Android Security & Exploitation

Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

Hooking using Introspy

- Comes with Introspy-core and Config
- Works on top of MobileSubstrate for Android - Written by Jay Freeman (Saurik)
- Could easily set up hooks on interesting functions

Setting up Introspy

- Install supersu
- Install CydiaSubstrate for Android
- Link using CydiaSubstrate
- Soft reboot
- Install Introspy-Core and Introspy-Config
- Select the APIs to hook in Introspy-Config app on the device

Analysing logs

- adb shell
- cd /data/data/[app-name]/databases/
- Find introspy.db
- adb pull [path to introspy.db] appname.db
- Navigate to Introspy-Analyser-Master
- python introspy.py -p android -o Appname appname.db

Where can you use these

- Debugging apps to know more about them
- Setting breakpoint and hooks at specific methods
- Identifying crypto keys
- Bypassing SSL Pinning
- Bypassing root detection