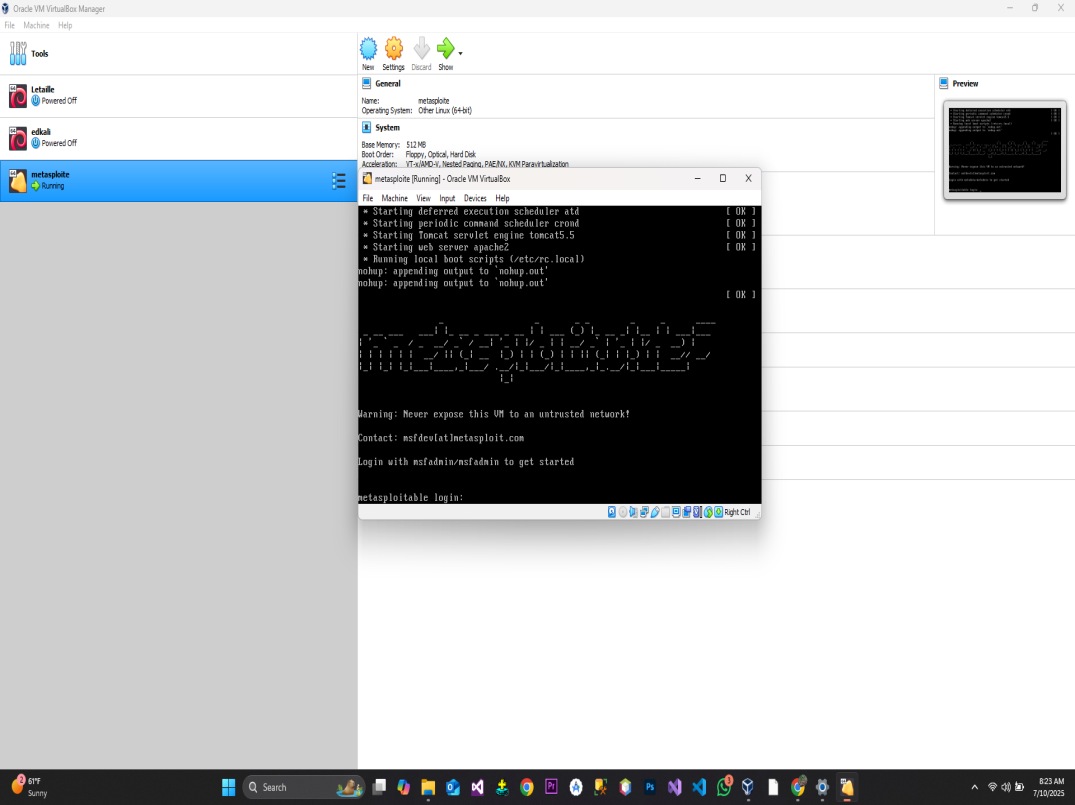
**Introduction**

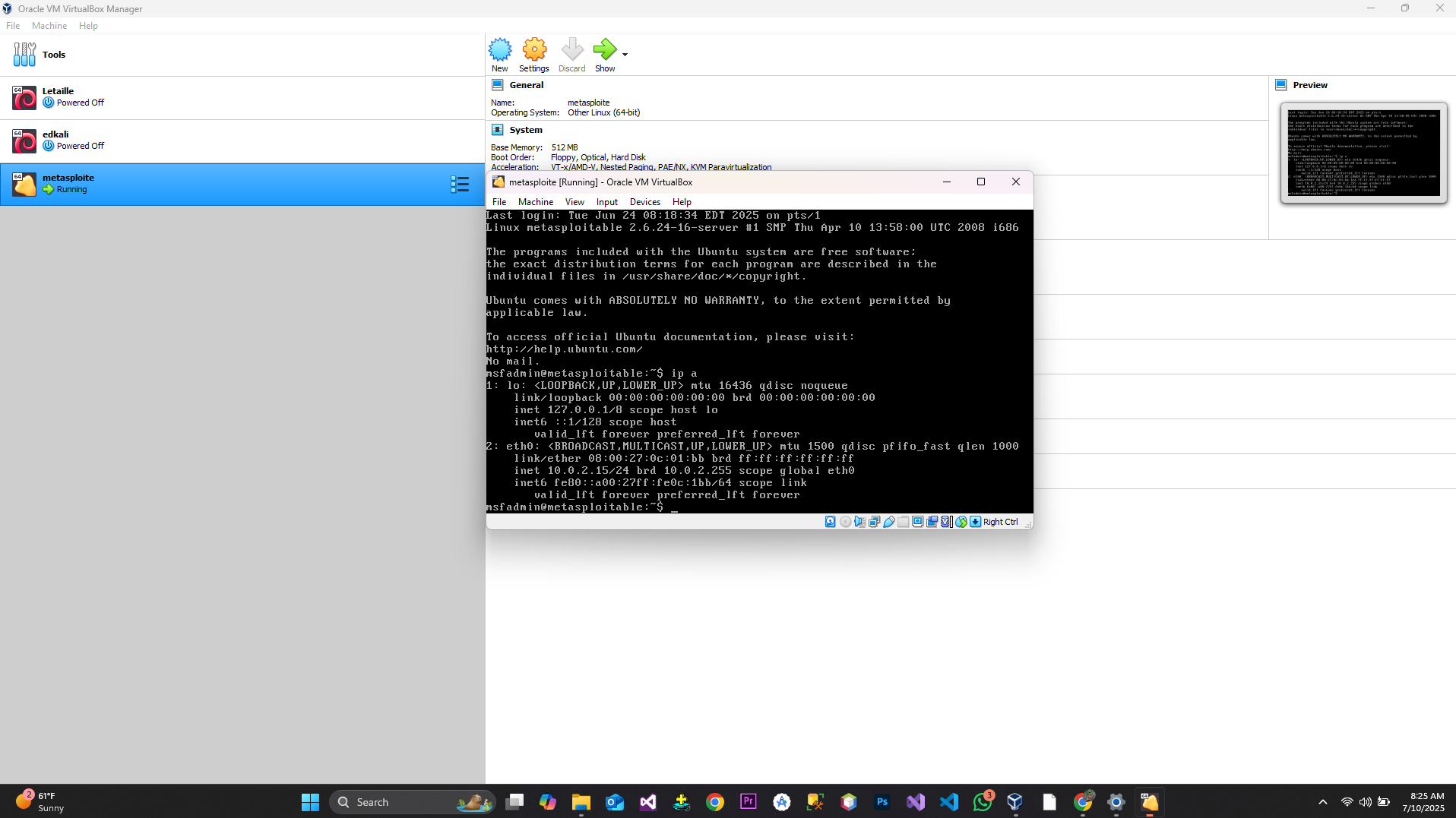
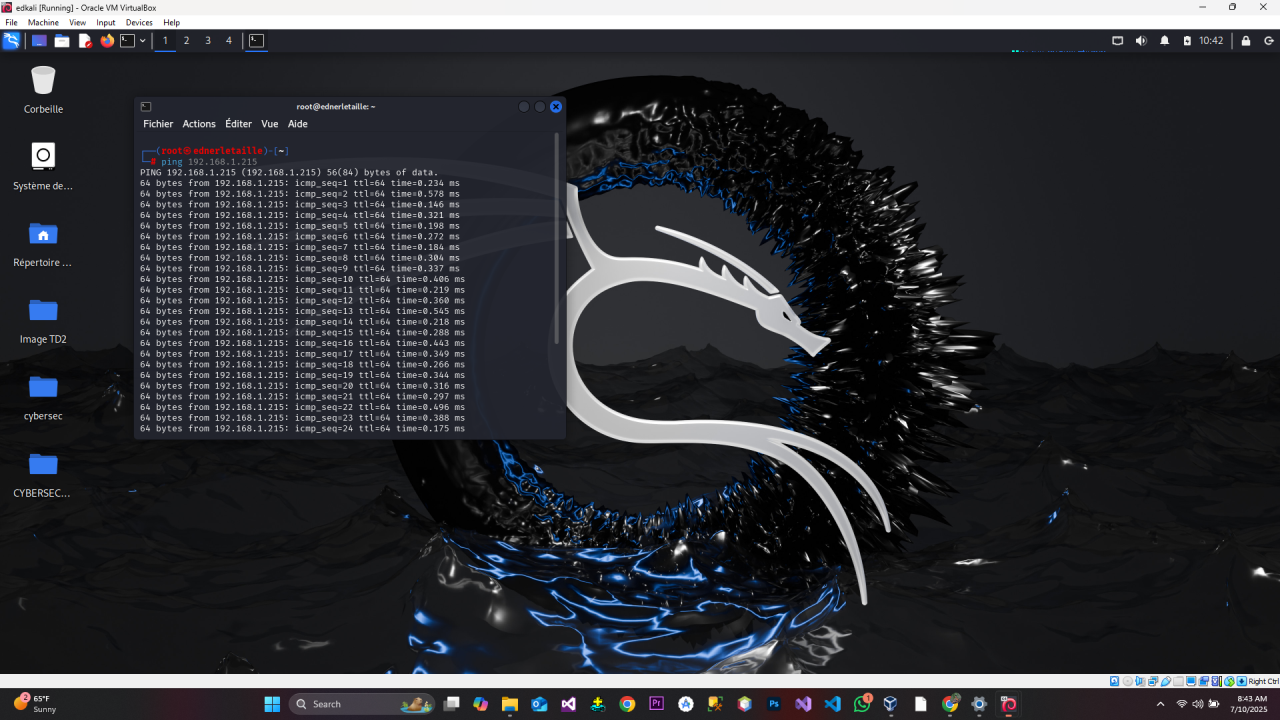
Dans le domaine de la cybersécurité, il est essentiel de comprendre les techniques utilisées par les attaquants afin de mieux sécuriser les systèmes informatiques. Ce travail dirigé (TD) s’inscrit dans cette démarche en proposant une mise en situation pratique d’un test d’intrusion à l’aide de l’outil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

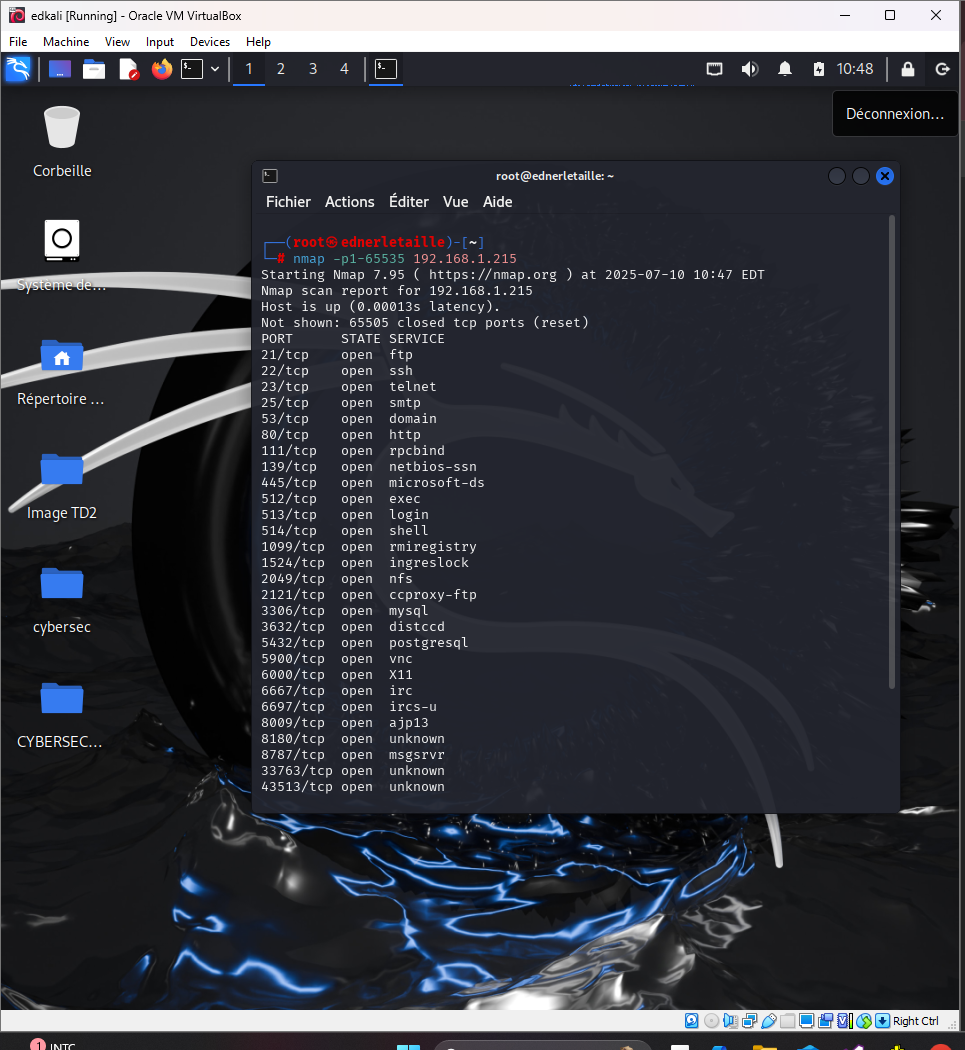


*Je crée la machine virtuelle metasploite puis je la lance*

­­­

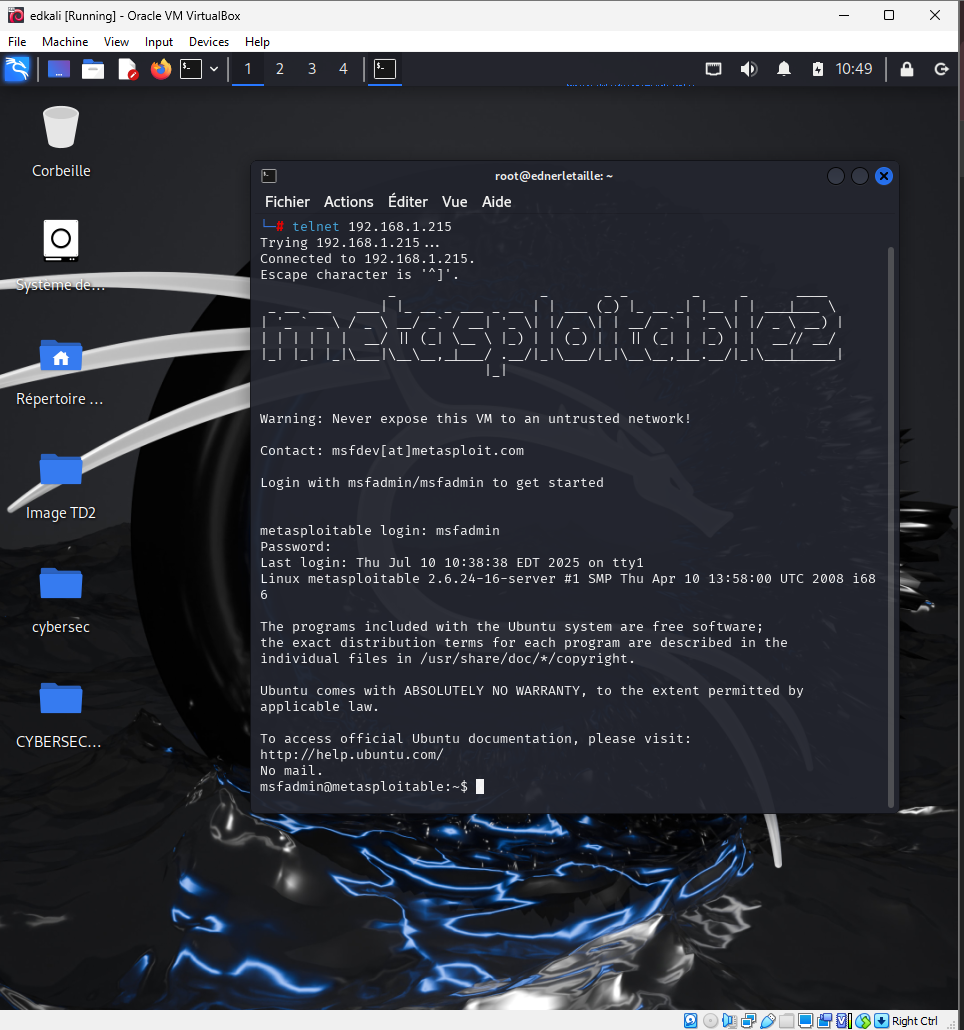
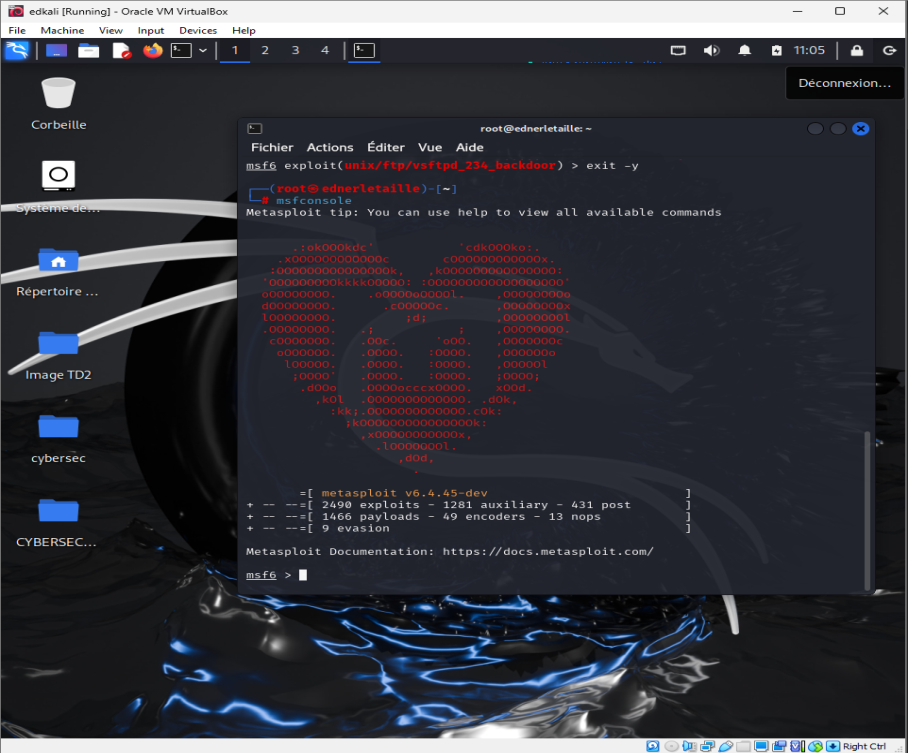
*On fait la commande ping pour pingé l’adresse ip de la machine virtuelle.*

*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.*



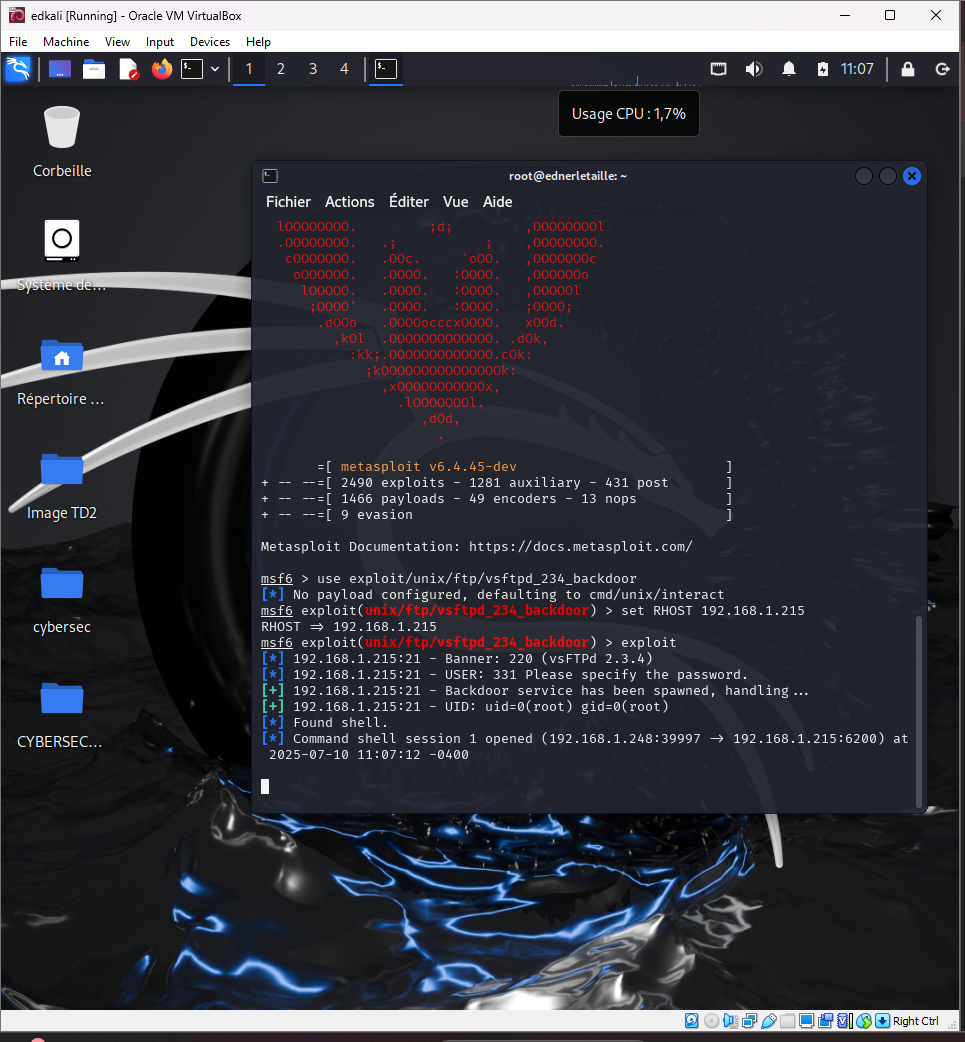
*On fait la commande nmap -p1-65535 192.168.1.215 Pour analyser tous les ports TCP (1 à 65535).*

*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****.*

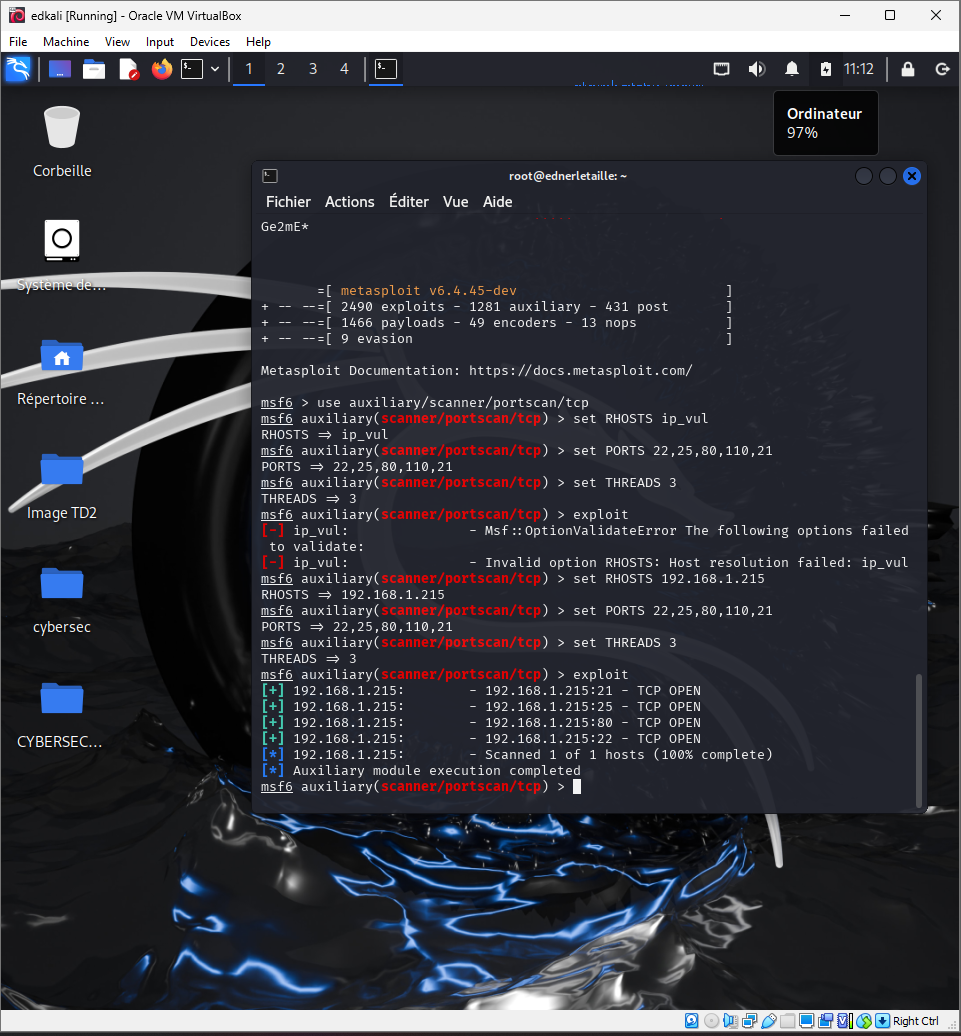


***Nous avons exécuté la commande msfconsole pour tenter d’établir une connexion avec la machine cible.*** *Cette commande permet de lancer l’interface en ligne de commande du framework Metasploit dans Kali Linux*

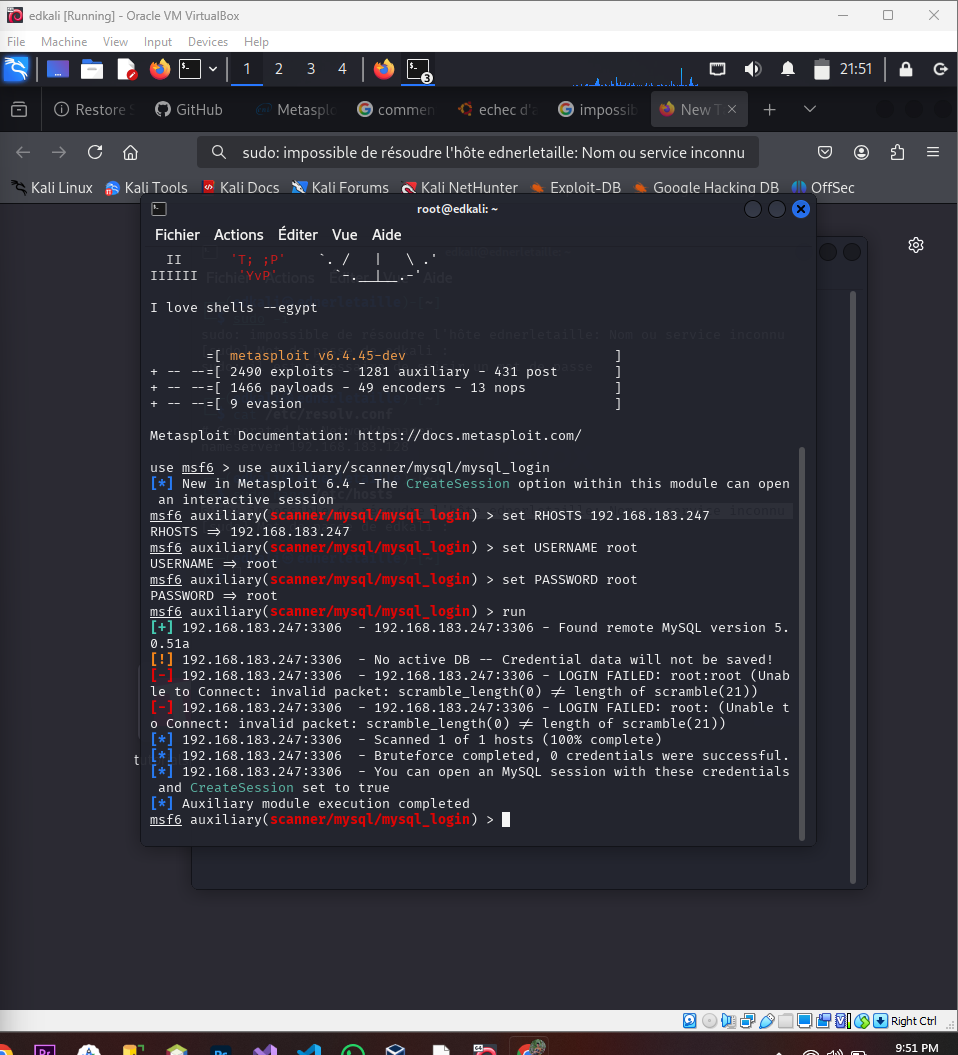
***Nous avons exécuté la commande telnet 192.168.1.215 pour tenter d’établir une connexion avec la machine cible.*** *Cette commande permet de vérifier si le service Telnet est actif sur l’hôte distant.*



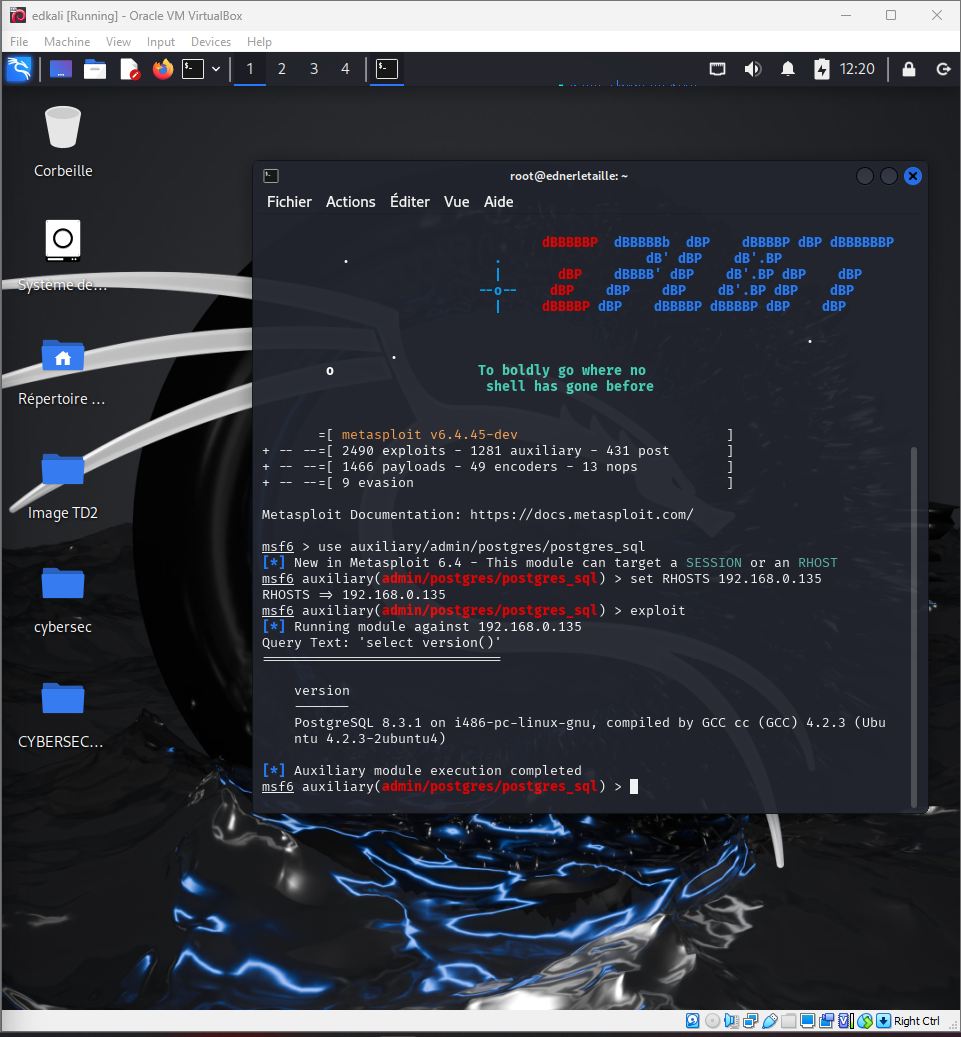
***Nous avons exécuté la commande msfconsole pour tenter d’établir une connexion avec la machine cible.*** *Nous avons ensuite utilisé le module exploit/unix/ftp/vsftpd\_234\_backdoor pour exploiter une faille dans le service FTP.  
La commande set RHOST 192.168.1.215 a permis de définir la cible, puis exploit a lancé l’attaque*



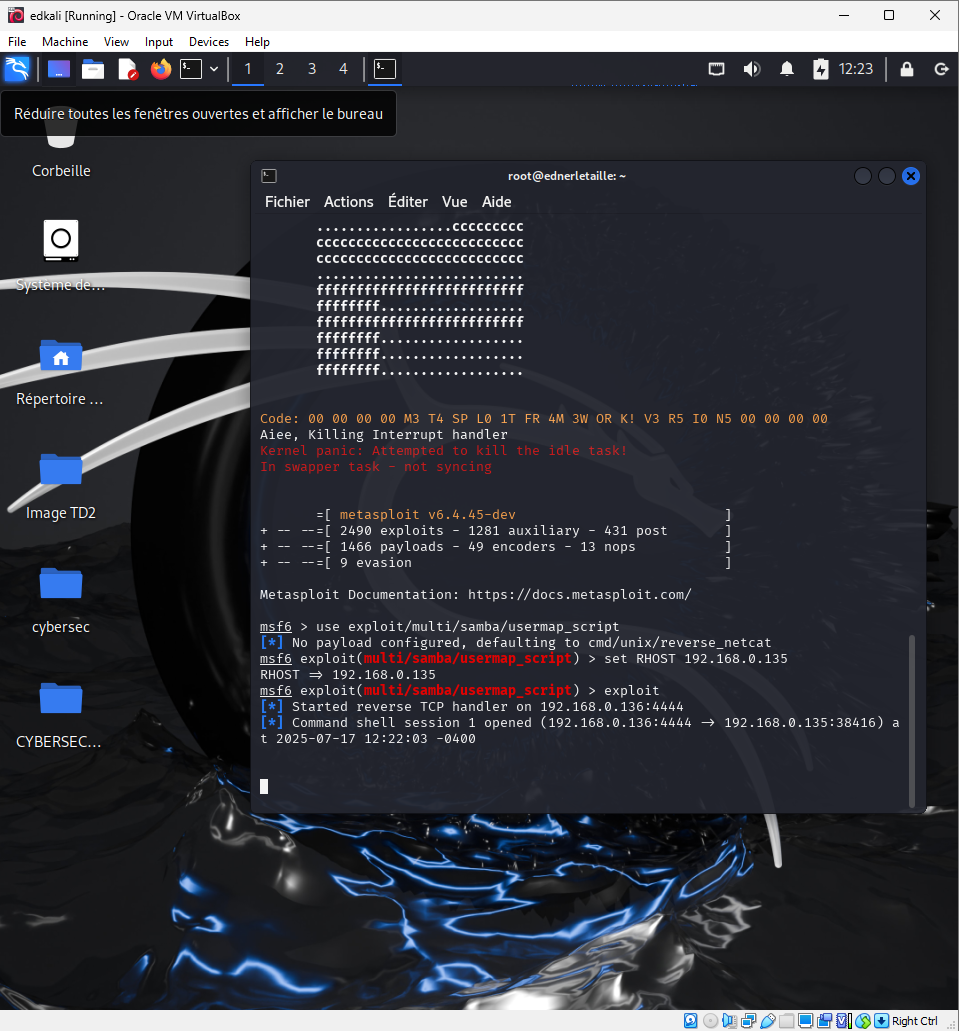
***Nous avons exécuté la commande msfconsole pour tenter d’établir une connexion avec la machine cible.*** *Après avoir quitté une session précédente avec exit -y, nous avons chargé le module auxiliary/scanner/portscan/tcp pour scanner les ports 22, 25, 80, 110 et 21.  
Nous avons défini l’hôte cible avec set RHOSTS, précisé les ports avec set PORTS, le nombre de threads avec set THREADS 3, puis lancé le scan avec exploit.*



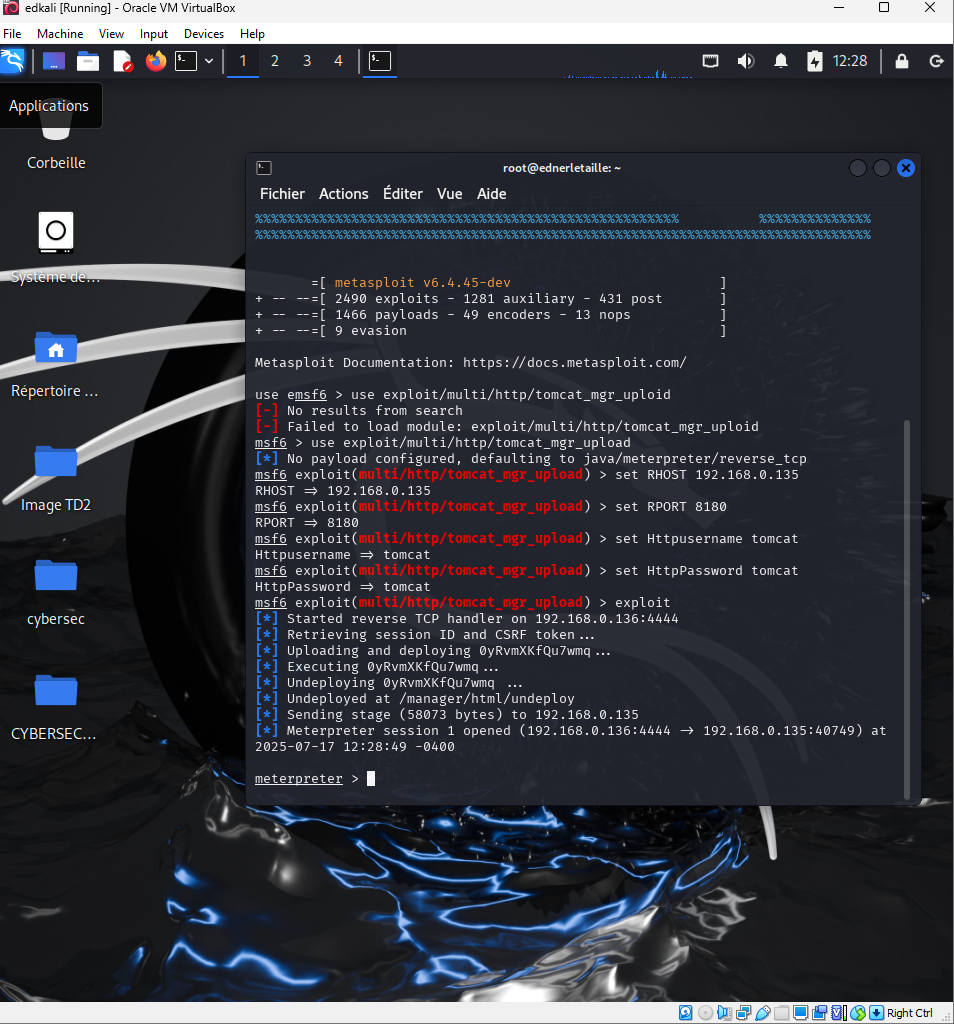
***Nous avons exécuté la commande msfconsole pour tenter d’établir une connexion avec la machine cible.*** *Nous avons utilisé le module auxiliary/scanner/mysql/mysql\_login pour tester des identifiants MySQL.  
Après avoir défini l’IP cible (set RHOSTS), le nom d’utilisateur (set USERNAME root) et le mot de passe (set PASSWORD root), nous avons lancé l’attaque avec run.*



***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.*



***Nous avons exécuté la commande msfconsole pour tenter d’établir une connexion avec la machine cible.*** *Nous avons utilisé le module exploit/multi/samba/usermap\_script pour exploiter une vulnérabilité Samba.  
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.*

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).