Fiche pratique : P2.3 : Exploitation

mardi 18 février 2025 12:02

TP 3 : Exploitation/Post Exploitation

- Recherche d'exploits : Utiliser Metasploit pour rechercher des vulnérabilités spécifiques dans la base de données d'exploits.
- Configuration et lancement d'un exploit : Guide étape par étape pour configurer un exploit et l'utiliser pour tester la sécurité d'un système cible.
- Interprétation des résultats : Analyse des résultats de l'exploit pour évaluer l'impact potentiel de la vulnérabilité.

Focus sur architecture web Apache/MySQL :

a. Reconnaissance (Facultative avec Metasploit)
   i. Metasploit n'est pas le plus approprié pour cette phase. Plutôt se servir des outils du TP 1 et TP 2.
b. Scanning et Analyse de Vulnérabilités
   i. Pour chercher le module : search "nom"
   ii. Pour activer use "nom"
   iii. Modules auxiliaires conçus pour scanner des vulnérabilités spécifiques :
      1) **http_version :** Utiliser ce module pour identifier la version du serveur web Apache et rechercher des vulnérabilités connues associées à cette version.
         1) SET RHOSTS pc-hp
         2) Run
         3) Résultats : Apache : 2.4.41 ; PHP : 7.4.33
      2) **mysql_version :** Détecter la version du serveur MySQL pour identifier les vulnérabilités potentielles.
         1) SET RHOSTS pc-hp
         2) Run
         3) Résultats : MySql 8.0.17
c. Exploitation
   i. Fournit des exploits prêts à l'emploi pour une grande variété de vulnérabilités.
      1) **Exploits Apache :** Rechercher dans la base de données de Metasploit les exploits ciblant des vulnérabilités spécifiques dans le serveur web Apache. Cela peut inclure des dépassements de tampon, des injections de commandes, ou des vulnérabilités de script cross-site.
         1)
      2) **Exploits MySQL :** Utiliser des exploits pour MySQL pour obtenir un accès non autorisé à la base de données. Cela peut inclure l'exploitation de vulnérabilités d'injection SQL ou d'autres failles de sécurité dans MySQL.
         1)
d. Post-Exploitation
   i. Offre une variété de payloads et de modules de post-exploitation pour extraire des données, élever les privilèges, ou maintenir l'accès.
      1) **Meterpreter :** Un payload avancé qui fournit un contrôle interactif sur le système cible. Il peut être utilisé pour explorer le système, accéder à la base de données MySQL, extraire des fichiers de configuration Apache, ou installer des backdoors.
      2) **mysql_sql :** Ce module de post-exploitation permet d'exécuter des commandes SQL sur une base de données MySQL compromise, facilitant l'extraction de données sensibles.
e. Rapport
   i. Permet d'exporter les résultats des exploits et des sessions de post-exploitation, qui peuvent ensuite être intégrés dans des rapports de pentest.
      1) **db_export :** Exporter les données recueillies pendant le pentest depuis la base de données de Metasploit vers des formats de fichier utilisables dans des rapports de pentest.