Labo 03 – Android –DAC, Permissions, Hardening, Virtualisation

1. Introduction

L'objectif de ce laboratoire se limite à une découverte pratique de la sécurité sous Android.

Rendu

Ce laboratoire doit être réalisé par groupe sauf dérogation exceptionnelle de l'équipe enseignante.

Le rendu consiste en une présentation de **20'** avec au moins **5' de démo**. La présentation sera suivie de 5' de questions. La langue pour la présentation est à choix le français ou l'anglais.

Aucun rapport n'est exigé. Seuls, les slides doivent être déposés dans le rendu au format **PDF** sur cyberlearn : https://cyberlearn.hes-so.ch/mod/assign/view.php?id=1349024. Les délais de rendu y sont indiqués. Chaque jour de retard pourra réduire la note d'un point.

Infrastructure

Vous pouvez utiliser n'importe quel poste sous Android. Alternativement, vous pouvez utiliser un émulateur qui peut vous faciliter l'atteinte des objectifs de votre démonstration en vous permettant notamment de devenir `root` sur l'appareil émulé. Pour vous guider, vous pouvez consulter le « readme » réalisé par des étudiants des années précédentes : https://cyberlearn.hes-so.ch/mod/resource/view.php?id=858579.

2. Réalisation

Vous allez démontrer l'utilisation et/ou l'effet des autorisations DAC Linux et/ou des permissions Android pour interdire/autoriser les accès à une application à l'aide de l'outil `adb`.

Autorisations DAC : Visualisez leur utilisation pour isoler les applications. Par exemple, vous pouvez :

- Trouver les UID des utilisateurs de votre appareil, visualiser comment ils sont initialisés.
- Récupérer ou créer une (ou des) application(s) utilisateur sur votre appareil et mettre en évidence son (leur) utilisation du DAC pour voir détailler les mécanismes d'isolation.

Permissions d'application : Visualisez les mécanismes d'assignation et de vérification avec leurs effets sur les applications (utilisateur ou système). Par exemple, vous pouvez :

- Lister les permissions possibles, exigées, acceptées.
- Récupérer ou créer une (ou des) application(s) et manipuler leurs permissions pour autoriser ou interdire l'accès à une ressource ou la communication avec une autre application.

Hardening ou virtualisation : Visualisez l'application de mécanisme(s) de sécurité avancé(s) vu(s) en cours sur la partie Linux.

Il est fortement recommandé de s'inspirer d'un tutoriel ou de la littérature existante sur le sujet, sans oublier de le(s) référencer. Quelques exemples (il y en a plein d'autres) :

- https://valsamaras.medium.com/the-application-sandbox-9abd09a5c6da
- https://stackoverflow.com/questions/21091022/listing-permissions-of-android-application-via-adb
- https://www.hexnode.com/mobile-device-management/help/grant-permissions-for-hexnode-apps-using-android-debug-bridge-adb/