IMT Mines Alès
École Mines-Télécom

Institut Mines-Télécom

IMT Mines Alès - Site Clavières

Département Systèmes et Réseaux (SR)

Ethical Hacking - TryHackMe Metasploit

Nathan Martel

Groupe : SR
IMT Mines Alès

24 novembre 2024

TLP :RED

Table des matières

1 Introduction :

Le challenge Metasploit de TryHackMe permet d'avoir un aperçu approfondi dans l'utilisation de Metasploit Framework, un outil polyvalent et puissant pour l'exploitation de vulnérabilités et les tests de pénétration.

URL du challenge : https://tryhackme.com/r/room/metasploitintro

@uthor : Nathan Martel.

Le document est classifié sous la marque **TLP :RED** (Traffic Light Protocol), ce qui signifie que le partage du document doit se limiter uniquement aux destinataires individuels, et qu'aucune autre divulgation n'est autorisée sauf avis favorable du propriétaire.

Ce document est privé et est uniquement déposé dans le répertoire Git de l'auteur. Merci de ne pas le diffuser, l'utiliser ou le modifier sans autorisation.

2 Metasploit :

2.1 Task 1 : Introduction to Metasploit :

Aucune réponse n'est demandée pour cette partie.

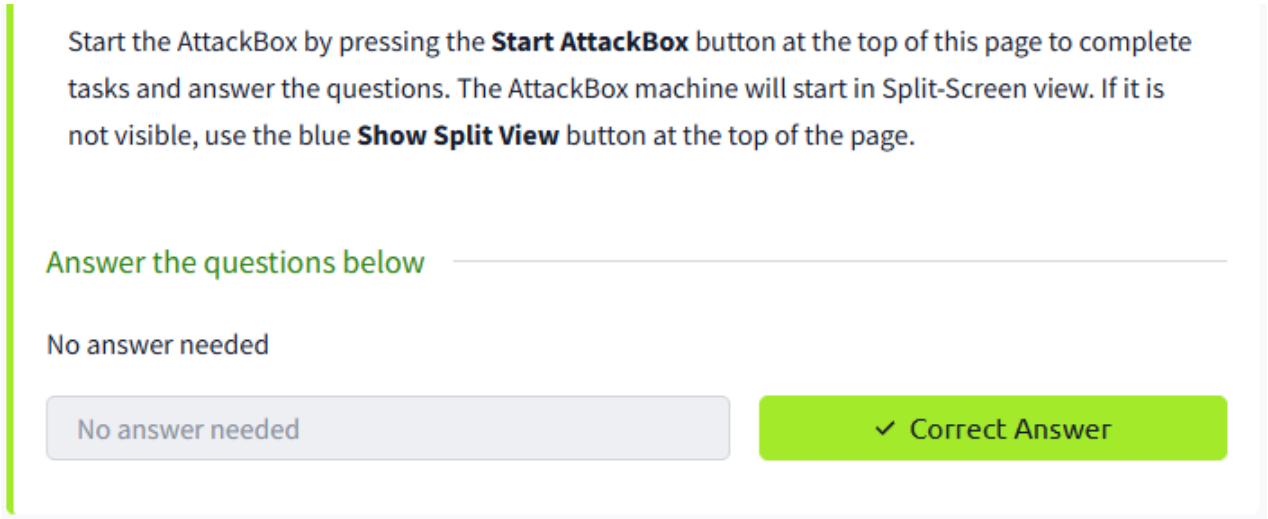

FIGURE 2.1 – Capture Task1

2.2 Task 2 : Main Components of Metasploit :

What is the name of the code taking advantage of a flaw on the target system ?

$\Longrightarrow$ La réponse est **Exploit**.

Un exploit est un bout de code ou un programme pour tirer parti d'une vulnérabilité ou d'une faiblesse dans un système/application/réseau/... Il existe selon Bitdefender et CrowdStrike trois types d'exploits :

- Exploits locaux : nécessite un accès préalable au système pour exploiter une faille ;
- Exploits distants : exploiter une faille à distance sans nécessiter d'accès préalable ;
- Zero-day exploits : vulnérabilités inconnues exploitées, donc dangereux.

What is the name of the code that runs on the target system to achieve the attacker's goal ?

$\Longrightarrow$ La réponse est **Payload**.

Le payload est la partie de l'exploit qui permet d'atteindre son objectif une fois que la vuln a été exploitée. C'est en fait, l'action finale effectuée sur le système. Par exemple, un reverseshell, extraire des infos importantes, etc.

Remarque : Il existe, à l'instar des exploits, trois types de payload : payload passif (e.g. keylogger, sniffers, ...), payload actif (e.g. exécution commande/code à distance, cheval de troie, ...) et payload connectif (e.g. bind shell, reverseshell, ...). [A creuser].

Lire pour la culture : https://www.offsec.com/metasploit-unleashed/payload-types/

What are self-contained payloads called ?

$\Longrightarrow$ La réponse est **Singles**.

Un single ne nécessite pas une connexion ou de dépendance extérieure, il est minimaliste et est autonome : il n'a pas besoin de dépendre de ressources

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload ?

$\Longrightarrow$ La réponse est **Singles**.

Les payloads Singles sont identifiés par un underscore (« _ ») dans leur nom, comme "pingback_reverse_tcp". Les payloads Staged, en revanche, sont nommés avec une barre oblique ("/"). Par exemple, dans "windows/x64/shell/reverse_tcp"

2.3 Task 3 : Msfconsole :

How would you search for a module related to Apache ?

$\Longrightarrow$ La réponse est **search apache**.

En tapant simplement « search apache », Metasploit affiche une liste de tous les modules (exploits, auxiliaires, payloads, etc.) contenant le mot-clé "apache" dans leur description, leur chemin ou leur nom. En fait, Metasploit fait une recherche dans sa base de données pour récupérer tous les modules correspondant au mot clé « apache ».

Who provided the auxiliary/scanner/ssh/ssh_login module ?

$\Longrightarrow$ La réponse est **todb**

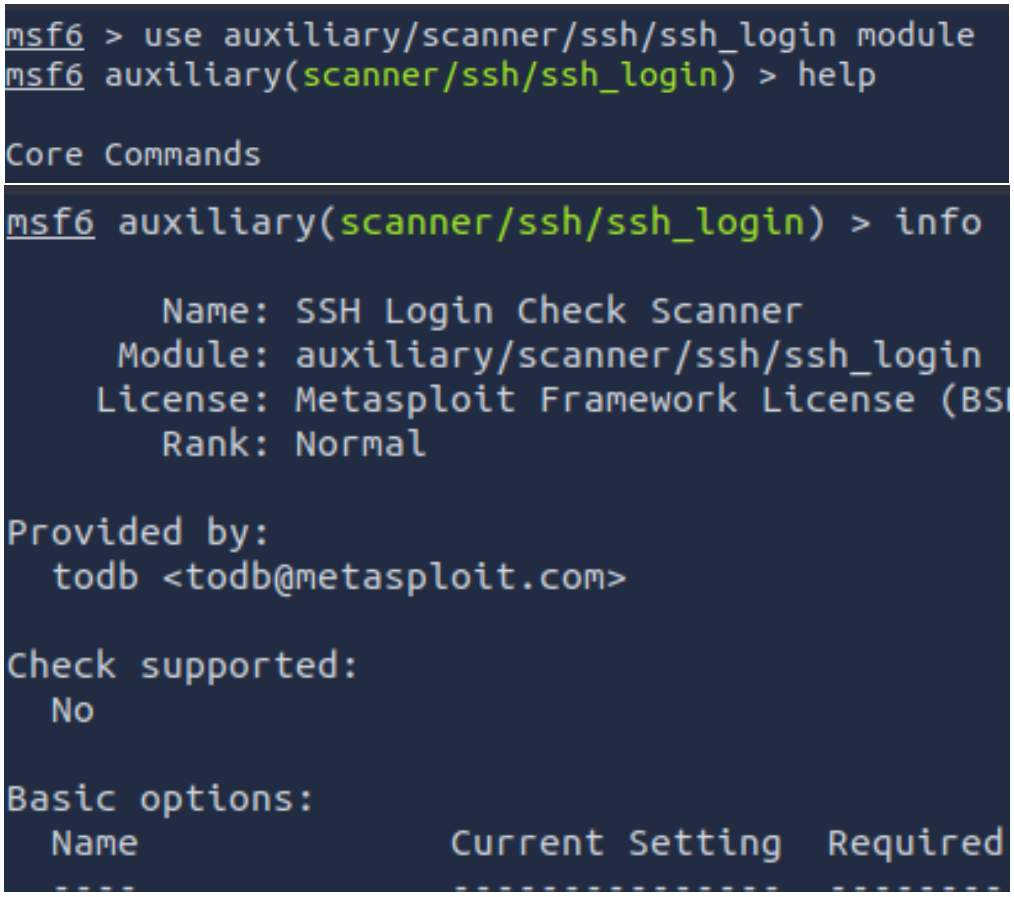

FIGURE 2.2 – Informations sur le module auxiliary/scanner/ssh/ssh_login

Après avoir fait un « use » de n'importe qu'elle module on peut saisir la commande « info » pour afficher les informations sur le module, comme sa description, ses options, son fonctionnement, etc.

2.4 Task 4 : Working with modules :

How would you set the LPORT value to 6666 ?

$\Longrightarrow$ La réponse est textbfset LPORT 6666.

Le LPORT (= local port) est une option dans Metasploit pour spécifier le port local sur lequel l'attaquant attend les connexions entrantes/sortantes lors de l'exploitation. Par exemple, dans un reverseshell, la cible (machine compromise) initie une connexion vers l'attaquant. Le LPORT est, dans l'exemple, le port sur lequel l'attaquant écoute pour recevoir cette connexion.

How would you set the global value for RHOSTS to 10.10.19.23 ?

$\Longrightarrow$ La réponse est **set RHOSTS 10.10.19.23**.

Le RHOSTS (= remote hosts) indique à Metasploit sur quel(s) système(s) l'exploit ou le module doit être exécuté. On spécifie l'adresse IP ou la plage d'adresses IP des cibles que l'attaquant souhaite analyser ou attaquer.

Remarque : La bonne réponse ici est « setg RHOSTS 10.10.19.23. On rajoute un « g » a la commande « set » pour spécifier que c'est une valeur globale, c'est-à-dire une valeur qu'on applique à tous les modules utilisés dans la « session msfconsole » en cours.

What command would you use to clear a set payload ?

$\Longrightarrow$ La réponse est **unset payload**.

L'option « unset payload » réinitialise l'option de payload et permet de définir un autre payload ou même de laisser le module sans payload.

What command do you use to proceed with the exploitation phase ?

$\Longrightarrow$ La réponse est **exploit**.

Pour passer à la phase d'exploitation dans Metasploit, on utilise la commande exploit. Cela lance l'attaque en exécutant le module configuré avec les options définies (comme RHOSTS, LPORT, payload, etc.). C'est la phase où Metasploit tente d'exploiter la vulnérabilité de la cible et d'exécuter le payload configuré (s'il y en a un).

Remarque : Il y a un alias de la commande exploit : run. Les deux commandes peuvent être utilisées de manière interchangeable dans Metasploit.

2.5 Task 5 : Summary :

Aucune réponse n'est demandée pour cette partie.

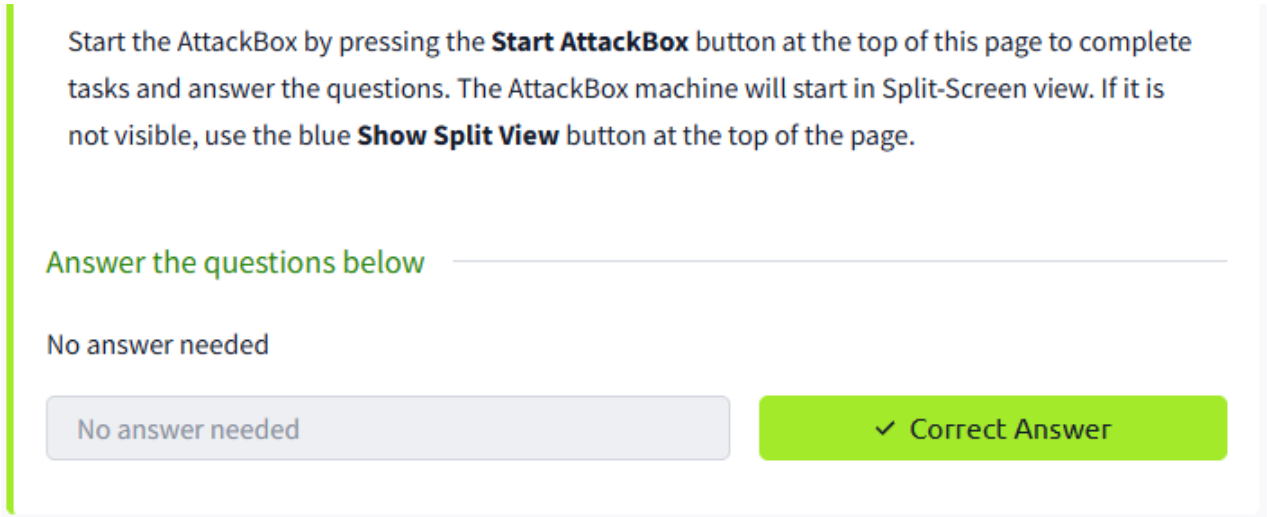

FIGURE 2.3 – Capture Task5

3 Conclusion :

Ce challenge TryHackMe a permis d'avoir des notions autour de l'outil Metasploit. J'ai pu découvrir/revoir les principaux composants de cette plateforme, tels que les exploits, qui tirent parti des vulnérabilités pour compromettre un système, et les payloads, qui exécutent des actions spécifiques après exploitation. C'est avoir l'interface msfconsole qu'on peut exécuter des modules en configurant des paramètres (RHOSTS, LPORTS, RPORT, SMBPIPE, etc.)

Fin du rapport.

Rapport écrit par Nathan Martel le 22/11/2024 et le 24/11/2024.
Version : v1.0

Outils utilisés : VM TryHackMe et VM Kali Linux

Logiciel utilisé : Texworks
Langage et systèmes de composition : LaTeX
Console : MiKTeX
Format du document : PDF

Table des figures