Iniziato	martedì, 9 gennaio 2024, 18:25
Stato	Completato
Terminato	martedì, 9 gennaio 2024, 18:39
Tempo impiegato	14 min. 23 secondi
Valutazione	**14,00** su un massimo di 17,00 (**82,35**%)

Domanda **1**

Risposta errata

Which statement accurately describes the role of Google SafetyNet Attestation in mobile app development?

○ a. Google SafetyNet Attestation ensures the security and integrity of the **device's hardware**.

● b. Google SafetyNet Attestation ensures the security and integrity of the **device's software**. ✗

○ c. Google SafetyNet Attestation ensures the security and integrity of the **device's software and hardware**.

Risposta errata.

La risposta corretta è:
Google SafetyNet Attestation ensures the security and integrity of the **device's software and hardware**.

Domanda **2**

Risposta corretta

Which of the following best describes the purpose of the Android bootloader in the device's boot process?

○ a. The bootloader determines the **order** in which system components are loaded during startup.

○ b. The bootloader is responsible for executing device **drivers** and managing **peripheral devices**.

● c. The bootloader verifies the **integrity** of the operating system and allows for its secure boot process. ✓

Risposta corretta.

La risposta corretta è:
The bootloader verifies the **integrity** of the operating system and allows for its secure boot process.

Domanda **3**

Risposta corretta

Which one is **NOT** a booting mode for a device?

● a. Debug mode. ✓

○ b. Recovery mode.

○ c. Normal mode.

Risposta corretta.

La risposta corretta è:
Debug mode.

Domanda **4**

Risposta corretta

What is the primary purpose of Android TrustZone in mobile device architecture?

○ a. TrustZone ensures **hardware-based** isolation for secure execution of **sensitive operations**.

● b. TrustZone ensures **hardware-based** isolation for secure execution of **sensitive operations and data**. ✓

○ c. TrustZone ensures **software-based** isolation for secure execution of **sensitive operations and data**.

Risposta corretta.

La risposta corretta è:
TrustZone ensures **hardware-based** isolation for secure execution of **sensitive operations and data**.

Domanda **5**

Risposta errata

Identify which one is an **UNCOMMON** threat model

○ a. Due to the Android OS fragmentation, **older or customized versions may have unpatched vulnerabilities**. Attackers can target specific OS versions or take advantage of inconsistencies across devices.

○ b. **Installation of malicious apps** that are disguised as legitimate applications and may perform activities such as data theft, unauthorized access, or aggressive advertising.

● c. **Android devices connected to various networks**, including public Wi-Fi networks, which can expose them to network-based attacks. ✗

Risposta errata.

La risposta corretta è:
Due to the Android OS fragmentation, **older or customized versions may have unpatched vulnerabilities**. Attackers can target specific OS versions or take advantage of inconsistencies across devices.

Domanda **6**

Risposta corretta

Which classes of attacker can we have in a threat model?

○ a. Remote, close or local

◉ b. Remote, proximal or local ✓

○ c. External, proximal or internal

Risposta corretta.

La risposta corretta è:
Remote, proximal or local

Domanda **7**

Risposta corretta

Select the correct statement

◉ a. Attackers rely on **security vulnerabilities** to bypass the **technical gap** between the **threat model** and the **attacker's aim**. ✓

○ b. Attackers rely on **security exploits** to bypass the **technical gap** between the **threat model** and the **attacker's aim**.

○ c. Attackers rely on **security vulnerabilities** to bypass the **technical gap** between the **defence model** and the **attacker's aim**.

Risposta corretta.

La risposta corretta è:
Attackers rely on **security vulnerabilities** to bypass the **technical gap** between the **threat model** and the **attacker's aim**.

Domanda **8**

Risposta corretta

Which one is **NOT** a vulnerability type?

○ a. Elevation of privilege

○ b. Information disclosure

◉ c. OS fragmentation ✓

Risposta corretta.

La risposta corretta è:
OS fragmentation

Domanda **9**

Risposta corretta

What is a repackaging attack?

● a. It is a malicious technique where an attacker **modifies** an **existing** app by adding malicious code and **redistributing** it. ✓

○ b. It is a malicious technique where an attacker **modifies** an **existing** app by adding malicious code at **runtime**.

○ c. It is a malicious technique where an attacker **creates a new** app by adding malicious code and **redistributing** it.

Risposta corretta.

La risposta corretta è:
It is a malicious technique where an attacker **modifies** an **existing** app by adding malicious code and **redistributing** it.

Domanda **10**

Risposta corretta

What is symbolic execution?

● a. Symbolic execution is a method that explores **all possible program paths** by using symbolic values as inputs to **detect program vulnerabilities** or **generate test cases**. ✓

○ b. Symbolic execution is a method that explores **all possible program paths** by using symbolic values as inputs to **cause program crashes**.

○ c. Symbolic execution is a method that explores **all reachable program paths** by using symbolic values as inputs to **launch exploits**.

Risposta corretta.

La risposta corretta è:
Symbolic execution is a method that explores **all possible program paths** by using symbolic values as inputs to **detect program vulnerabilities** or **generate test cases**.

Domanda **11**

Risposta corretta

What is the primary purpose of the Android Zygote process?

○ a. It manages the **communication between the Android runtime and the hardware components**.

● b. It handles the **management of app processes and their life cycles**. ✓

○ c. It is responsible for **compiling and optimizing the Java bytecode** of Android apps.

Risposta corretta.

La risposta corretta è:
It handles the **management of app processes and their life cycles**.

Domanda 12

Risposta corretta

Which information is **NOT** contained in an Android app certificate?

○ a. The issuer, i.e. the entity that issued the certificate.

○ b. The validity period.

● c. The developer private key. ✓

Risposta corretta.

La risposta corretta è:
The developer private key.

Domanda 13

Risposta corretta

How does a bound service in Android communicate with components in the application?

○ a. Bound services communicate using **explicit intents**.

○ b. Bound services use **broadcast receivers** for communication.

● c. Bound services provide an **interface** through which components can bind and communicate. ✓

Risposta corretta.

La risposta corretta è:
Bound services provide an **interface** through which components can bind and communicate.

Domanda 14

Risposta corretta

How does an Android Content Provider facilitate data sharing between different applications?

● a. Content Providers provide a **structured interface** for accessing and sharing data between applications. ✓

○ b. Content Providers use **implicit intents** to share data between applications.

○ c. Content Providers **expose a set of APIs** for inter-process communication.

Risposta corretta.

La risposta corretta è:
Content Providers provide a **structured interface** for accessing and sharing data between applications.

Domanda **15**

Risposta corretta

The Android instrumentation

- ● a. provides a framework for running tests on Android applications, automating interactions, and monitoring the application's behavior **during testing and debugging**. ✓
- ○ b. provides a framework for running tests on Android applications, automating interactions, and monitoring the application's behavior **during the compilation**.
- ○ c. provides a framework for running tests on Android applications, automating interactions, and monitoring the application's behavior **during the development**

Risposta corretta.

La risposta corretta è:
provides a framework for running tests on Android applications, automating interactions, and monitoring the application's behavior **during testing and debugging**.

Domanda **16**

Risposta corretta

What is the purpose of taint analysis?

- ● a. to track and identify the **data flow**. ✓
- ○ b. to help in **optimizing** code execution.
- ○ c. to identify **memory leaks** in a software application.

Risposta corretta.

La risposta corretta è:
to track and identify the **data flow**.

Domanda **17**

Risposta errata

Which technique is mostly affected by scalability issues?

- ● a. Dynamic analysis. ✖
- ○ b. Taint analysis.
- ○ c. Static analysis.

Risposta errata.

La risposta corretta è:
Static analysis.

Iniziato	venerdì, 6 ottobre 2023, 08:41
Stato	Completato
Terminato	venerdì, 6 ottobre 2023, 08:47
Tempo impiegato	5 min. 31 secondi
Valutazione	**7,00** su un massimo di 10,00 (**70**%)

Domanda **1**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

What are the main features of the system apps?

○ a. They are considered more secure than user installed apps, they can be uninstalled, they are installed under the /system partition

○ b. They are considered more secure than user installed apps, they cannot be uninstalled, they are installed under the /data partition

● c. They are considered more secure than user installed apps, they cannot be uninstalled, they are installed under the /system partition ✓

Risposta corretta.

La risposta corretta è:
They are considered more secure than user installed apps, they cannot be uninstalled, they are installed under the /system partition

Domanda **2**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

An Android app very likely has

○ a. multiple UID and multiple GIDs

○ b. a unique UID and multiple GIDs

● c. a unique UID ✓

Risposta corretta.

La risposta corretta è:
a unique UID

Domanda **3**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Webmail | Uniweb

System services provide unique Android features and

- ○ a. they run in the same process of the invoking app
- ● b. they can be queried through alternative mechanisms than IPC ✗
- ○ c. they run in dedicated processes

Risposta errata.

La risposta corretta è:
they run in dedicated processes

Domanda **4**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

The Android sandbox model guarantees isolation

- ○ a. only at the file system level
- ● b. at both the process and the system file level ✓
- ○ c. only at the process level

Risposta corretta.

La risposta corretta è:
at both the process and the system file level

Domanda **5**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

An Android app has many entry points

- ○ a. as the number of components declared in the manifest file
- ● b. as the number of exported components declared in the manifest file ✓
- ○ c. as the number of activities declared in the manifest file

Risposta corretta.

La risposta corretta è:
as the number of exported components declared in the manifest file

Domanda **6**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Webmail | Uniweb

The Android OS is event-driven, which means that

● a. whenever there is an event, the sender app finds the components able to handle it and forwards the event to them ✗

○ b. whenever there is an event, the Android OS finds the components able to handle it and forwards the event to them

○ c. whenever there is an event, the components able to handle it automatically intercept it

Risposta errata.

La risposta corretta è:
whenever there is an event, the Android OS finds the components able to handle it and forwards the event to them

Domanda **7**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Explicit intents

● a. are more secure than implicit ones ✓

○ b. are secure as much as the implicit ones

○ c. are less secure than implicit ones

Risposta corretta.

La risposta corretta è:
are more secure than implicit ones

Domanda **8**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

App signature

○ a. can be used to check the identity of the developers with trust towards them

● b. can be used to check the identity of the developers without any trust towards them ✓

Risposta corretta.

La risposta corretta è:
can be used to check the identity of the developers without any trust towards them

Domanda **9**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Webmail | Uniweb

Android permissions

○ a. cannot be changed after the app installation

○ b. can be changed after the app installation if the app is updated, too

● c. can be changed after the app installation ✗

Riepilogo della conservazione dei dati

Politiche

Ottieni l'app mobile

Risposta errata.

La risposta corretta è:
can be changed after the app installation if the app is updated, too

Domanda **10**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Android permissions

○ a. are all automatically granted at runtime

● b. are granted at different times according to their severity level ✓

○ c. are all automatically granted at the installation time

Risposta corretta.

La risposta corretta è:
are granted at different times according to their severity level

Iniziato	venerdì, 13 ottobre 2023, 08:38
Stato	Completato
Terminato	venerdì, 13 ottobre 2023, 08:48
Tempo impiegato	9 min. 31 secondi
Punteggio	6,00/7,00
Valutazione	**8,57** su un massimo di 10,00 (**85,71**%)

Domanda **1**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Two apps can have a sharedUserID if

○ a. they share the same signature

○ b. they share the same AndroidManifest file

● c. they share the same package name and the same signature ✗

Risposta errata.

La risposta corretta è:
they share the same signature

Domanda **2**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Why do we need a separation between user space and kernel space?

● a. because apps can contain malicious code and might complete malicious actions if given access to the kernel space ✓

○ b. because apps are sandboxed

○ c. because this is how Linux works

Risposta corretta.

La risposta corretta è:
because apps can contain malicious code and might complete malicious actions if given access to the kernel space

Domanda **3**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

The binder kernel driver allows an app to

○ a. be executed and interact with other apps

○ b. be executed

● c. be executed, interact with other apps and access to shared resources ✓

Risposta corretta.

La risposta corretta è:
be executed, interact with other apps and access to shared resources

Domanda **4**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Normal permissions

● a. are automatically granted without the user involvement ✓

○ b. are automatically granted with a notification to inform the user

○ c. are granted at runtime

Risposta corretta.

La risposta corretta è:
are automatically granted without the user involvement

Domanda **5**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Signature permissions are granted to

○ a. system apps

○ b. apps signed with the platform keys

● c. apps signed with the same signature as the app defining the permission ✓

Risposta corretta.

La risposta corretta è:
apps signed with the same signature as the app defining the permission

Domanda **6**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

A component declared in the manifest file

● a. in older Android versions, is exported by default if it declares also an intent filter ✓

○ b. is exported by default if it is an activity

○ c. is exported by default

Risposta corretta.

La risposta corretta è:
in older Android versions, is exported by default if it declares also an intent filter

Domanda **7**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

In Android, what is the relationship between app permissions and GIDs (Group IDs)?

○ a. Android app permissions and GIDs are unrelated; they serve different security purposes within the Android ecosystem.

● b. Each Android permission corresponds to a unique GID, allowing apps with specific permissions to access resources and services within their associated GID. ✓

○ c. Android app permissions are associated with various system-defined GIDs, granting apps access to resources and services based on their assigned GID.

Risposta corretta.

La risposta corretta è:
Each Android permission corresponds to a unique GID, allowing apps with specific permissions to access resources and services within their associated GID.

Iniziato	venerdì, 20 ottobre 2023, 08:34
Stato	Completato
Terminato	venerdì, 20 ottobre 2023, 08:42
Tempo impiegato	7 min. 36 secondi
Punteggio	7,00/9,00
Valutazione	**7,78** su un massimo di 10,00 (**77,78**%)

Domanda **1**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

What is the main purpose of Android signatures?

○ a. Verifying the developers' real identity

● b. Distinguishing between developers ✓

○ c. Identifying developers

Risposta corretta.

La risposta corretta è:
Distinguishing between developers

Domanda **2**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

What else can an app signature used for?

○ a. Guaranteeing the Android permission model

○ b. Guaranteeing the integrity of an Android app content

● c. Guaranteeing the Android sandbox model ✗

Risposta errata.

La risposta corretta è:
Guaranteeing the integrity of an Android app content

Domanda **3**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

If you try to install an app with the same package name of a different one that is already installed

- ● a. the Android OS will check the signature of the new one and, if equal to the already installed one, it will update the latter with the former ✓
- ○ b. the Android OS will deny the installation of the new app by default
- ○ c. the Android OS will check the signature of the new one and, if both apps have a sharedUserID, it will update the old with the new one

Risposta corretta.

La risposta corretta è:
the Android OS will check the signature of the new one and, if equal to the already installed one, it will update the latter with the former

Domanda **4**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Which of the following is true about Android app signatures?

- ● a. Every Android app must be signed with a certificate. ✓
- ○ b. Android apps can be distributed without any signature.
- ○ c. Android app signatures are optional.

Risposta corretta.

La risposta corretta è:
Every Android app must be signed with a certificate.

Domanda **5**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

How are Android app certificates managed in the development process?

- ● a. Developers create and manage their own certificates. ✓
- ○ b. All Android apps share a common certificate.
- ○ c. Certificates are not required during development.

Risposta corretta.

La risposta corretta è:
Developers create and manage their own certificates.

Domanda **6**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Which type of certificate is typically used for Android apps during the development?

○ a. Release certificate

● b. Self-signed certificate ✓

○ c. Debug certificate

Risposta corretta.

La risposta corretta è:
Self-signed certificate

Domanda **7**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Why is it essential to protect the private key associated with an Android app certificate?

○ a. To improve the app's user interface

○ b. To ensure compatibility with older devices

● c. To prevent unauthorized signing of apps ✓

Risposta corretta.

La risposta corretta è:
To prevent unauthorized signing of apps

Domanda **8**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

How can you generate a self-signed certificate for Android app development?

● a. Generate it using the keytool or a similar tool ✓

○ b. Use a built-in Android system certificate

○ c. Purchase it from Google Play Store

○ d. Request one from a Certificate Authority (CA)

Risposta corretta.

La risposta corretta è:
Generate it using the keytool or a similar tool

Domanda **9**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

How can you check the certificate information of an installed Android app?

○ a. Using the "keytool" command or a certificate viewer tool

○ b. Through the "About" section of the app

● c. By looking at the app's source code ✖

Risposta errata.

La risposta corretta è:
Using the "keytool" command or a certificate viewer tool

Iniziato	venerdì, 27 ottobre 2023, 09:16
Stato	Completato
Terminato	venerdì, 27 ottobre 2023, 09:24
Tempo impiegato	7 min. 39 secondi
Valutazione	**6,00** su un massimo di 8,00 (**75**%)

Domanda **1**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Activities

○ a. can run automatically

● b. are the only way for a user to interact with an app ✓

○ c. can perform long-running operations

Risposta corretta.

La risposta corretta è:
are the only way for a user to interact with an app

Domanda **2**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Activities transitions between states are

○ a. triggered by the user

● b. triggered by the user and by events sent by the OS ✓

○ c. triggered by events sent by the OS

Risposta corretta.

La risposta corretta è:
triggered by the user and by events sent by the OS

Domanda **3**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Services

- ● a. should be started through explicit intents ✓
- ○ b. should be started through both explicit and implicit intents
- ○ c. should be started through implicit intents

Risposta corretta.

La risposta corretta è:
should be started through explicit intents

Domanda **4**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

A bound service keeps running

- ○ a. until it completes its action
- ● b. until one of the calling component is running ✓
- ○ c. until the Android OS decides so

Risposta corretta.

La risposta corretta è:
until one of the calling component is running

Domanda **5**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

If a calling component wants to communicate with a service, it should rely on

- ○ a. messengers or AIDL
- ○ b. intents
- ● c. broadcast events ✗

Risposta errata.

La risposta corretta è:
messengers or AIDL

Domanda **6**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Broadcast receivers

○ a. intercept explicit intents

○ b. intercept any system wide events

● c. intercept specific system wide events ✓

Risposta corretta.

La risposta corretta è:
intercept specific system wide events

Domanda **7**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

A content provider authority can handle

○ a. a single table

● b. multiple tables of the same content provider ✓

○ c. multiple tables of different content providers

Risposta corretta.

La risposta corretta è:
multiple tables of the same content provider

Domanda **8**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Content Providers

● a. might depend from the underlying structure of the data source according to the developer ✗

○ b. do not depend from the underlying structure of the data source

○ c. depend from the underlying structure of the data source

Risposta errata.

La risposta corretta è:
do not depend from the underlying structure of the data source

1) From which Android version was ART originally introduced?

a. 8.0

b. 6.0

c. 4.4

It was introduced in 4.4, so it became the standard soon after

2) Why did Google introduce DVM in Android?

a. Due to performance issues, because Android is a mobile OS and it has more hardware restrictions than a desktop OS

b. For security reasons, because the DVM can guarantee the isolation among apps

c. For performance reasons because the execution of an app is faster when performed inside a DVM

The third one is not formally wrong, but the first one it’s more correct, we must say.

3) A dex file contains

a. the Dalvik bytecode obtained after the compilation of Java, Kotlin and C/C++ source code

b. the Dalvik bytecode obtained after the compilation of Java and Kotlin source code

c. the Dalvik bytecode obtained after the compilation of C/C++ source code

For C/C++ everything is compiled inside shared objects, while Java/Dalvik is bytecode for the machine.

4) Resources are

a. zipped in the APK file in a compressed format

b. compiled into the APK file

c. zipped in the APK file in an uncompressed format

The resources are not compiled, inside the compressed resources there are Manifest/Classes/Resources files compressed.

5) What is the main difference between DVM and ART?

a. The compilation procedure of Dalvik bytecode into machine code

b. The compilation procedure of Java source code into Dalvik bytecode

c. The compilation procedure of Java source code into binary code

6) What is the main criterion used by the current Android versions to compile an app code AOT?

a. methods that are classified as "hot" ones are compiled AOT

b. by default, all methods of the Android framework are compiled AOT

c. by default, all methods of the developers' custom code are compiled AOT

The mirrored classes are created inside the Android compiler and creates something that can be used for the AOT mechanism.

7) Zygote is...

a. the name of the process in which a system service is executed

b. the name of the process in which an app is executed

c. the parent process of all the apps as the processes they execute in are forked from Zygote

8) What's the difference between the files boot.art and boot.oat?

a. boot.art contains pre-initialized classes and objects from the Android framework, while boot.oat contains pre-compiled classes from the Android framework
b. boot.art contains pre-initialized classes and objects from the developers' custom code, while boot.oat contains pre-compiled classes from developers' custom code
c. boot.oat contains pre-initialized classes and objects from the developers' custom code, while boot.art contains pre-compiled classes from developers' custom code

The part of the framework is inside the ART files, which happens just copy-pasting inside Android files, while developers' code in the answer does not matter.

9) Disassembling means...

a. Obtaining the uncompressed Dalvik bytecode from the compressed one
b. Obtaining the C/C++ source code from a shared object file
c. Obtaining the Java source code from the Dalvik bytecode

The disassembling procedure revolves around conversion also for C/C++ files, but here we take the bytecode and make it in a format which is human-readable. Here there is a mapping between unconverted/converted code.

10) Decompiling means...

a. Obtaining the Dalvik bytecode from the machine code
b. Obtaining the Java source code from the Dalvik bytecode
c. Obtaining the assembly code from a shared object file

The third option is again diassembling, the first is again the compiling, while the second option is the right one, where we take the procedure.

Iniziato	venerdì, 10 novembre 2023, 08:34
Stato	Completato
Terminato	venerdì, 10 novembre 2023, 08:42
Tempo impiegato	7 min. 37 secondi
Valutazione	**7,00** su un massimo di 10,00 (**70**%)

Domanda **1**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Among the following ones identify which is NOT a limitation for a static analysis approach

○ a. Reflection

○ b. Amount of app's code

● c. Dynamic code loading ✖

○ d. Obfuscated strings

○ e. Obfuscated code

Risposta errata.

La risposta corretta è:
Amount of app's code

Domanda **2**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Among the following ones identify which one is a limitation for a dynamic analysis approach

○ a. Reflection

○ b. Obfuscated strings

○ c. Obfuscated code

● d. Dynamic code loading ✖

Risposta errata.

La risposta corretta è:
Reflection

Domanda **3**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Debugging means

○ a. that you insert new source code in the app which is going to be executed at runtime

○ b. that you insert new smali code in the app which is going to be executed at runtime

● c. that you have a debugger running in a different process of the app's one and that one injects interrupt signals to stop the execution of the app and inspect the runtime values of its memory ✓

Risposta corretta.

La risposta corretta è:
that you have a debugger running in a different process of the app's one and that one injects interrupt signals to stop the execution of the app and inspect the runtime values of its memory

Domanda **4**

Risposta errata

Punteggio ottenuto 0,00 su 1,00

Instrumentation means

○ a. that you inject new code in the app at runtime

● b. that you trace all the APIs invoked by an app ✗

○ c. that you stop the runtime execution of the app and modify its variables values

Risposta errata.

La risposta corretta è:
that you inject new code in the app at runtime

Domanda **5**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Taint analysis is used for...

● a. tracking the flow of sensitive data within an app ✓

○ b. intercepting the communication between different app's components

○ c. intercepting the communication between two apps

Risposta corretta.

La risposta corretta è:
tracking the flow of sensitive data within an app

Domanda **6**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Symbolic execution is generally used for...

● a. build a general model based on input variables that could lead to the execution of different paths in the app ✓

○ b. trace the sensitive data flow within an app

○ c. trace the APIs invoked by an app

Risposta corretta.

La risposta corretta è:
build a general model based on input variables that could lead to the execution of different paths in the app

Domanda **7**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Code coverage is

○ a. the amount of code available inside an app

● b. the amount of code inside an app that you are able to execute ✓

○ c. the amount of code dynamically loaded by an app at runtime

Risposta corretta.

La risposta corretta è:
the amount of code inside an app that you are able to execute

Domanda **8**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Which technique is used for evading static analysis?

○ a. smali code

○ b. Java/kotlin source code

● c. native code ✓

Risposta corretta.

La risposta corretta è:
native code

Domanda **9**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Webmail | Uniweb

A malware can bypass dynamic analysis techniques by

○ a. dynamically loading new code at runtime

● b. detecting that it is under debugging/instrumentation and thus hiding its malicious behaviour ✓

○ c. using encrypted network traffic

Risposta corretta.

La risposta corretta è:
detecting that it is under debugging/instrumentation and thus hiding its malicious behaviour

Domanda **10**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Riepilogo della conservazione dei dati Ottieni l'app mobile
Politiche

Any assumption that is acquired through a static analysis

○ a. is always true

● b. should be validated through a dynamic analysis ✓

○ c. is always false

Risposta corretta.

La risposta corretta è:
should be validated through a dynamic analysis

Iniziato	venerdì, 1 dicembre 2023, 08:33
Stato	Completato
Terminato	venerdì, 1 dicembre 2023, 08:39
Tempo impiegato	5 min. 41 secondi
Valutazione	**6,00** su un massimo di 9,00 (**66,67**%)

Domanda **1**

Risposta errata

Which one is the least likely motivation for developing a malware?

○ a. Financial gain

○ b. Causing chaos, damaging devices, or disrupting the normal functioning of systems

● c. Espionage ✖

Risposta errata.

La risposta corretta è:
Causing chaos, damaging devices, or disrupting the normal functioning of systems

Domanda **2**

Risposta corretta

Which of the following malware types is least likely to exploit SMS premium services for unauthorized charges or subscriptions in Android?

○ a. Spyware

● b. Keyloggers ✓

○ c. Adware

Risposta corretta.

La risposta corretta è:
Keyloggers

Domanda **3**

Risposta corretta

Which of the following actions is least associated with mobile ransomware?

○ a. Encrypting files and demanding a ransom for decryption.

● b. Displaying intrusive advertisements on the device. ✓

○ c. Locking the device and demanding a ransom for unlocking.

Risposta corretta.

La risposta corretta è:
Displaying intrusive advertisements on the device.

Domanda **4**

Risposta corretta

Which of the following activities is least associated with spyware on mobile devices?

○ a. Gathering sensitive information such as login credentials and personal data.

○ b. Monitoring and recording user's keystrokes and online activities.

● c. Displaying intrusive advertisements on the device. ✓

Risposta corretta.

La risposta corretta è:
Displaying intrusive advertisements on the device.

Domanda **5**

Risposta corretta

Who DOES NOT gain money in an advertisement framework used in a mobile context?

○ a. The advertisement framework developer

● b. The user ✓

○ c. The mobile app developer

Risposta corretta.

La risposta corretta è:
The user

Domanda **6**

Risposta corretta

Which of the following is NOT a characteristic of adware?

○ a. It can slow down your mobile device.

● b. It is a type of virus. ✓

○ c. It displays unwanted advertisements.

Risposta corretta.

La risposta corretta è:
It is a type of virus.

Domanda 7

Risposta corretta

Which of the following is a way to prevent cross-device tracking on mobile devices?

○ a. Disable ad tracking in your mobile device's settings.

● b. All of the above. ✓

○ c. Use a VPN or Tor.

Risposta corretta.

La risposta corretta è:
All of the above.

Domanda 8

Risposta errata

Which one is NOT a possible way for an attacker to install a malware on the victim device?

● a. Social engineering ✗

○ b. Repackaging attack

○ c. Triggering the automatic installation of the malware

Risposta errata.

La risposta corretta è:
Triggering the automatic installation of the malware

Domanda 9

Risposta errata

Which of the following statements least accurately describes an Android repackaging attack?

● a. An Android repackaging attack disguises malicious code within a legitimate app to deceive users and bypass security measures. ✗

○ b. An Android repackaging attack involves modifying a legitimate app's package name and signing it with a different digital certificate.

○ c. An Android repackaging attack is a technique used to intercept and modify network traffic between an Android device and external servers.

Risposta errata.

La risposta corretta è:
An Android repackaging attack is a technique used to intercept and modify network traffic between an Android device and external servers.

1) Which of the following actions is an attacker not able to perform when gaining root access on a device, thus introducing a novel attack if managing to complete it?

a. Install and run a malicious app

b. Modify system files and configurations

c. Perform a software update for increased security

2) Specify which of the following attack scenarios is less common:

a. NFC Hacking

b. Phishing Attacks

c. Malicious App Downloads

3) Assuming the attacker can lure the victim to visit an arbitrary URL, which attack would not be able to complete?

a. Remote Device Takeover

b. Drive-By Downloads

c. Phishing Attack

4) If an attacker successfully runs code in the kernel of a mobile device, which attacks cannot he complete?

a. Rootkit Installation

b. Privilege Escalation

c. Complete Remote Control

5) Which of the following statements accurately describes the process of exploitation in cybersecurity?

a. Exploitation is the process of "taking advantage" of a vulnerability so that an attacker can perform unintended actions.

b. Exploitation is the process of enhancing system performance and efficiency.

c. Exploitation is the process of identifying and patching vulnerabilities in software.

6) When assessing the severity and relevance of a bug, what factors play a crucial role in determining its impact?

a. The combination of the "type" of bug and "where" it is (i.e., which component is affected).

b. The programming language used to develop the software.

c. The target victim device.

7) Among the following ones, select which is NOT an EOP attack

(where EOP = Escalation Of Privilege, I write it for you to remember)

a. Remote attacker ⇒ local attacker

b. Attacker with code execution with app's sandbox ⇒ write files in its private directory

c. Attacker with code execution with app's sandbox ⇒ system user/root

What does the term "attack surface" refer to in the context of cybersecurity?

8) What does the term "attack surface" refer to in the context of cybersecurity?

a. The sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.

b. The level of encryption used to protect sensitive data.

c. The total number of physical servers in an organization's data center.

Iniziato	domenica, 17 dicembre 2023, 11:15
Stato	Completato
Terminato	domenica, 17 dicembre 2023, 11:15
Tempo impiegato	28 secondi
Valutazione	**5,00** su un massimo di 6,00 (**83,33**%)

Domanda **1**

Risposta corretta

Select which attack does not involve social engineering among the following ones:

◉ a. Data Masking: a technique used to protect sensitive information by replacing it with fictional or obfuscated data ✓

○ b. Phishing: sending fraudulent emails or messages that appear to be from a trustworthy source to deceive individuals into revealing sensitive information or performing certain actions

○ c. Impersonation: Pretending to be someone else, such as a coworker or a representative from a reputable organization, to gain trust and manipulate individuals into providing confidential information

Risposta corretta.

La risposta corretta è:
Data Masking: a technique used to protect sensitive information by replacing it with fictional or obfuscated data

Domanda **2**

Risposta corretta

How can you attack an app by exploiting dynamic code loading technique?

○ a. By inspecting the code to be dynamically loaded in the private directory of the app

◉ b. By replacing the original downloaded binary file with a malicious one ✓

○ c. By sniffing the network traffic during the download of the binary file from a remote server

Risposta corretta.

La risposta corretta è:
By replacing the original downloaded binary file with a malicious one

Domanda **3**

Risposta errata

Which is NOT a possible reason that leads towards cryptographic vulnerabilities?

- ● a. Misuse of cryptographic libraries ✖
- ○ b. Network traffic in cleartext
- ○ c. Poor implementation of cryptographic libraries

Risposta errata.

La risposta corretta è:
Network traffic in cleartext

Domanda **4**

Risposta corretta

What is the Android Confused Deputy attack, and how does it work? Select the correct answer

- ● a. The Confused Deputy attack is a security vulnerability that occurs when an Android app grants excessive permissions to other apps without appropriate authorization checks. It allows a malicious app to misuse the granted permissions and access sensitive user data or perform unauthorized actions. ✔
- ○ b. The Confused Deputy attack is a method of exploiting vulnerabilities in the Android operating system to gain unauthorized root access to a device. It works by bypassing the security mechanisms and gaining escalated privileges.
- ○ c. The Confused Deputy attack is a social engineering technique where an attacker tricks an Android user into downloading and installing a malicious app that steals sensitive information. The attack typically involves phishing emails or fake app stores.

Risposta corretta.

La risposta corretta è:
The Confused Deputy attack is a security vulnerability that occurs when an Android app grants excessive permissions to other apps without appropriate authorization checks. It allows a malicious app to misuse the granted permissions and access sensitive user data or perform unauthorized actions.

Domanda **5**

Risposta corretta

What is Android overpermissioning, and what are its implications?

○ a. Android overpermissioning refers to the practice of granting unnecessary permissions to Android apps, leading to reduced performance and increased battery consumption.

○ b. Android overpermissioning is a technique used by malicious apps to gain unauthorized access to user data by exploiting vulnerabilities in the Android operating system.

● c. Android overpermissioning is the phenomenon where Android apps request more permissions than necessary for their intended functionality. This can potentially expose user data to privacy risks and increase the attack surface for potential security breaches. ✓

Risposta corretta.

La risposta corretta è:
Android overpermissioning is the phenomenon where Android apps request more permissions than necessary for their intended functionality. This can potentially expose user data to privacy risks and increase the attack surface for potential security breaches.

Domanda **6**

Risposta corretta

What is zip path traversal, and how does it pose a security risk?

○ a. Zip path traversal is a feature in ZIP compression that allows users to navigate through the directory structure of a compressed archive. While it may confuse users, it does not pose any security risk.

● b. Zip path traversal is a security vulnerability that allows an attacker to extract files to arbitrary locations on a system, potentially overwriting sensitive files or executing malicious code. ✓

○ c. Zip path traversal is a technique used to compress and extract files and folders in a compressed ZIP archive. It does not pose any security risk but is solely a method for managing files.

Risposta corretta.

La risposta corretta è:
Zip path traversal is a security vulnerability that allows an attacker to extract files to arbitrary locations on a system, potentially overwriting sensitive files or executing malicious code.

1) What is Android SafetyNet attestation, and how does it enhance security?

a. Android SafetyNet attestation is a method used to bypass security measures on Android devices, allowing unauthorized access to protected data and services

b. Android SafetyNet attestation is a feature that enables users to clone and replicate their Android devices, allowing them to use multiple instances of the same device simultaneously

c. Android SafetyNet attestation is a feature that verifies the integrity and compatibility of an Android device's operating system and software, ensuring a secure environment for sensitive applications

2) Select the wrong statement

a. Verify Apps (Google Play Protect) is a system-level security feature that scans and protects against potentially harmful or malicious apps on the Google Play Store

b. SafetyNet Attestation helps protect sensitive applications by ensuring they run on trusted devices and protecting against potential attacks

c. SafetyNet Attestation and Verify Apps are both security features provided by Google for Android devices, but they serve different purposes

Safetynet runs at the physical layer while the other runs at the application layer. Safetynet checks also for hardware components if they were compromised. The other one is wrong because it runs on the device locally, so it's scanned there.

3) What is Project Treble, and how does it impact Android device updates?

a. Project Treble is a program that allows Android users to customize the appearance and layout of their device's user interface, providing a more personalized experience.

b. Project Treble is an architectural change in the Android operating system that separates the vendor implementation from the core Android framework. It simplifies the process of delivering Android updates to devices by enabling faster and more frequent updates from manufacturers.

c. Project Treble is a feature that improves battery life on Android devices by optimizing power consumption and managing background processes efficiently.

4) Which one is an example of MAC on Android?

a. App Permissions

b. File System Permissions

c. SELinux policies

5) What is the role of SELinux in Android, and how does it enhance the operating system's security?

a. SELinux in Android is a security mechanism that enforces discretionary access control policies, limiting the actions and permissions of processes and applications based on their security contexts.

b. SELinux in Android is a security mechanism that enforces mandatory access control policies, limiting the actions and permissions of processes and applications based on their security contexts.

c. SELinux in Android is a feature that scans and detects malicious apps on the device, providing real-time protection against potential security threats.

6) Which one is NOT a direct consequence of unlocking the Android bootloader?

a. compromise the device hardware components

b. exploiting a vulnerability to install malware that can compromise the device's security

c. running untrusted software that may contain security vulnerabilities

7) What is Android TrustZone, and how does it contribute to the security of the operating system?

a. Android TrustZone is a hardware-based security extension that provides a secure execution environment for handling sensitive operations and storing sensitive data.

b. Android TrustZone is a security mechanism that prevents unauthorized access to the device by encrypting all data stored on the device's internal storage.

c. Android TrustZone is a feature that enables users to securely transfer files between Android devices using encrypted communication channels.

As seen by slides, this is basically an ARM feature, depending on the architecture.

8) What is defense in depth?

a. cybersecurity strategy that involves implementing multiple layers of security controls to protect against the different threats

b. cybersecurity strategy that involves implementing multiple layers of security controls to protect against the same threat

c. a vulnerability scanning tool