

Android Security & Exploitation



Aditya Gupta (@adi1391)

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

adi@attify.com

Certifications : <http://securitytube-training.com>

Pentester Academy : <http://PentesterAcademy.com>

© 2015 - Pentester Academy and Attify

Traffic Analysis

Traffic Interception

- Active : Burp, MITMProxy, Charles, Mallory
- Passive : TcpDump

Passive Traffic Interception

- Download the TCPDump binary for ARM (or cross-compile)
- <http://www.eecs.umich.edu/~timuralp/tcpdump-arm>
- `adb push tcpdump /data/local/tcpdump`
- `adb shell chmod 777 /data/local/tcpdump`
- `tcpdump -w output.pcap tcp port 80`
- `adb pull /data/local/output.pcap -> Analyze in Wireshark`

Traffic Interception with tcpdump and nc

- Cross compile netcat binary for ARM Android
- `adb push nc /data/local/nc`
- `adb shell chmod 777 /data/local/nc`
- `tcpdump -w - | nc -l -p 31337`
- `adb forward tcp:12345 tcp:31337 && nc 127.0.0.1 12345 | wireshark -k -S -i -`



Any.do To-do List & Task List


Any.do - 14 February 2014

Productivity

Install



Add to wishlist

 This app is compatible with all of your devices. **Offers in-app purchases**

★★★★★ (117,369)



+104441 Recommend this on Google

Additional information

Updated

14 February 2014

Size

8.6M

Installs

5,000,000 - 10,000,000

Current Version

2.40

Requires Android

2.2 and up

Content Rating

Low Maturity

Contact Developer

[Visit Developer's Website](#)

[Email Developer](#)

[Privacy Policy](#)

SSL Traffic Interception

- Set up Burp proxy as normal
- Open `http://burp` in the browser
- `cacert.cer` will get downloaded to SD Card
- Rename it to `cacert.crt`

(`adb shell mv /mnt/sdcard/Download/cacert.cer /mnt/sdcard/Download/cacert.crt`)

- Settings | Security | Install Certificates

Emulator with proxy

- `emulator -avd [avd name] -http-proxy
127.0.0.1:8080`