

- In PhoneSploit, select the option to take a screenshot.



2. Pull the Screenshot to Your Kali Machine:

- After taking the screenshot, you can pull the file to your Kali machine:

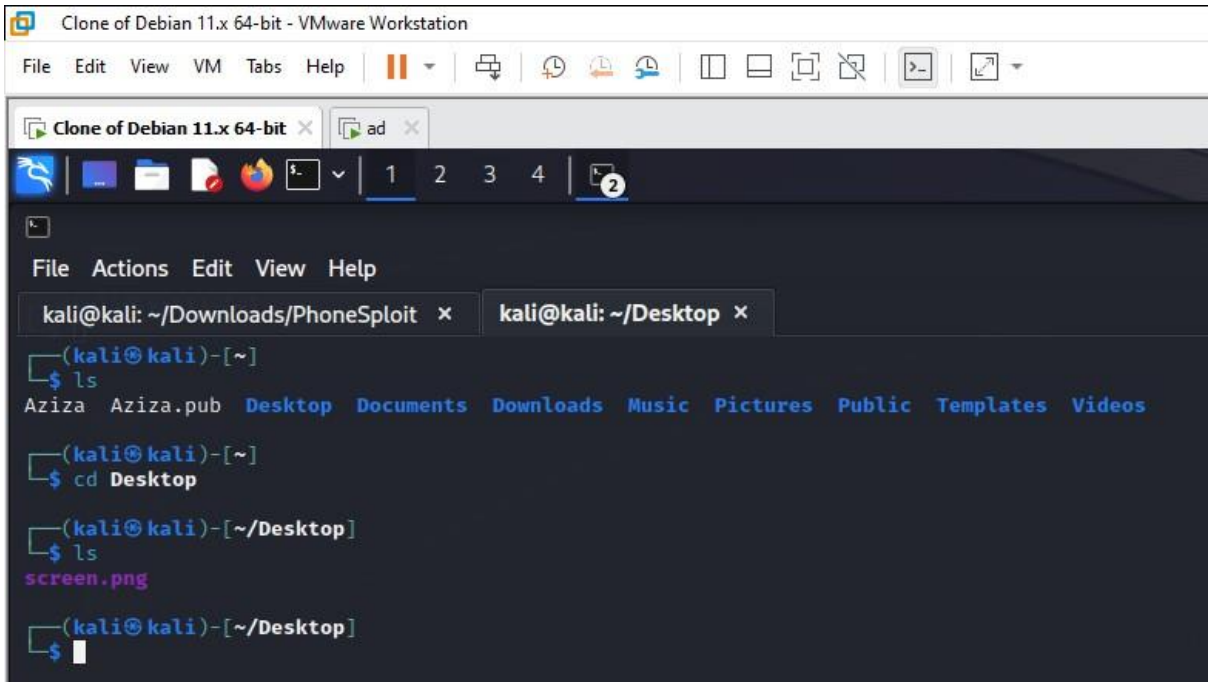
- **adb pull /sdcard/screen.png ~/Desktop/**

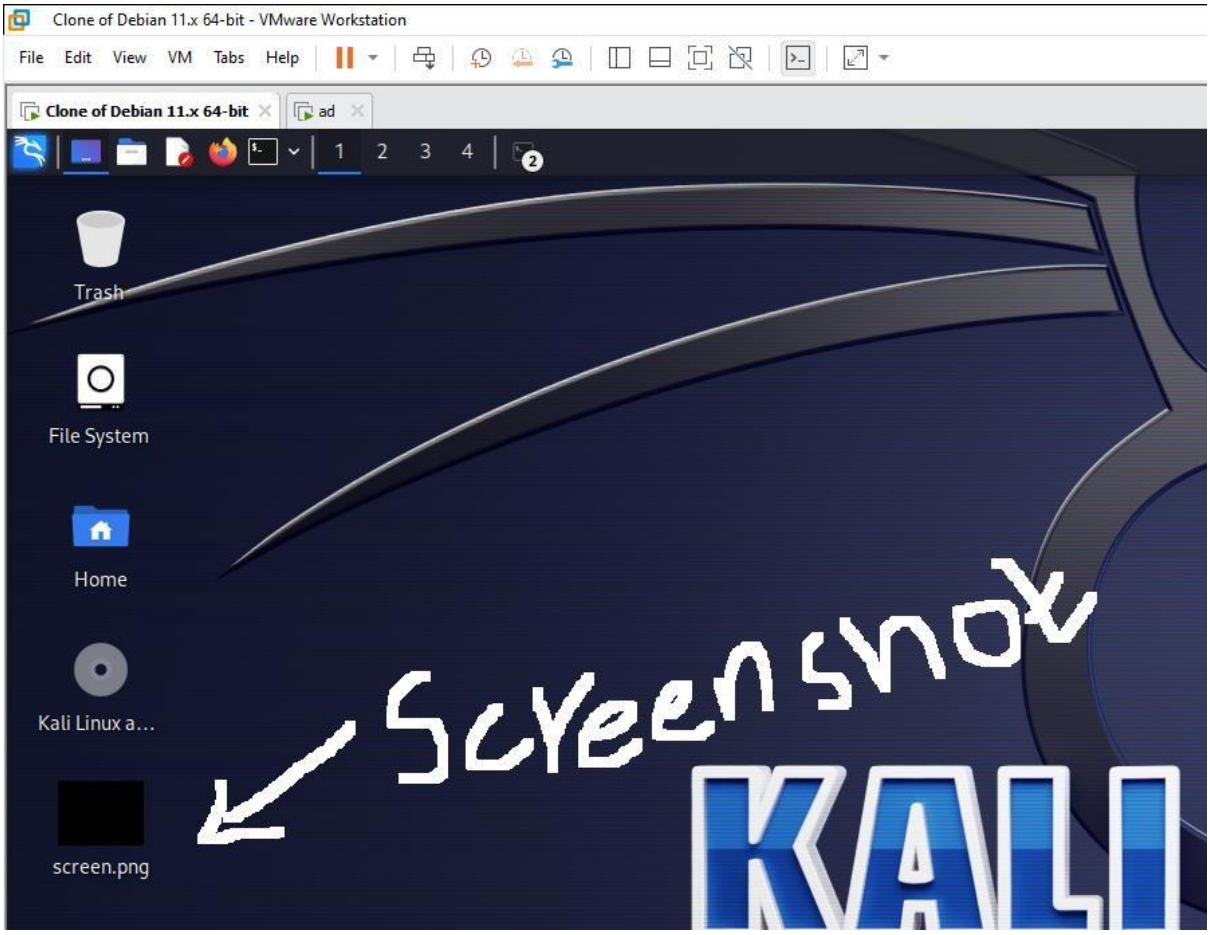
3. Verify the Screenshot:

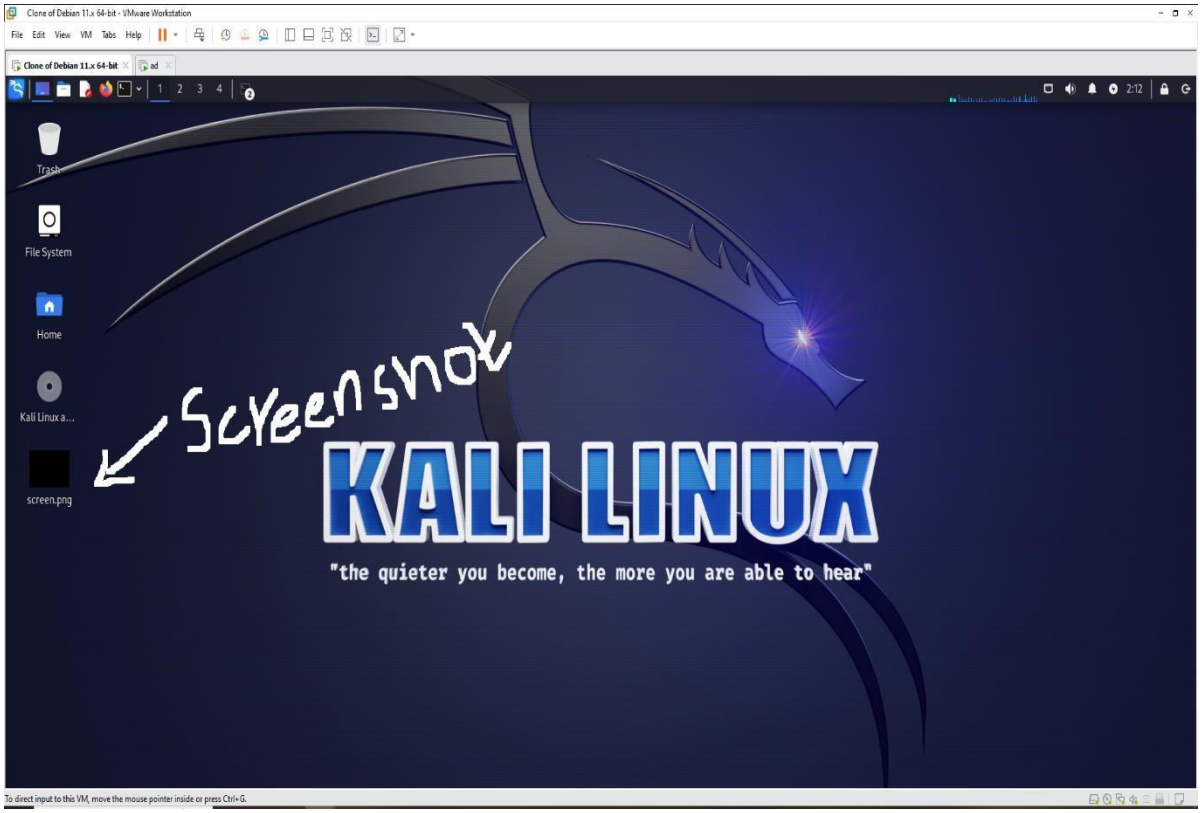
- Check if the screenshot has been stored on the Desktop of your Kali machine.

- Take a screenshot showing the command and the output for **Task 3**.

Screenshot to Your Kali Machine




Clone of Debian 11.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Clone of Debian 11.x 64-bit
ad
1 2 3 4
Trash
File System
Home
Kali Linux a...
screen.png
Screenshot
KALI


Clone of Debian 11.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Clone of Debian 11.x 64-bit
ad
1 2 3 4
Trash
File System
Home
Kali Linux a...
screen.png
Screenshot
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Task 4: Turning Off the Android Device

1. **Turn Off the Android Device**:

    - In PhoneSploit, use the command to power off the device:

2. **Screenshot for Task 4**:

    - Take a screenshot showing the command execution and the device turning off.