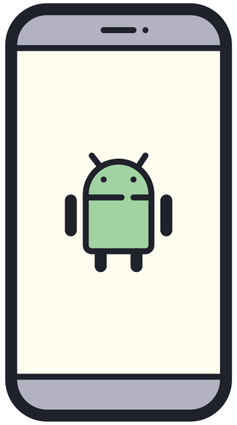


ANDROID PENETRATION TESTING 101

INTRODUCTION TO THE COURSE

Structure of the course

WE HAVE 4 MODULES

- Penetration Testing
- Basic Android Concepts
- Static Analysis
- Dynamic analysis

ANDROID PENETRATION TESTING

CHAPTER-1

TOPIC-1: PENETRATION TESTING

It describes the intentional launching of simulated cyberattacks that seek out exploitable vulnerabilities in computer systems, networks, websites, and applications.

CHAPTER-1

PHASES OF PENETRATION TESTING

CHAPTER-1

TOPIC-2: ANDROID PENETRATION TESTING

Android penetration testing is a process of finding security vulnerabilities in an android application. It is a systematic approach to searching for weaknesses in an Android app, verifying the app's security, and making sure it abides by the security policies.

CHAPTER-1

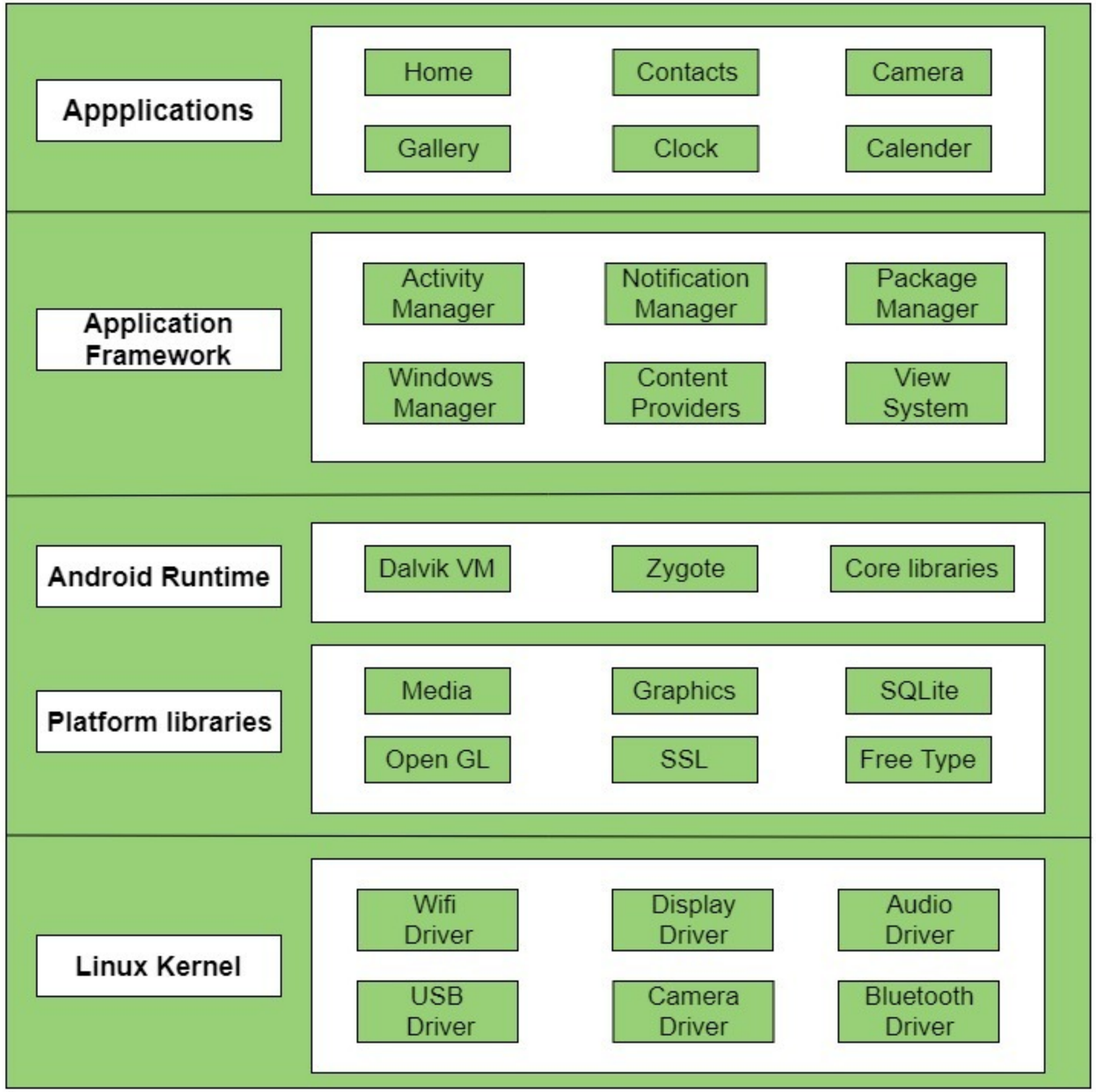
PHASES OF ANDROID PENETRATION TESTING

CHAPTER-2

TOPIC-1: ANDROID AND ITS ARCHITECTURE

Android is a mobile operating system based on a modified version of the Linux kernel and other open source software, designed primarily for touchscreen mobile devices such as smartphones and tablets.

CHAPTER-2



ANDROID ARCHITECTURE

BASIC ANDROID CONCEPTS

CHAPTER-2

LINUX KERNEL

It is the heart of android architecture. It manages all the available drivers such as display drivers, camera drivers, Bluetooth drivers, audio drivers, memory drivers, etc. which are required during the runtime.

Platform libraries

The Platform Libraries includes various C/C++ core libraries and Java based libraries such as Media, Graphics, Surface Manager, OpenGL etc. to provide a support for android development.

Application RunTime

Android Runtime environment is one of the most important parts of Android. It contains components like core libraries and the Dalvik virtual machine(DVM). Mainly, it provides the base for the application framework and powers our application with the help of the core libraries.

ANDROID ARCHITECTURE

CHAPTER-2

APPLICATION FRAMEWORK

Application Framework provides several important classes which are used to create an Android application. It provides a generic abstraction for hardware access and also helps in managing the user interface with application resources. Generally, it provides the services with the help of which we can create a particular class and make that class helpful for the Applications creation.

Applications

Applications are the top layer of the android architecture. The pre-installed applications like home, contacts, camera, gallery, etc, and third-party applications downloaded from the play store like chat applications, games, etc. will be installed on this layer only.

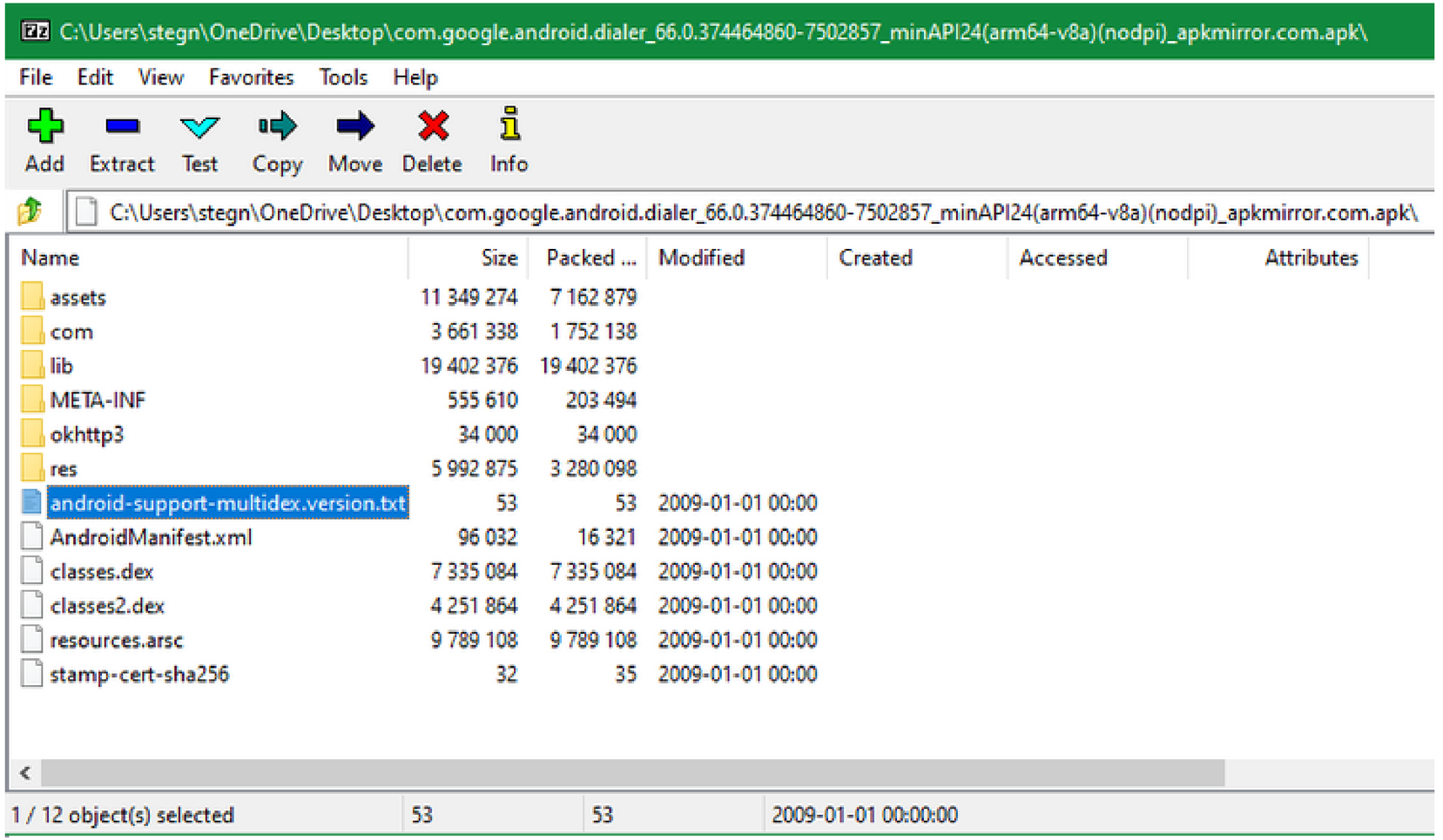
ANDROID ARCHITECTURE

CHAPTER-2

TOPIC-2: APK AND ITS STRUCTURE

- **APK stands for Android Package (sometimes Android Package Kit or Android Application Package). An APK is an archive file, meaning that it contains multiple files, plus some metadata about them.**
- **APK can be unpacked by Apktool, WinRAR, 7-zip, and other unzipping tools.**

CHAPTER-2



APK STRUCTURE

CHAPTER-2

TOPIC-3: ANDROID COMPONENTS AND LIFECYCLE

ACTIVITIES

Activities are said to be the presentation layer of our applications. The UI of our application is built around one or more extensions of the Activity class. By using Fragments and Views, activities set the layout and display the output and also respond to the user's actions.

SERVICES

Services are like invisible workers of our app. These components run at the backend, updating your data sources and Activities, triggering Notification, and also broadcast Intents. They also perform some tasks when applications are not active.

CHAPTER-2

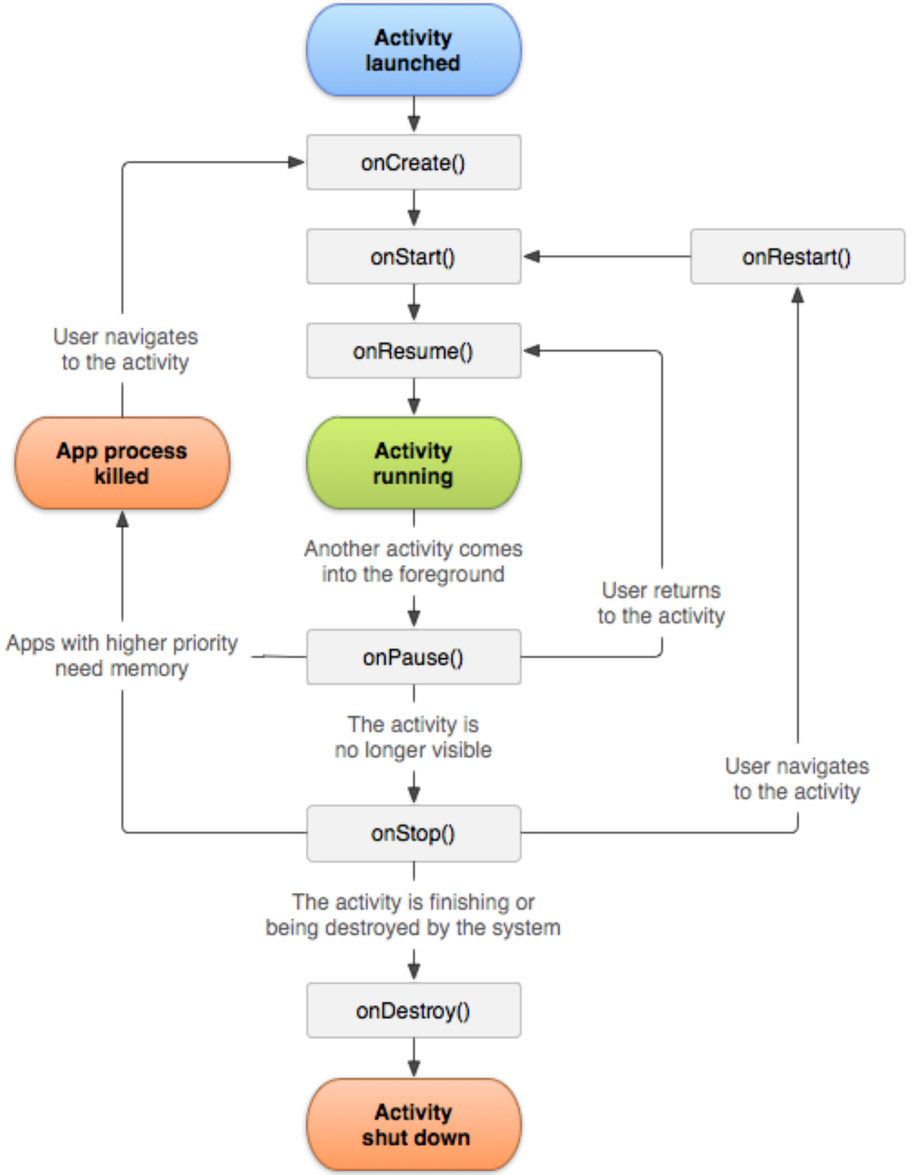
CONTENT PROVIDERS

It is used to manage and persist the application data also typically interacts with the SQL database. They are also responsible for sharing the data beyond the application boundaries. The Content Providers of a particular application can be configured to allow access from other applications, and the Content Providers exposed by other applications can also be configured.

BROADCAST RECEIVERS

They are known to be intent listeners as they enable your application to listen to the Intents that satisfy the matching criteria specified by us. Broadcast Receivers make our application react to any received Intent thereby making them perfect for creating event-driven applications.

CHAPTER-2



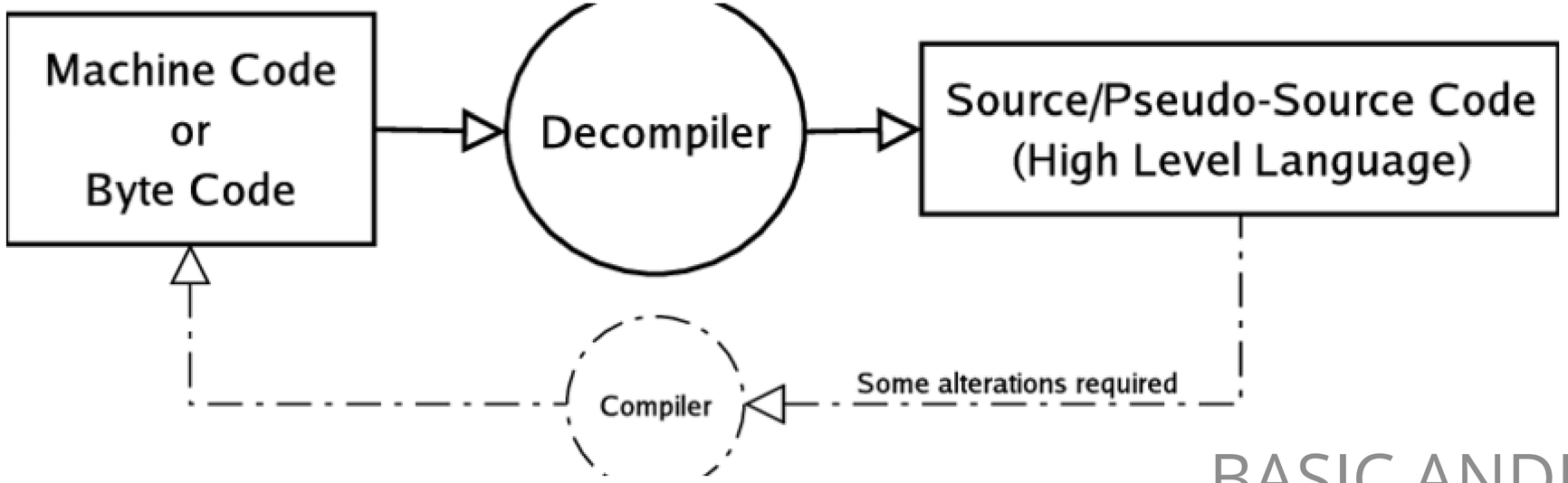
ANDROID LIFECYCLE METHODS

BASIC ANDROID CONCEPTS

CHAPTER-2

TOPIC-4: DECOMPILING AND DECOMPILERS

- **The process of converting the machine-level/Assembly level language to High-level language or pseudo source code.**



CHAPTER-2

- **A decompiler is a computer program that helps to convert machine level/computer-readable code to Pseudo source code/human-readable format.**

- **There are many android decompilers, but most used angd appropriate tools are Jadx-gui, GDA and JEB decompilers**

CHAPTER-3

TOPIC-1: STATIC ANALYSIS AND ITS IMPORTANCE

- **Static code analysis is a method of debugging by examining source code before a program is run. It's done by analyzing a set of code against a set (or multiple sets) of coding rules. This type of analysis addresses weaknesses in source code that might lead to vulnerabilities.**
- **The static analysis gives an understanding of business logic, it'll help to find hardcoded secrets or hardcoded IP and credentials.**

CHAPTER-3

TOPIC-2: INSTALLATION AND INTRODUCTION TO STATIC ANALYSIS TOOLS

CHAPTER-3

JADX-GUI

https://github.com/skylot/jadx/releases/tag/v1.3.1

GDA

https://github.com/charles2gan/GDA-android-reversing-Tool/releases

JNB

https://www.pnfsoftware.com/jeb/community-edition

CHAPTER-3

TOPIC-3: INSTALLATION AND INTRODUCTION TO MOBSF

CHAPTER-3

MOBSF

https://mobsf.github.io/docs/#/

CHAPTER-3

TOPIC-4: DEMONSTRATION OF STATIC ANALYSIS, COMMON VULNERABILITIES THAT CAN BE FOUND.

CHAPTER-4

TOPIC-1:DYNAMIC ANALYSIS AND ITS IMPORTANCE

- **Dynamic analysis, also known as dynamic program analysis, is the evaluation of a program or technology using real-time data. Instead of taking code offline, vulnerabilities and program behavior can be monitored while the program is running, providing visibility into its real-world behavior.**
- **To monitor the real-time data exchange between client and server, to identify whether the sensitive data is in transit. Also to identify the week endpoints.**

CHAPTER-4

TOPIC-2:DYNAMIC ANALYSIS LAB SETUP

BURPSUITE+GENYMOTION

CHAPTER-4

TOPIC-2: SSL-PINNING AND ITS IMPORTANCE

- **Pinning is an optional mechanism that can be used to improve the security of a service or site that relies on SSL Certificates. Pinning allows you to specify a cryptographic identity that should be accepted by users visiting your site**

- **Certificate pinning was originally created to protect against the threat of a rogue CA. Pinning also ensures that none of your app's network data is compromised even if a user has a malicious root certificate installed on their device**

CHAPTER-4

TOPIC-3: INSTALLATION AND INTRODUCTION TO FRIDA AND OBJECTION

CHAPTER-4

TOPIC-4: BYPASSING SSL-PINNING IN 3 DIFFERENT WAYS

CHAPTER-4

TOPIC-5: DEMONSTRATION OF DYNAMIC ANALYSIS

CHAPTER-5

TOPIC-1: ANDROID PENTESTING CHECKLIST

SUMMARY AND THANK YOU

CHAPTER-5

TOPIC-2: HIGHLIGHTS OF ANDROID PENETRATION TESTING 201

SUMMARY AND THANK YOU

CHAPTER-5

TOPIC-3: SUMMARY

CHAPTER-5

SUMMARY AND THANK YOU