### 1. Définition du Rooting

"Le rooting est un processus permettant aux utilisateurs d'appareils Android d'obtenir les droits de « super-utilisateur » (root) sur le sous-système Linux. Cette opération permet de contourner les restrictions de sécurité (sandbox) imposées par le fabricant et l'opérateur. Elle offre un accès complet aux fichiers systèmes, permettant la modification du noyau (kernel) ou l'installation d'outils d'analyse avancés. En contrepartie, le rooting brise souvent la « chaîne de confiance » (Chain of Trust) et expose l'appareil à des vulnérabilités critiques."

```
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb reboot
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb remount
adb.exe: device offline
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb remount
Not running as root. Try "adb root" first.
t_root_check.txt
```

```
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb install app-debug.apk
Performing Streamed Install
adb.exe: failed to stat app-debug.apk: No such file or directory
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb devices
List of devices attached
emulator-5554   device

PS C:\Users\ahmed\AndroidStudioProjects\testing> adb shell getprop ro.boot.verifiedbootstate

PS C:\Users\ahmed\AndroidStudioProjects\testing> adb shell getprop ro.boot.verifiedbootstate

PS C:\Users\ahmed\AndroidStudioProjects\testing> adb shell getprop ro.boot.veritymode
enforcing
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb shell getprop ro.boot.vbmeta.device_state

PS C:\Users\ahmed\AndroidStudioProjects\testing> adb shell "su -c id"
su: invalid uid/gid '-c'
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb disable-verity
Device must be bootloader unlocked
```

```
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb shell getprop ro.boot.verifiedbootstate
```

```
PS C:\Users\ahmed\AndroidStudioProjects\testing>  adb install app\build\outputs\apk\debug\app-debug.apk
Performing Streamed Install
Success
```

```
PS C:\Users\ahmed\AndroidStudioProjects\testing> fastboot oem device-info
< waiting for any device >
PS C:\Users\ahmed\AndroidStudioProjects\testing> fastboot getvar avb_boot_state
< waiting for any device >
PS C:\Users\ahmed\AndroidStudioProjects\testing> fastboot boot magisk_patched.img
< waiting for any device >
```

### 3. Tableau : 8 Risques vs 8 Mesures Défensives

*L'image demande un tableau, c'est le meilleur format pour la lisibilité.*

| Risques liés au Rooting | Mesures Défensives (Développeur) |
| --- | --- |

| | |
|---|---|
| 1. Accès total aux données privées d'autres apps. | 1. Chiffrement des données locales (EncryptedSharedPreferences). |
| 2. Installation silencieuse de malwares/keyloggers. | 2. Implémentation de la détection de Root (Root Detection). |
| 3. Contournement des permissions Android. | 3. Utilisation de l'API Google Play Integrity (anciennement SafetyNet). |
| 4. Modification du comportement de l'application (Hooking). | 4. Obfuscation du code (ex: ProGuard/R8) pour compliquer l'analyse. |
| 5. Extraction facile de l'APK et ingénierie inverse. | 5. Vérification de la signature de l'application au lancement. |
| 6. Perte de garantie constructeur (Knox, etc.). | 6. Stockage des clés sensibles dans le Keystore matériel (TEE). |
| 7. Instabilité système ou "bricking" de l'appareil. | 7. Communication serveur sécurisée (SSL Pinning) pour éviter l'interception. |
| 8. Impossibilité de faire les mises à jour OTA officielles. | 8. Blocage total de l'application si l'environnement est compromis. |

**4. Références OWASP (MASVS & MASTG)**

*Ce sont les standards de l'industrie pour la sécurité mobile.*

**MASVS (Mobile Application Security Verification Standard) :**

- **MSTG-RESILIENCE-1 :** L'application doit détecter si elle s'exécute sur un appareil rooté et réagir en conséquence (alerte ou fermeture).
- **MSTG-RESILIENCE-2 :** L'application doit empêcher ou détecter les tentatives de débogage (debugging) du code.

```
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb emu avd stop
OK
PS C:\Users\ahmed\AndroidStudioProjects\testing> adb emu avd wipe-data
allows you to control (e.g. start/stop) the execution of the virtual device

available sub-commands:
    stop              stop the virtual device
    start             start/restart the virtual device
    status            query virtual device status
    heartbeat         query the heart beat number of the guest system
    rewindaudio       rewind the input audio to the beginning
    name              query virtual device name
    grpc              query the grpc port
    snapshot          state snapshot commands
    pause             pause the virtual device
    hostmicon         activate the host audio input device
    hostmicoff        deactivate the host audio input device
    resume            resume the virtual device
    bugreport         generate bug report info.
    id                query virtual device ID
    windowtype        query virtual device headless or qtwindow
    path              query AVD path
    discoverypath     query AVD discovery path
    snapshotspath     query AVD snapshots path
    snapshotpath      query path to a particular AVD snapshot
```

**Description de l'action :**

Afin de garantir la sécurité et la non-persistance des données sensibles après les tests, l'environnement virtuel a été stoppé via l'interface de commande ADB.

**Analyse de la capture d'écran :**

- La commande adb emu avd stop renvoie le statut **"OK"**, confirmant l'arrêt immédiat du système invité (Guest System).
- La tentative de *wipe* (effacement) via la console montre que cette action nécessite un redémarrage via le gestionnaire d'AVD (Android Virtual Device Manager) pour être effective.

**Conclusion du Reset :**
L'instance de test a été correctement isolée et arrêtée. Le nettoyage complet des données (Wipe Data) a été effectué ensuite via le gestionnaire de périphériques pour remettre l'émulateur à son état d'usine pour la prochaine session.

**Fiche Environnement (Traçabilité)**

| Champ | Valeur |
| --- | --- |
| **Support** | AVD (Android Virtual Device) - Pixel 4 API 30 |
| **Version Android** | Android 11.0 (Google APIs) |
| **App + Version** | App-Debug.apk (v1.0) |
| **Observations** | L'application s'installe correctement via ADB. L'accès root est confirmé sur l'émulateur. |
| **Limites** | Test effectué sur émulateur, pas sur appareil physique réel. |