
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:

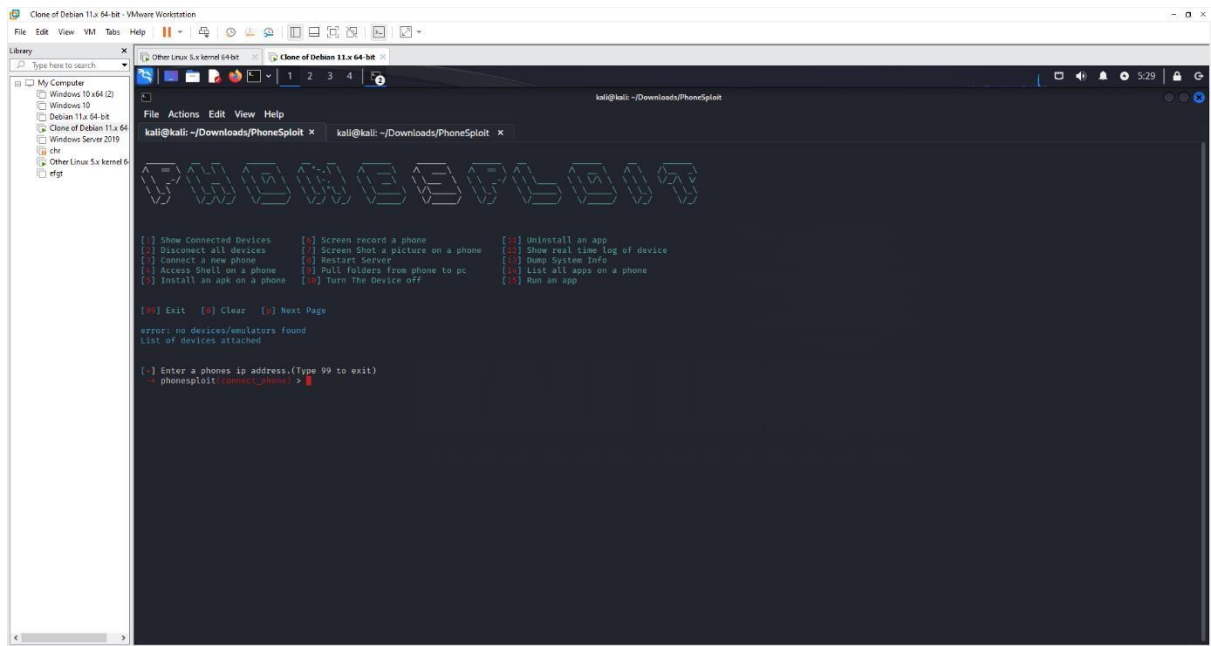
```
 git clone https://github.com/prbhtkumr/PhoneSploit
 cd PhoneSploit
```

4. Run PhoneSploit:

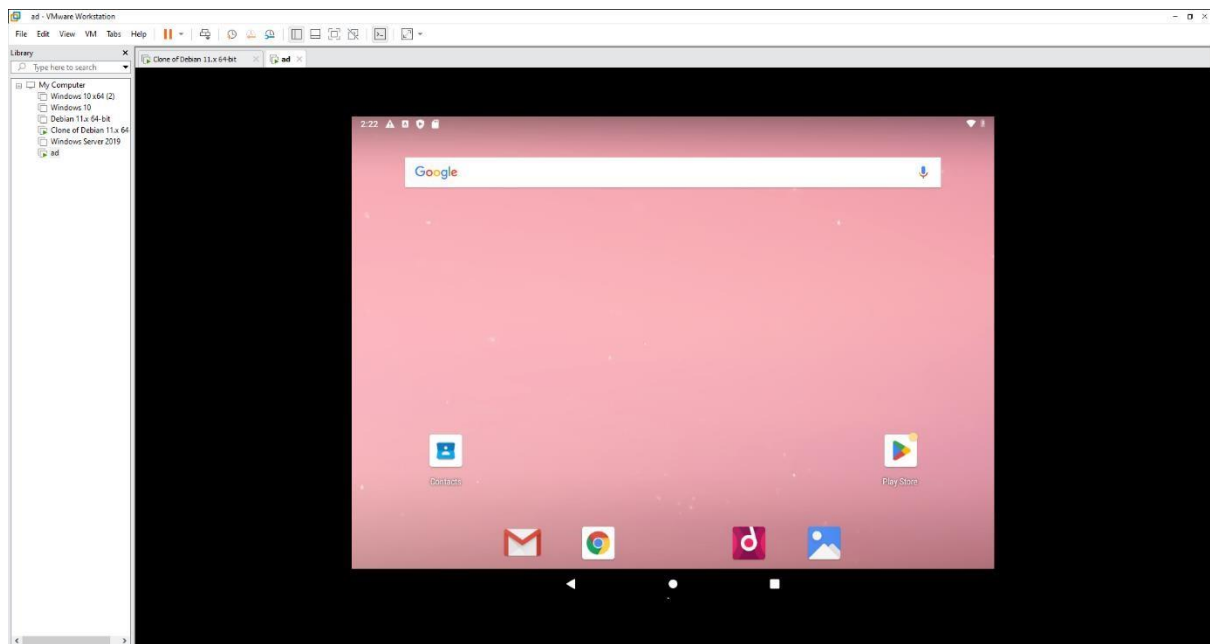
```
 python3 phonesploit.py
```

Verify Installation (Task 1):

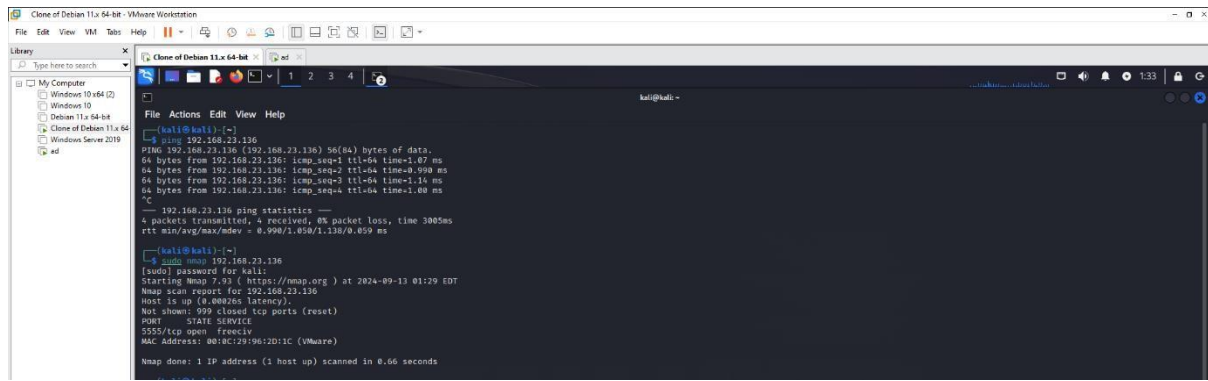
- Once PhoneSploit is running, it should display a menu of options.
- Take a screenshot of the tool running to fulfill **Task 1**



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:

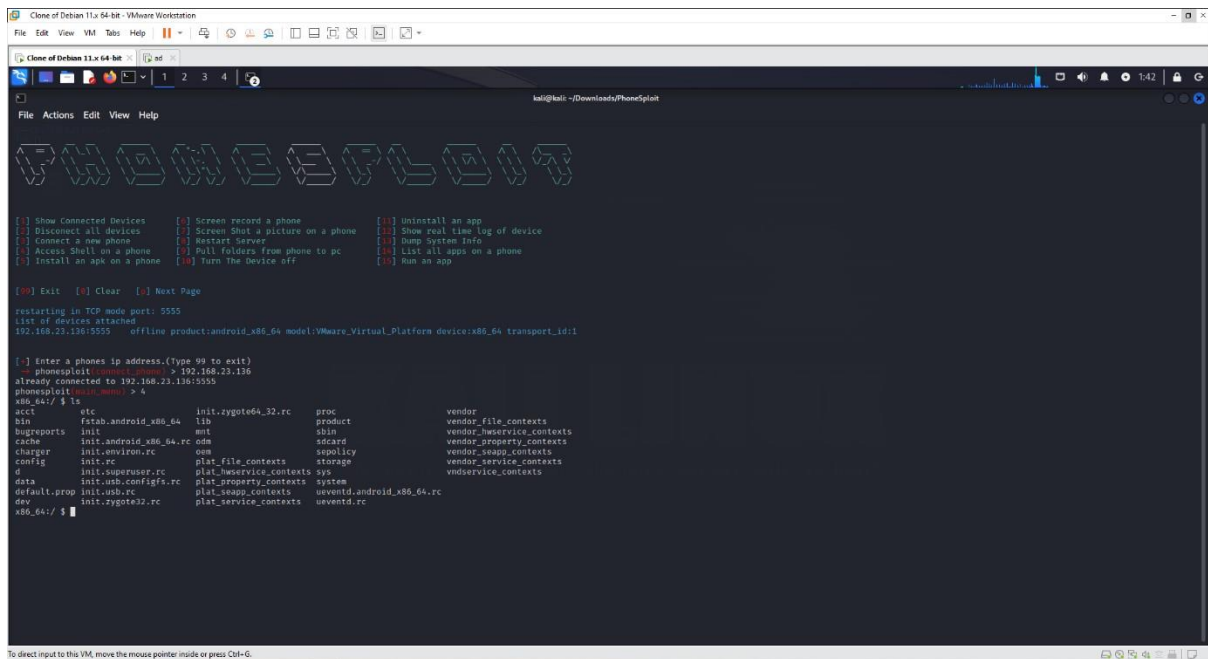
- In PhoneSploit, choose the option that connect to a device by IP.

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.



```

Clone of Debian 11.x 64-bit - VMware Workstation
File Edit View VM Tabs Help

Clone of Debian 11.x 64-bit x86_64
kali@kali: ~/Downloads/PhoneSploit

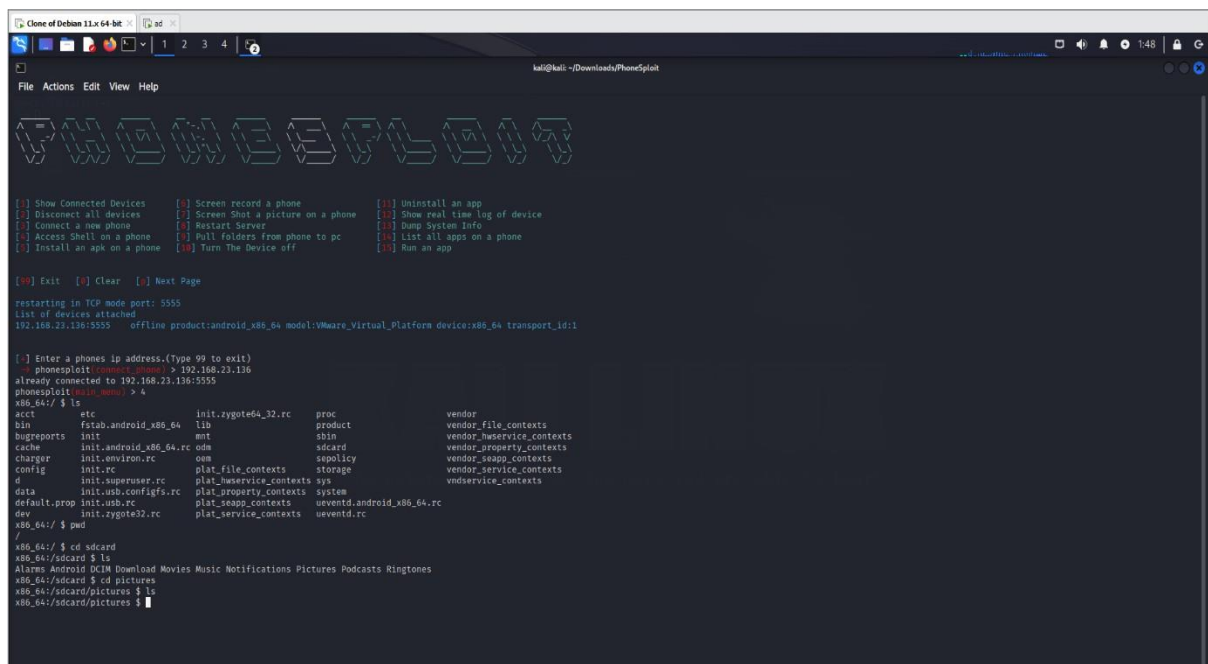
[1] Show Connected Devices [2] Screen record a phone [3] Uninstall an app
[2] Disconnect all devices [3] Screen Shot a picture on a phone [4] Show real time log of device
[3] Connect a new phone [4] Restart Server [5] Dump System Info
[4] Access Shell on a phone [5] Pull folders from phone to pc [6] List all apps on a phone
[5] Install an apk on a phone [6] Turn The Device off [7] Run an app

[00] Exit [0] Clear [0] Next Page

restarting in TCP mode port: 5555
list of devices attached
192.168.23.136:5555 offline product:android_x86_64 model:VMware_Virtual_Platform device:x86_64 transport_id:1

[~] Enter a phones ip address.(Type 99 to exit)
~ phonesploit(connected_phone) > 192.168.23.136
already connected to 192.168.23.136:5555
phonesploit(main_menu) > 4
x86_64:/ $ ls
acct      etc       init.zygote64_32.rc  proc      vendor
bin       fsstab.android_x86_64  lib          product  vendor_file_contexts
bugreports  init      mnt            sbin      vendor_hwservice_contexts
cache      init.android_x86_64.rc  odm          sdcard   vendor_property_contexts
charger    init.envirion.rc       oem          sepolicy  vendor_seapp_contexts
config     init.rc             plat_file_contexts  sys       vendor_service_contexts
d          init.superuser.rc      plat_hwservice_contexts  vndservice_contexts
data       init.usb.configfs.rc   plat_property_contexts  system
default.prop  init.usb.rc          plat_seapp_contexts  ueventd.android_x86_64.rc
dev        init.zygote32.rc       plat_service_contexts  ueventd.rc
x86_64:/ $

```



```

Clone of Debian 11.x 64-bit x86_64
kali@kali: ~/Downloads/PhoneSploit

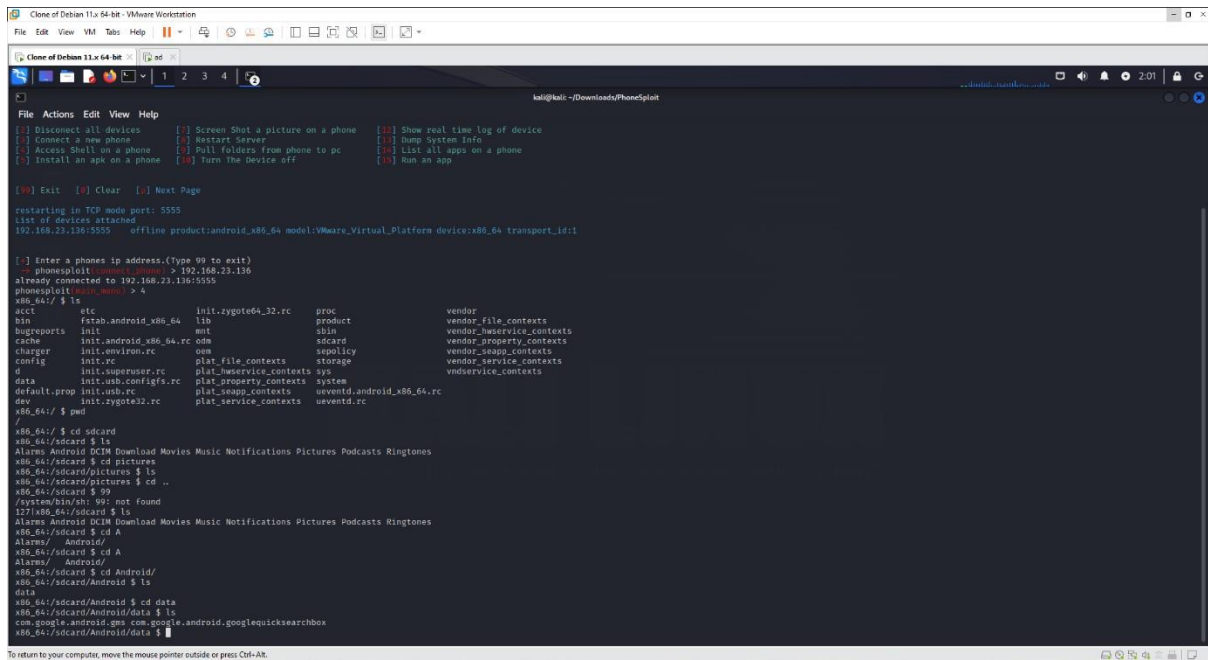
[1] Show Connected Devices [2] Screen record a phone [3] Uninstall an app
[2] Disconnect all devices [3] Screen Shot a picture on a phone [4] Show real time log of device
[3] Connect a new phone [4] Restart Server [5] Dump System Info
[4] Access Shell on a phone [5] Pull folders from phone to pc [6] List all apps on a phone
[5] Install an apk on a phone [6] Turn The Device off [7] Run an app

[00] Exit [0] Clear [0] Next Page

restarting in TCP mode port: 5555
list of devices attached
192.168.23.136:5555 offline product:android_x86_64 model:VMware_Virtual_Platform device:x86_64 transport_id:1

[~] Enter a phones ip address.(Type 99 to exit)
~ phonesploit(connected_phone) > 192.168.23.136
already connected to 192.168.23.136:5555
phonesploit(main_menu) > 4
x86_64:/ $ ls
acct      etc       init.zygote64_32.rc  proc      vendor
bin       fsstab.android_x86_64  lib          product  vendor_file_contexts
bugreports  init      mnt            sbin      vendor_hwservice_contexts
cache      init.android_x86_64.rc  odm          sdcard   vendor_property_contexts
charger    init.envirion.rc       oem          sepolicy  vendor_seapp_contexts
config     init.rc             plat_file_contexts  sys       vendor_service_contexts
d          init.superuser.rc      plat_hwservice_contexts  vndservice_contexts
data       init.usb.configfs.rc   plat_property_contexts  system
default.prop  init.usb.rc          plat_seapp_contexts  ueventd.android_x86_64.rc
dev        init.zygote32.rc       plat_service_contexts  ueventd.rc
x86_64:/ $ pwd
/
x86_64:/ $ cd /sdcard
x86_64:/sdcard $ ls
Alarms Android DCIM Downloads Movies Music Notifications Pictures Podcasts Ringtones
x86_64:/sdcard $ cd pictures
x86_64:/sdcard/pictures $ ls
x86_64:/sdcard/pictures $

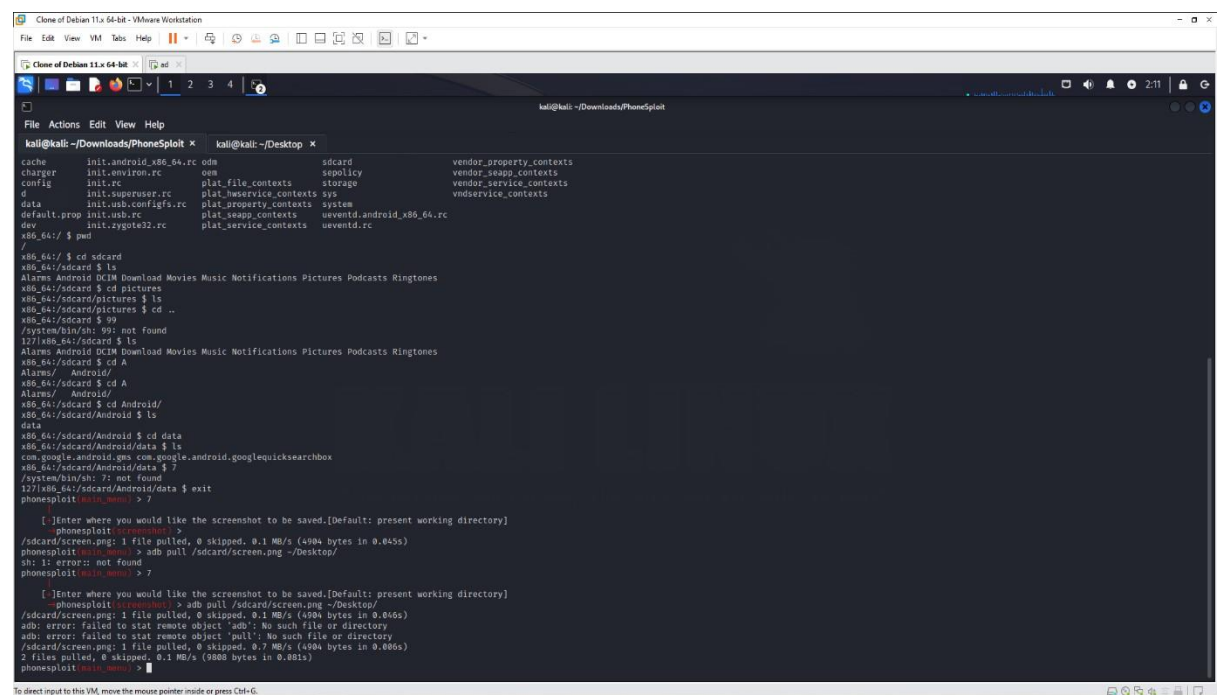
```



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:

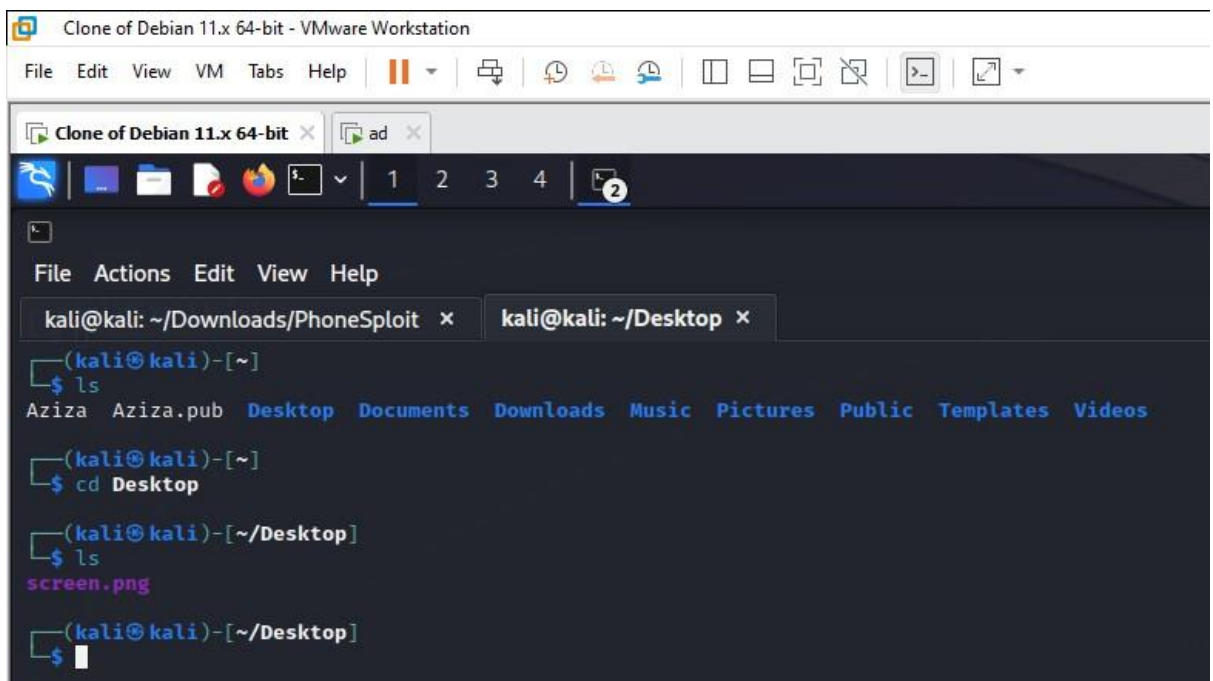
- After taking the screenshot, you can pull the file to your Kali machine:

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

3. Verify the Screenshot:

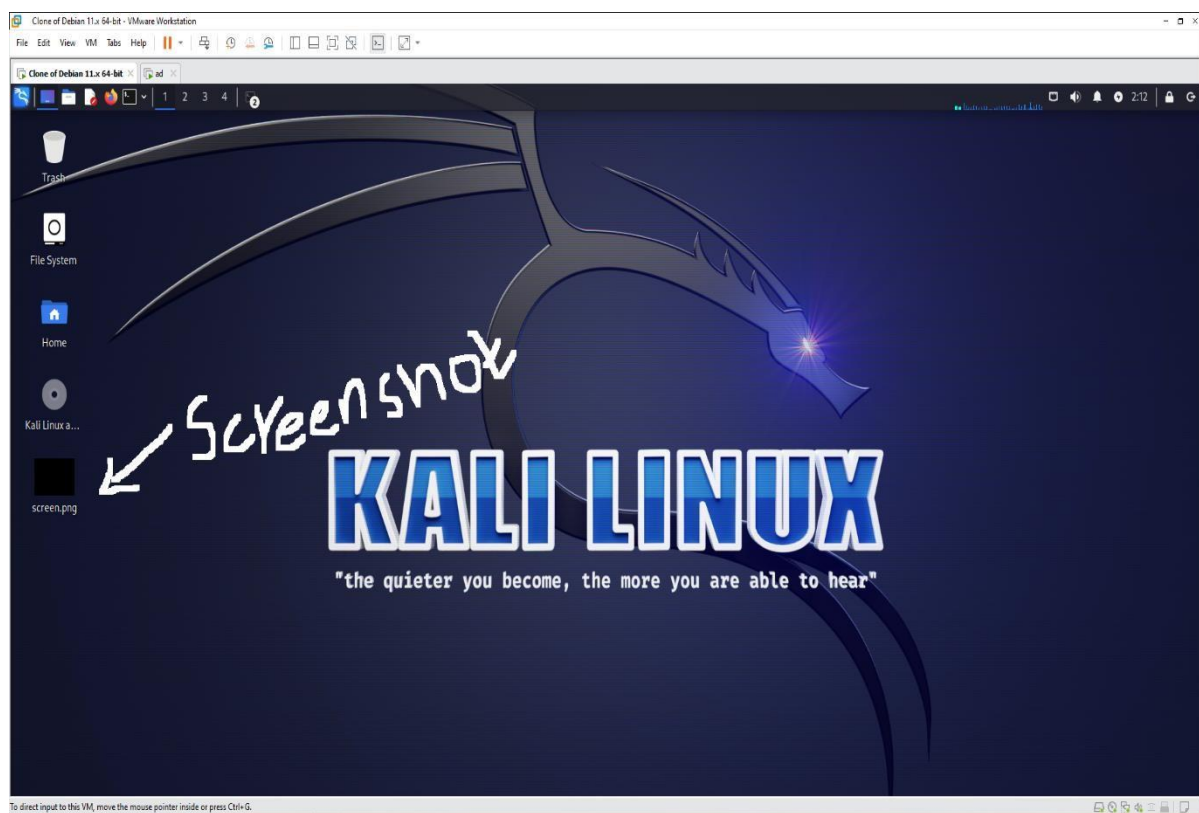
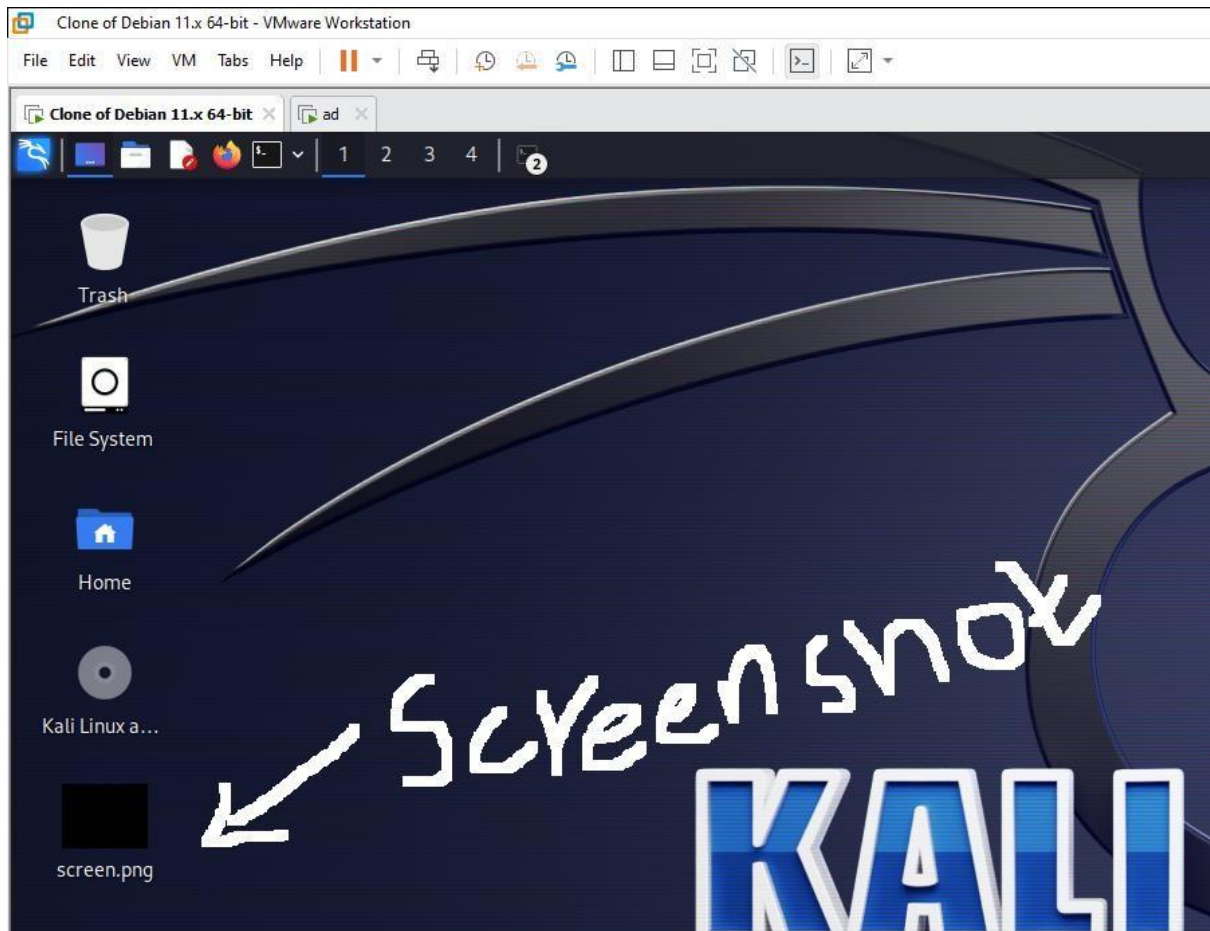
- Check if the screenshot has been stored on the Desktop of your Kali machine.
- Take a screenshot showing the command and the output for **Task 3**.

Screenshot to Your Kali Machine



The image shows a VMware Workstation window titled "Clone of Debian 11.x 64-bit - VMware Workstation". Inside the VM, a Kali Linux terminal is open. The terminal has a menu bar with "File", "Actions", "Edit", "View", and "Help". There are two tabs: "kali@kali: ~/Downloads/PhoneSploit" and "kali@kali: ~/Desktop". The terminal shows the following commands and output:

```
(kali@kali)-[~]  
$ ls  
Aziza  Aziza.pub  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  
  
(kali@kali)-[~]  
$ cd Desktop  
  
(kali@kali)-[~/Desktop]  
$ ls  
screen.png  
  
(kali@kali)-[~/Desktop]  
$
```



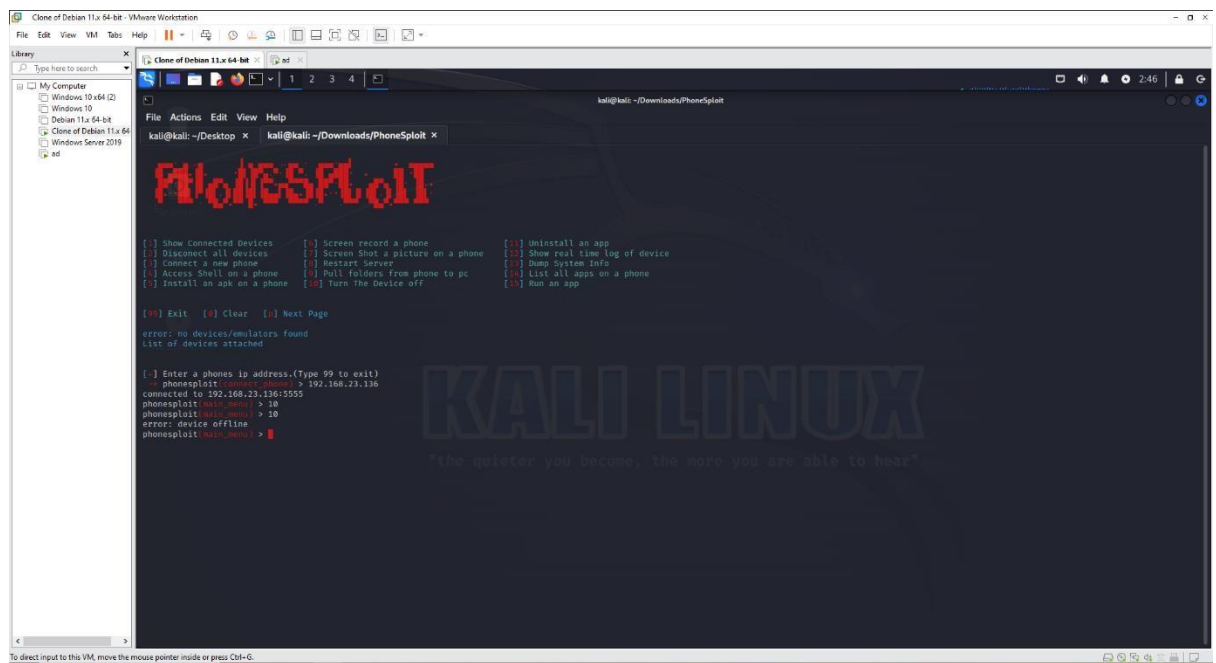
Task 4: Turning Off the Android Device

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.



```
Clone of Debian 11.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
  Windows 10 x64 (2)
  Debian 11.x 64-bit
  Clone of Debian 11.x 64-bit
  Windows Server 2019
  ad
kali@kali: ~/Downloads/PhoneSploit
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Downloads/PhoneSploit x
PHONESPLOIT
[ ] Show Connected Devices [ ] Screen record a phone [ ] Uninstall an app
[ ] Disconnect all devices [ ] Screen Shot a picture on a phone [ ] Show real time log of device
[ ] Connect a new phone [ ] Restart Server [ ] Dump System Info
[ ] Access Shell on a phone [ ] Pull folders from phone to pc [ ] List all apps on a phone
[ ] Install an apk on a phone [ ] Turn The Device off [ ] Run an app
[+] Exit [0] Clear [u] Next Page
error: no devices/emulators found
List of devices attached
[ ] Enter a phones ip address.(Type 99 to exit)
phonesploit: ~$ ip netns exec ns1 192.168.23.136
connected to 192.168.23.136:5555
phonesploit(ns1:~$) > 10
phonesploit(ns1:~$) > 10
error: device offline
phonesploit(ns1:~$) >
```