1)

Select the correct statement regarding Android's ContentResolver:

- ContentResolver provides a **unified** interface for accessing and manipulating data across **different Android components in the same app**.
- ContentResolver provides a **dedicated** interface, **one for each Android app** accessing and manipulating the ContentProvider data.
- ContentResolver provides a **unified** interface for accessing and manipulating data across **different Android applications**. ✔

2)

What is the purpose of the Android sandbox?

- The Android sandbox isolates **third-party apps from system apps**, preventing malicious ones from accessing sensitive data or performing **unauthorized actions**.
- The Android sandbox isolates individual apps from **each other** and the **underlying OS**, preventing malicious ones from accessing **sensitive data** or performing **unauthorized actions**. ✔
- The Android sandbox isolates individual apps from the **underlying OS**, preventing malicious ones from accessing **sensitive data** or performing **unauthorized actions**.

3)

The Android signature

- is a security mechanism that **prevents repackaging attacks**
- is a security mechanism that guarantees the **trust in the Android app**
- is a security mechanism required for **building the Android sandbox** ✖

[correct: the first]

4)

The entry point of an Android app

- might be **any component**, as far as it has a **GUI**
- might be **any component**
- should always be the **Main Activity** ✖

[correct: the second]

5)

An Android app component declared in the app Manifest file

- can be reached by the **components of other apps** if it declares an **Intent Filter** and it is **exported**
- can be reached by the **components of other apps by default**
- can be reached by the **other components** of the same app only if it is **exported** ✖

[correct: the first]

6)

Considering explicit and implicit intents,

- the **implicit** intents are classified as **more secure** because the user can always choose the app to be started through the chooser
- the **implicit** intents are classified as **more secure** because the Android OS is responsible for redirecting them towards the appropriate target component
- the **explicit** intents are classified as **more secure** because they are intercepted only by the specific target component ✔

7)

The Android permission model is an example of

- a combination of MAC and DAC
- MAC ✖
- DAC

[correct: DAC]

8)

Select the correct statement

- Secure Boot is a process that checks the **integrity of the Android system** during the boot process, protecting against unauthorized modifications. ✔
- Secure Boot ensures that **only apps from verified developers** can be installed on the device
- Secure Boot is a feature that encrypts the device's storage to **prevent unauthorized access to user data**.

9)

Select the correct statement regarding Android's SafetyNet API:

- SafetyNet API provides a set of services that help protect **data confidentiality** and attests the **confidentiality of the device**.
- SafetyNet API provides a set of services that help protect against **device tampering** and attests the **integrity of the device**. ✔
- SafetyNet API provides a set of services that help protect against **app tampering** and attests the **integrity of the apps**.

10)

What is the purpose of Android's Runtime Environment (ART)?

- To **execute** application bytecode
- To **interpret** and **execute** application bytecode ✖
- To **compile** and **execute** application bytecode

[correct: the last]

11)

Binder is

- a communication mechanism between **Android devices**.
- a communication mechanism between **Android apps** and **system services**.
- a communication mechanism between **Android apps**. ✖

[correct: the second]

12)

Which technique allows to bypass a dynamic analysis approach?

- Obfuscated code
- Encrypted code
- Unreachable code ✔

13)

What is the primary goal of static analysis in Android security?

- To examine the **source code, Dalvik code and binary code** of an Android app without executing it.
- To examine the **source code** of an Android app without executing it. ✖
- To examine the **source code and binary code** of an Android app without executing it.

[correct: last one]

14)

Select the correct statement about taint analysis in Android security:

- Taint analysis is a method to identify **memory leaks in Android applications**.
- Taint analysis is used to track and identify the **flow of sensitive data within an application**. ✔
- Taint analysis helps **optimize code execution** by tracking data flow.

15)

16)

17)

What role does symbolic execution play in static analysis?

- Symbolic execution is a method to explore **all possible program paths** by using **symbolic values as inputs** to detect **vulnerabilities**.
- Symbolic execution is a method to explore **all possible program paths** by using **symbolic values as inputs** to prove **reachability**. ✖
- Symbolic execution is a method to explore **reachable program paths** by using **symbolic values as inputs** to detect **vulnerabilities**.

[correct: first one]

18)

Activities

- are **mandatory** components which serve as **entry points by default** ✖
- are **not mandatory** components and serve as **entry points by default**
- are **not mandatory** components and **may** serve as **entry points**

[correct: last one]