PLOUZENNEC Eliaz

# TP KALI LINUX : Failles de sécurité sous Système d'exploitation ANDROID

13/12/2023

# Sommaire



# Introduction :

L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion. Ici nous allons utiliser kali linux pour exploiter les failles du système d'exploitation android.

# Description du système d'exploitation ANDROID :

Android est un OS mobile basée sur Linux, développée par Google, et distribuée sous licence open source Apache v2. Ce système d'exploitation a été développé par Google et Open Handset Alliance (OHA), une coalition d'opérateurs de télécommunication, d'équipementiers et d'intégrateurs système.

L'ensemble est organisé en cinq couches distinctes :

- le noyau Linux avec les pilotes ;
- des bibliothèques logicielles telles que WebKit/Blink, OpenGL ES, SQLite ou FreeType ;
- un environnement d'exécution et des bibliothèques permettant d'exécuter des programmes prévus pour la plate-forme Java ;
- un framework — kit de développement d'applications ;
- un lot d'applications standard qui comprend un environnement de bureau, un carnet d'adresses, un navigateur web et une application téléphone.

# Liste et description des plus importantes failles ANDROID :

1. Stagefright (2015) :Cette faille a permis l'exécution de code malveillant via des fichiers médias MMS. Les utilisateurs pouvaient être infectés simplement en ouvrant un message texte.

2. QuadRooter (2016) :Cette vulnérabilité affectait les processeurs Qualcomm, permettant à des applications malveillantes d'obtenir des privilèges élevés sur l'appareil, compromettant ainsi la sécurité.

3. BlueBorne (2017) :Utilisant des vulnérabilités dans la connectivité Bluetooth, cette faille permettait à des attaquants de prendre le contrôle d'un appareil Android sans interaction de l'utilisateur.

4. Spectre et Meltdown (2018) :Bien que principalement liées aux processeurs, ces vulnérabilités affectaient également certains appareils Android, permettant la fuite de données sensibles.

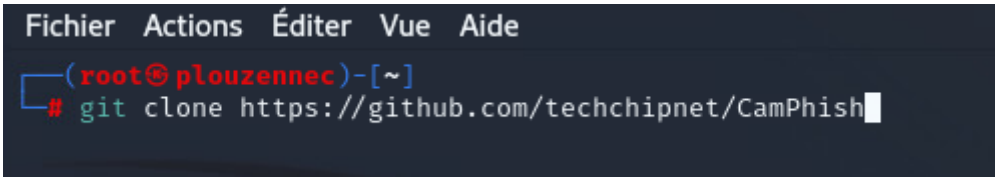
5. StrandHogg (2019) :Cette faille a été exploitée pour créer des applications malveillantes qui pouvaient imiter d'autres applications légitimes, incitant les utilisateurs à divulguer des informations sensibles.

## Installation de l'outil :

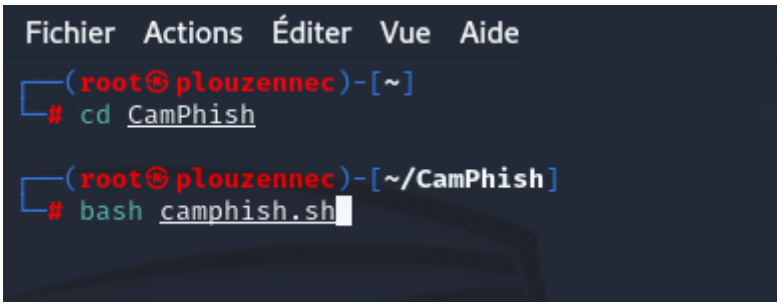
### Utilité :

CamPhish est une technique permettant de prendre des photos de la caméra frontale du téléphone ou de la webcam du PC de la cible. CamPhish héberge un faux site Web sur un serveur PHP intégré et utilise ngrok & serveo pour générer un lien que nous transmettrons à la cible, qui peut être utilisé sur Internet. le site Web demande l'autorisation de la caméra et si la cible le permet, cet outil récupère des photos de l'appareil de la cible.

Il faut commencer par un sudo apt update puis un sudo apt upgrade pour le bon fonctionnement de l'installation. Il faut prélablement que openssh soit installé, ici c'est déjà le cas.

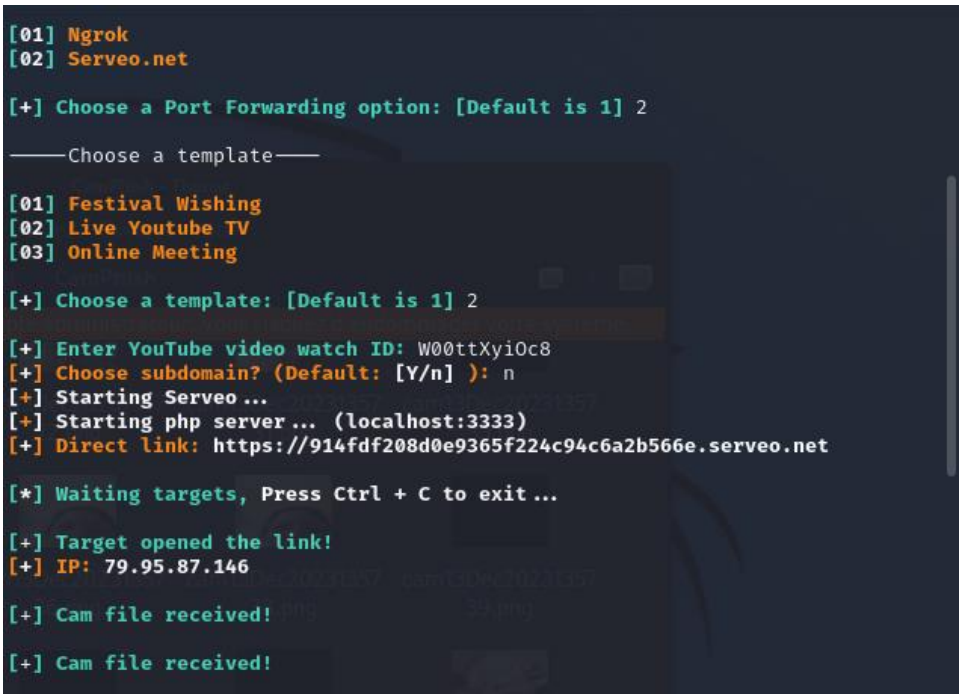



On installe camphish via le lien github



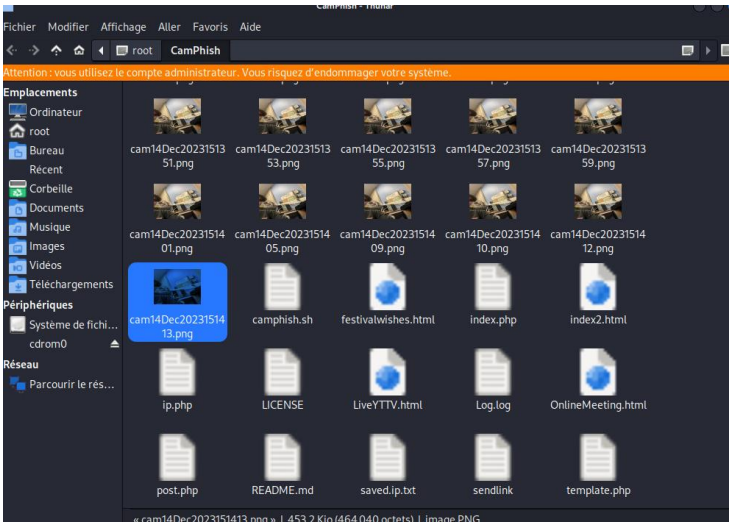

Pour ensuite rentrer dans le fichier et lancer le logiciel.

## Exploitation de l'outil et test de fonctionnement :




On entre dans le logiciel, pour ensuite choisir les caracteristiques que l'on souhaite pour le phishing. Ici 2 pour Serveo.net, 2 pour Youtube, et l'id de la video, ici W00ttXyi0c3.

Lorsqu'on ouvre le lien donné, le logiciel capte l'adresse ip de la victime, et capture des photos de la caméra avant.




Maintenant il faut rentrer dans le dossier camphish et toutes les photos prises sont là.