ANDROID APPLICATION PENETRATION TESTING

Raja Nagori

$WHOAMI

- Senior Information Security Engineer at FIS Global.
- Cyber Crime Intervention Officer from ISAC (NSD).
- Synack Red Team Member.
- Actively contributing to OWASP Community.

TODAY'S DISCUSSION

- Some Kick off Resources for Mobile VA and PT
- Device Requirements and Tools Requirements for starting a Android Application VA and PT
- Concept about Android Architecture
- Practical implementation for Android Application VA and PT

RESOURCES

- MOBILE SECURITY TESTING GUIDE
  - https://mobile-security.gitbook.io/mobile-security-testing-guide/
- OWASP Mobile Top 10
  - https://owasp.org/www-project-mobile-top-10/
- HACKTRICKs
  - https://book.hacktricks.xyz/mobile-apps-pentesting/android-app-pentesting

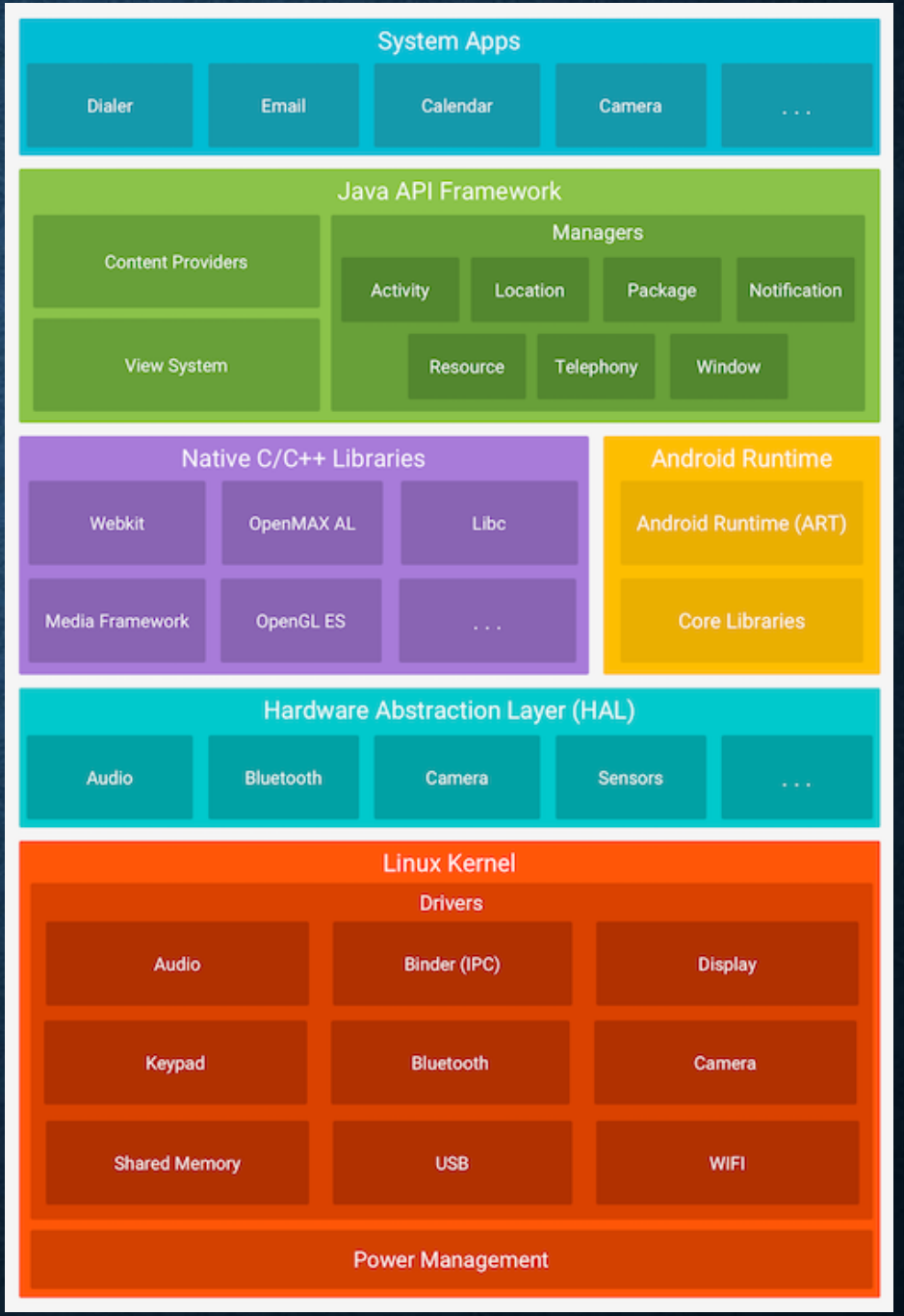
DEVICE REQUIREMENTS

- Android Penetration Testing
  - Windows, Kali linux, Parrot OS or MacBook
    - Preferable with 8-16GB of RAM or more and greater than 250GB of drive storage.
    - For Android interface
      - You can use emulator like (Android Studio (My fav) Memu, nox, bluestacks, Genymotion)
      - You can use rooted a physical device.

TOOLS REQUIREMENTS

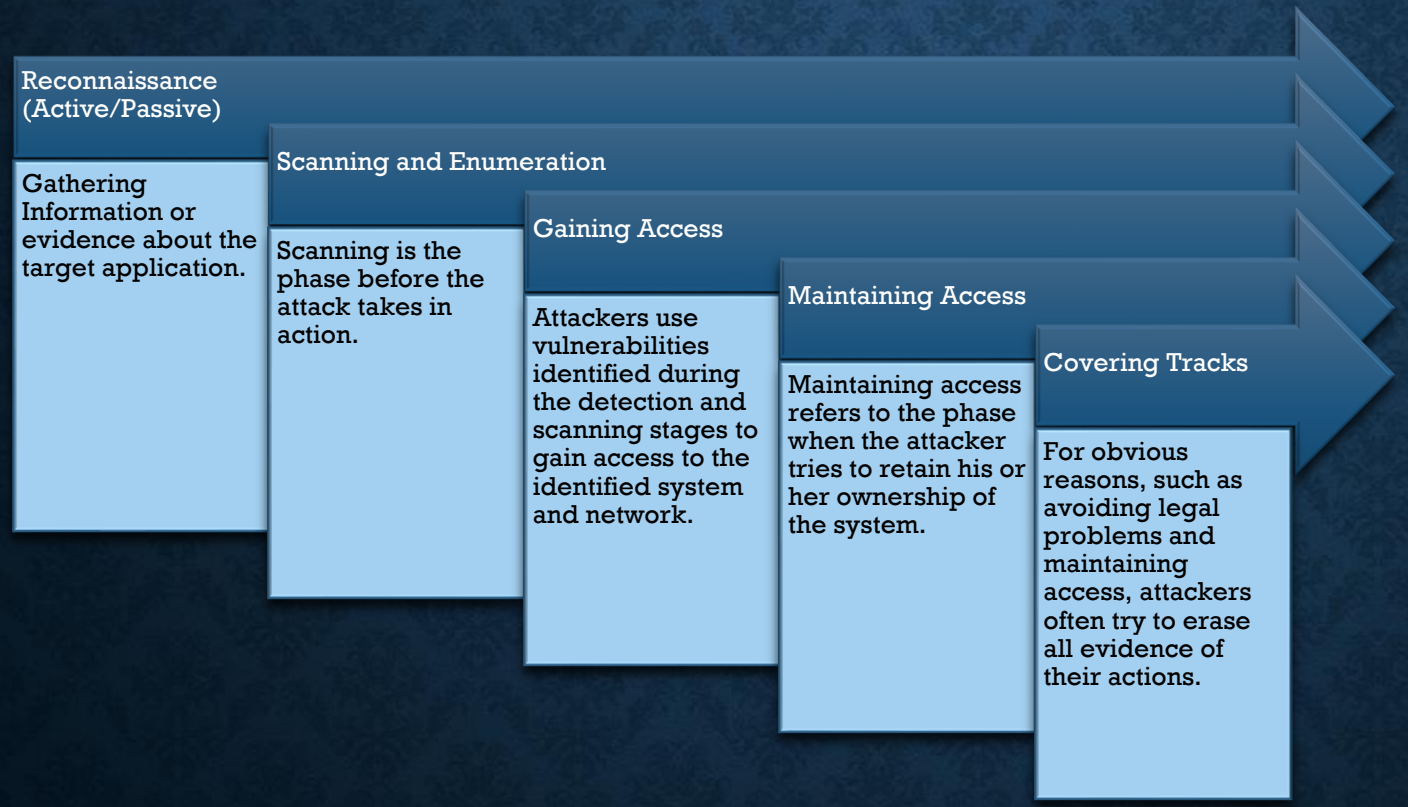
- JDAX-GUI
- APKTOOL
- MobSF
- Frida
- Objection
- BurpSuite

ANDROID ARCHITECTURE



Ref: OWASP Mobile Security Testing (Link)

LET'S TALK ABOUT PENETRATION TESTING PROCESS



PENETRATION TESTING

LET'S TALK ABOUT MOBILE APPLICATION PENETRATION TESTING PROCESS

MOBILE PENETRATION TESTING

SEE, WHO CAME

“THE ANDROID”

STATIC ANALYSIS

ANDROID MANIFEST FILE

- Extension is .xml
- You'll get basic information about the application
  - SDK version
  - Permission
  - Activities
  - Content Providers
  - Intent

PERMISSION

- Doesn't have any extension unfortunately 😐
- It defines what data and hardware component can be need at the runtime
  - Camera
  - Internet
  - Access external storage
  - Bluetooth
  - ETC.

ACTIVITIES

- It also do not have any extension too 😐
- UI element of the application or different screen in the application.

  (take example of Gpay)

  - First screen will show you Gpay Logo.
  - Second will ask you the Fingerprint.
  - Third will display all the payment you did in past.

NOTE: Here INTENT is changing from one screen to other.

FINDING HARDCODED STRINGS

- Usually find in resources/strings.xml
- Threat Vector
  - Login Bypass
  - URL's Exposed
  - API Keys Exposed
  - Firebase URL's

DYNAMIC ANALYSIS

ANDROID DYNAMIC ANALYSIS

- Intro to SSL Pinning
  - Bypassing with BurpSuite
- Intro Frida/Objection
  - Inject Frida Manually /Automatically
- Dumping Memory and Sensitive Data
- Runtime analysis of Local Storage

SSL PINNING

- It's a methodology which ensure no traffic will intercept from the application.
- Some application VERIFY the receiving traffic into the phone as KNOWN CERTIFICATE.
- App may crash when we try to intercept the network.

ROOT DETECTION

- An adversary will use an automated tool to reverse engineer the code and modify it using malware to perform some hidden functionality.
- Root detection are related to binaries
  - /system/bin/su
  - /system/xbin/su
  - /sbin/su
  - /system/su
  - /system/bin/.ext/.su

Q-n-A