

**UNIVERSITE DE TECHNOLOGIE D’HAITI**

**(UNITECH)**

**FACULTE DES SCIENCES INFORMATIQUES**

**TRAVAUX DIRIGES EXPLOITATION DE VULNERABILITES SUR METASPLOITABLE 2**

**MATIЀRE CYBERSECURITE**

**ETUDIANTE CADET ESTHER**

**NIVEAU II (3EME ANNEE)**

**DEPARTEMENT INFORMATIQUES**

**ENCADREUR SAINT AMOUR ISMAEL**

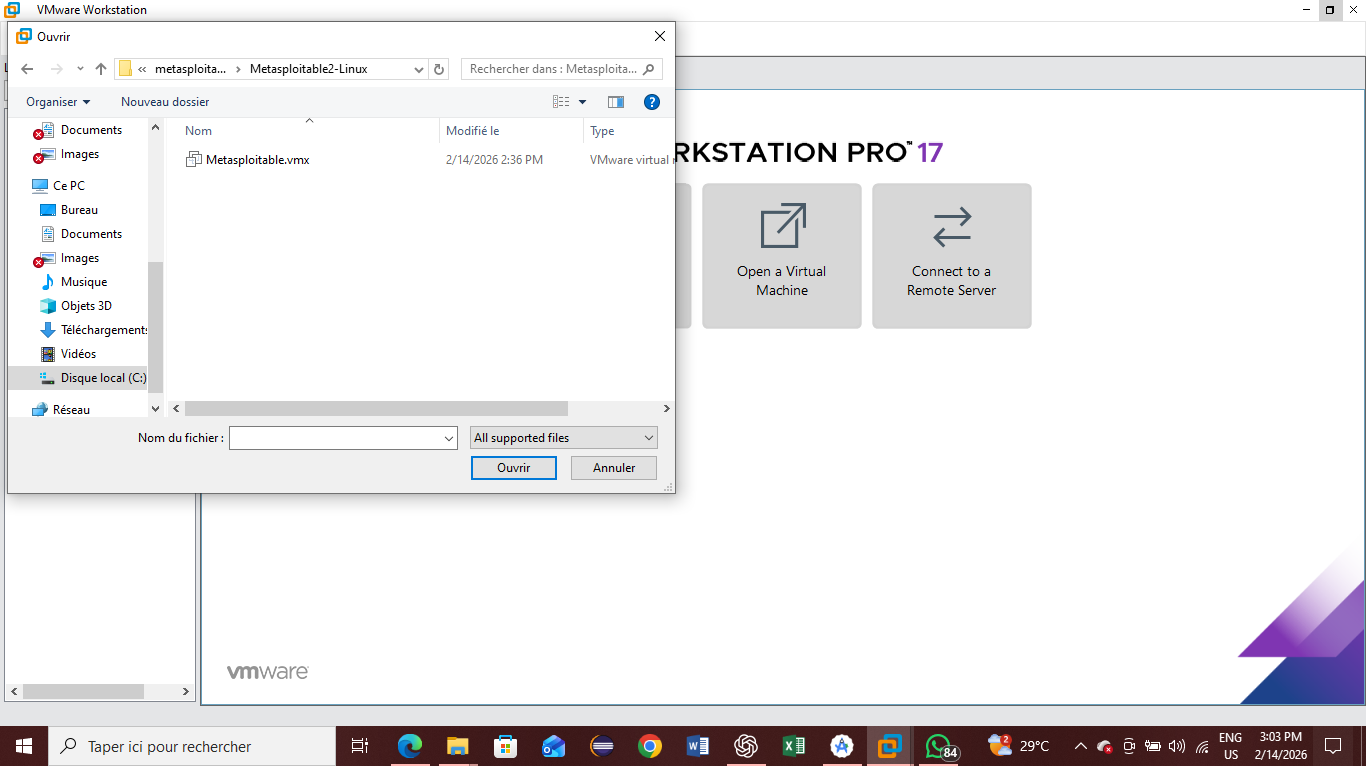
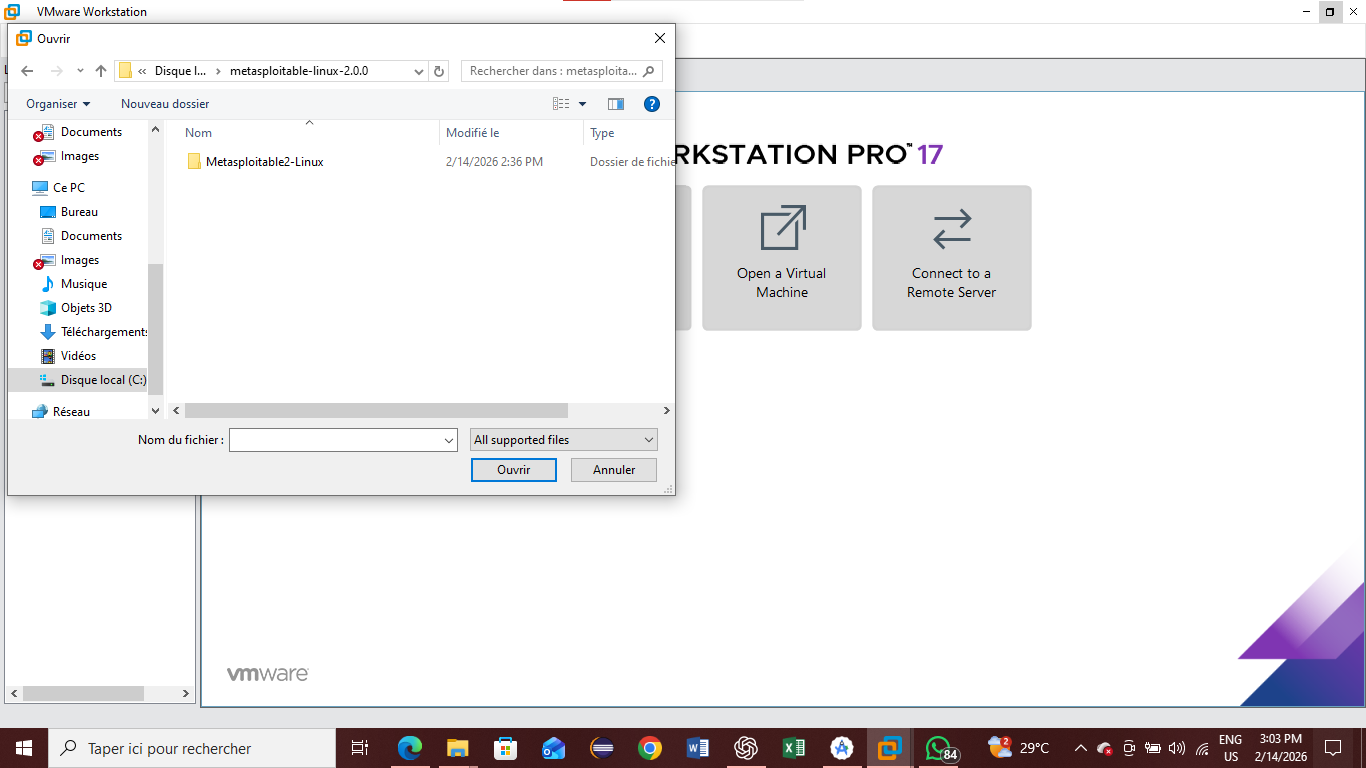
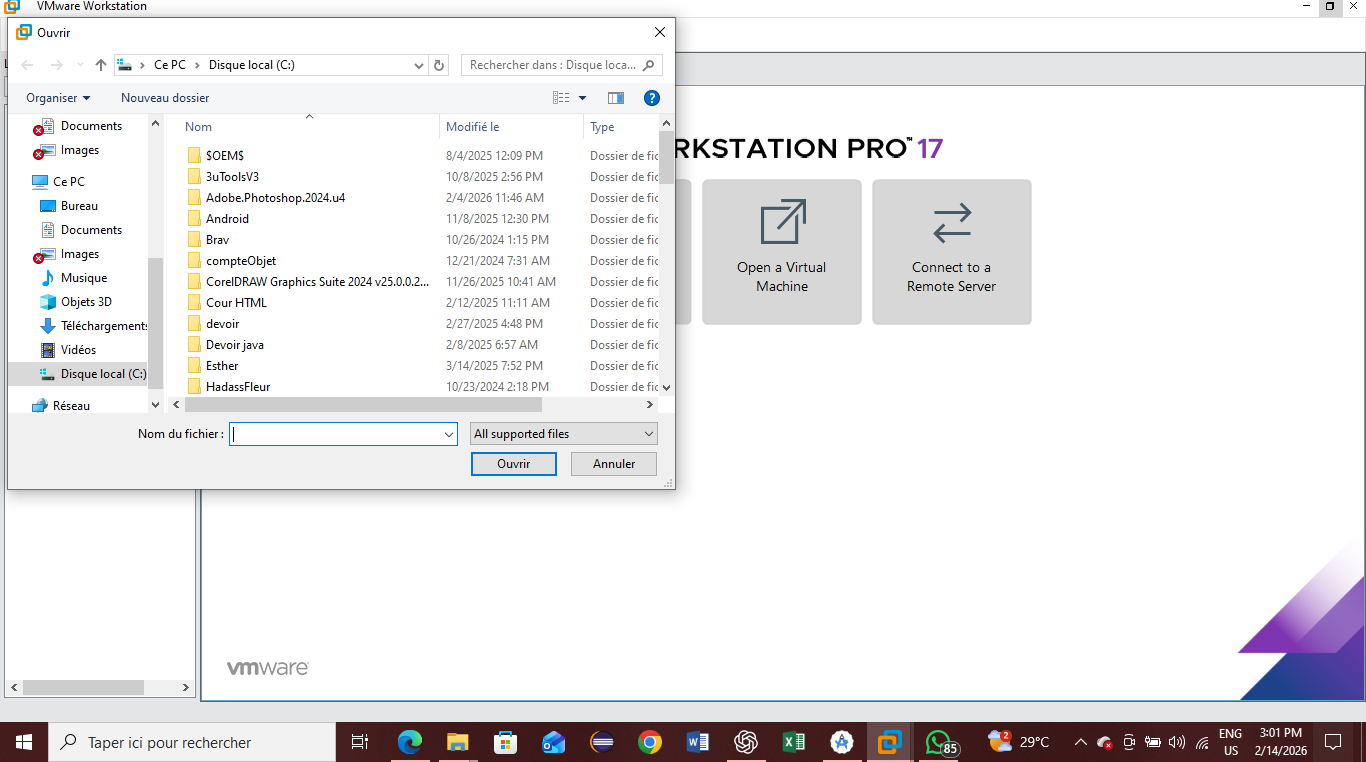
**DATE LE/23/2/26**

**Intro** L’objectif de ce TD est de se familiariser avec les outils et méthodes utilises en sécurité offensive. A l’aide d’une machine vulnérable Mestasploitable 2 et d’une plateforme d’attaque Kali Linux, nous allons réaliser un audit de sécurité : découverte des services réseau, identification de vulnérabilité connues et exploitation de celles-ci via le framework Metasploit. Ce rapport détaille les étapes réalisées, les résultats obtenus et les conclusions qui en découlent.

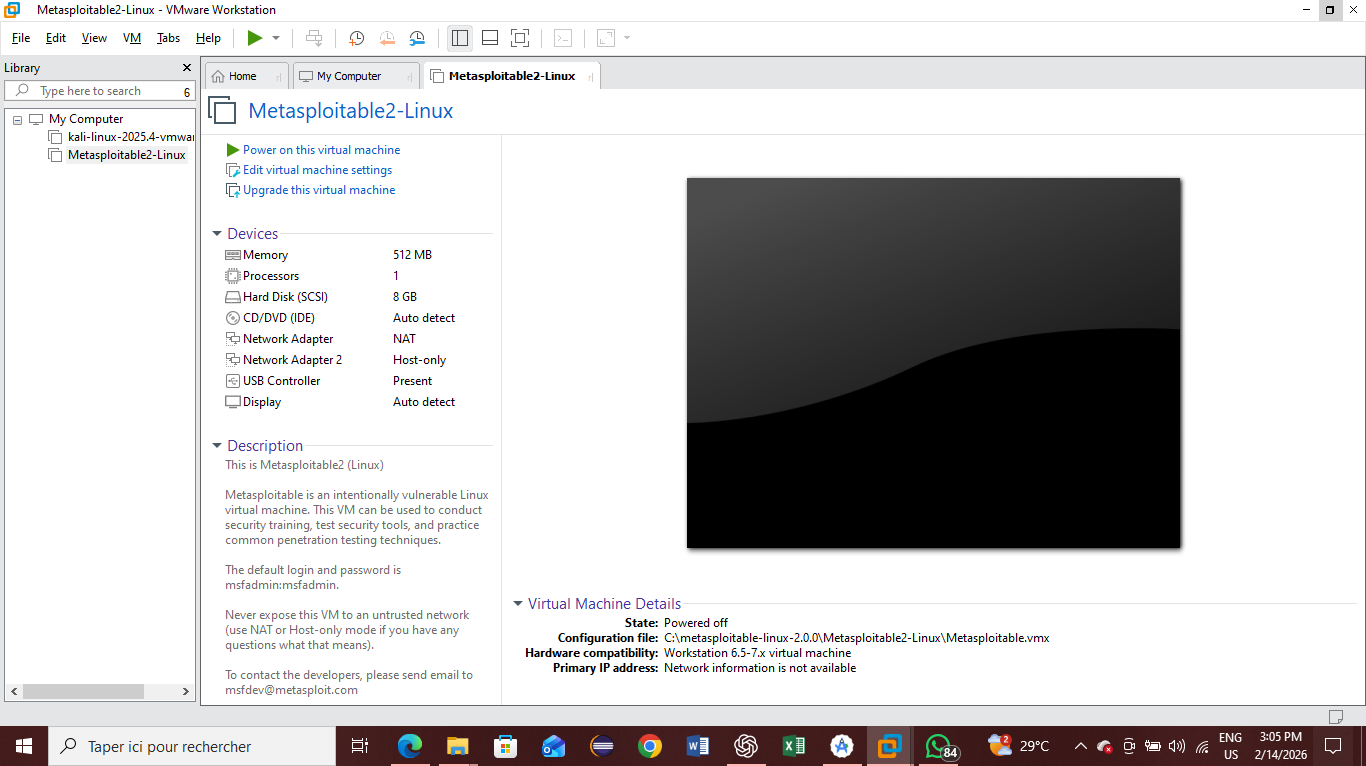
**Mise en place de l’environnement**

**.. Importation de la machine virtuelle Metasploitable**

Metasploitable 2 est une machine virtuelle Linux délibérément vulnérable. L’importation dans VMware s’est fait via le menu Fichier importer un appareil virtuel. La source choisie est Local File System et le fichier .vmx a été sélectionné.



Paramètre de l’Appliance après importation

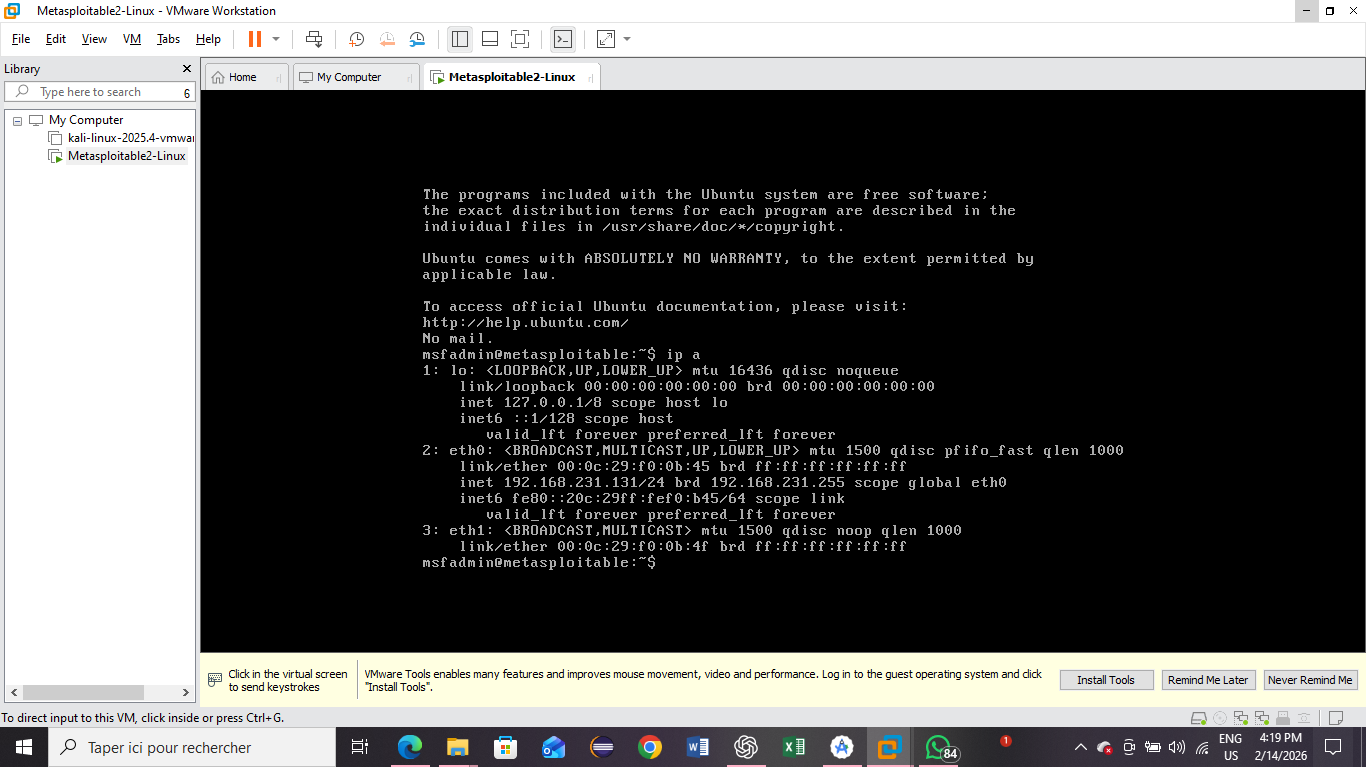


La machine a été démarrée sans modification supplémentaire.

**.. Obtention de l’adresse IP de la cible**

Une fois la machine démarrée, l’écran de connexion s’affiche.

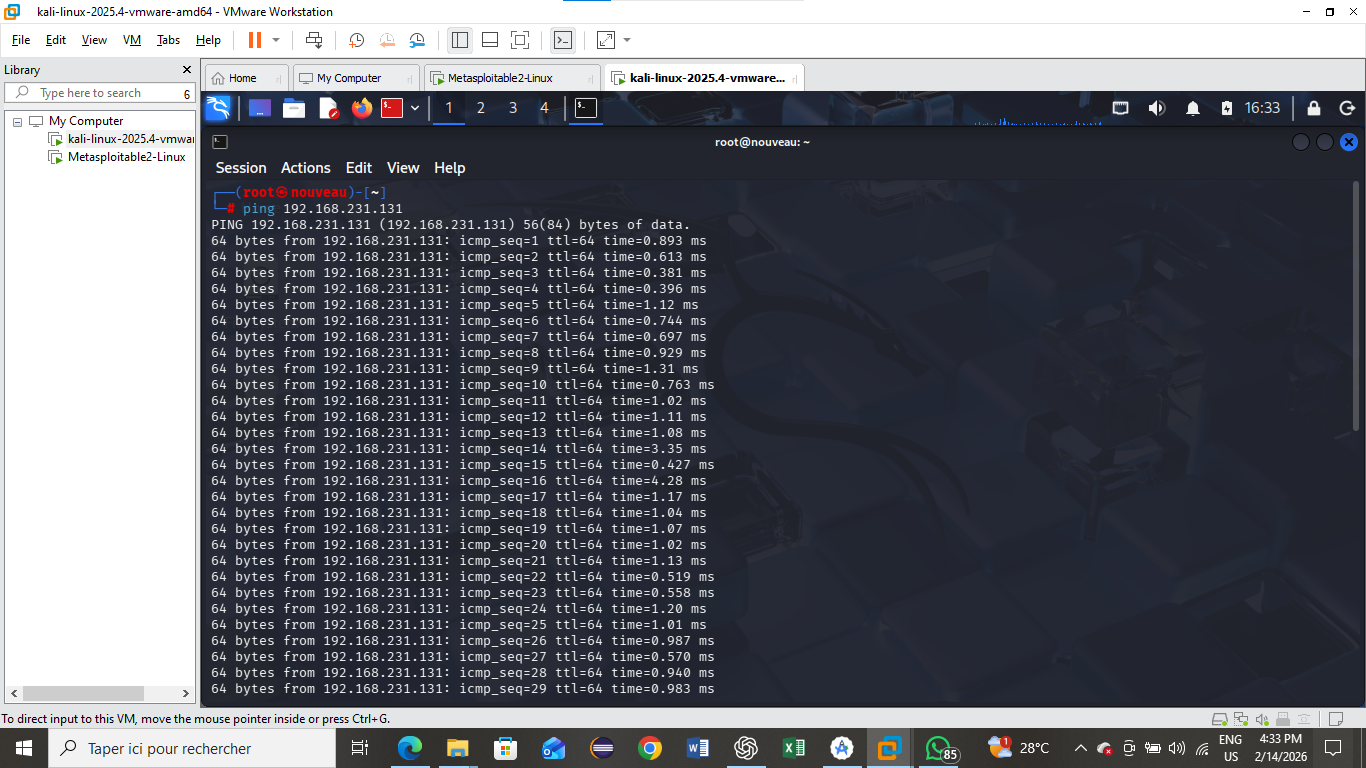
Les identifiants par défaut msfadmin / msfadmin permettent d’accéder au système. La commande IP a donné la configuration réseau :

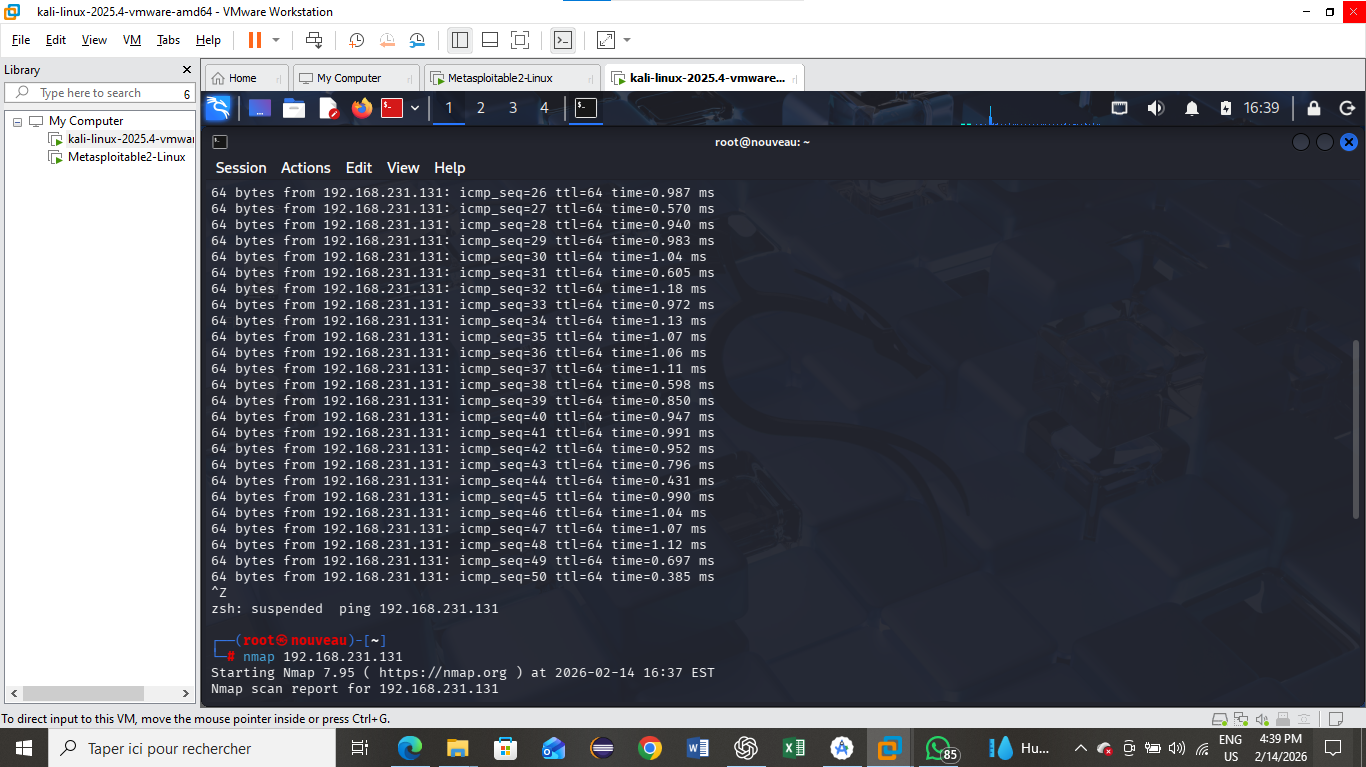


L’adresse IP de la machine sur le réseau hôte est 192.168.231.131. Elle servira de cible pour toutes les attaques.

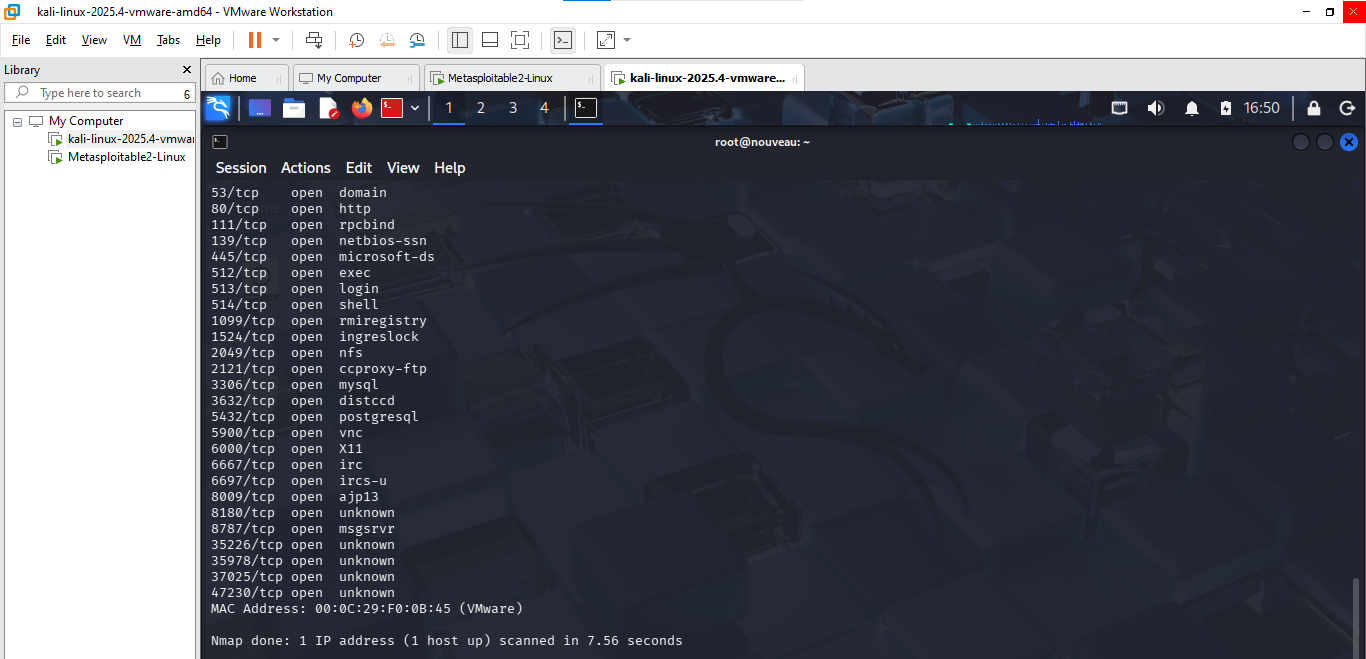
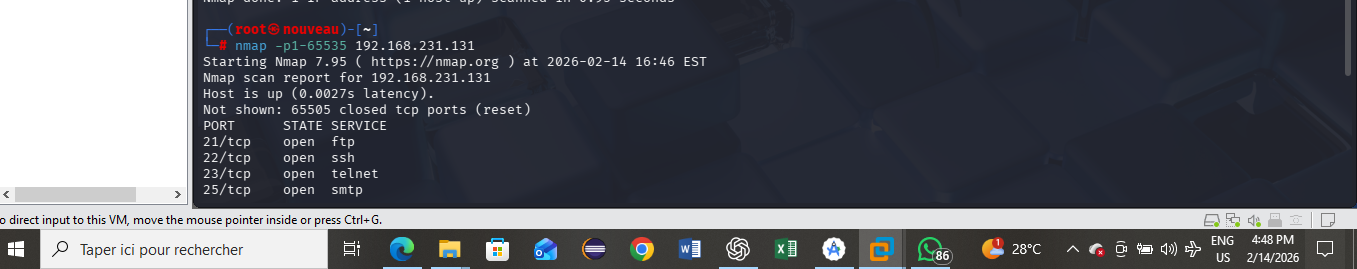
1. **Scan de vulnérabilité avec Nmap**

Depuis Kali Linux, après avoir passé les privilèges root (sudo-i), nous avons lancé un scan complet des ports TCP :





* 1. **Pour analyser tous les ports TCP**



* 1. **Exploitation des services vulnérables**

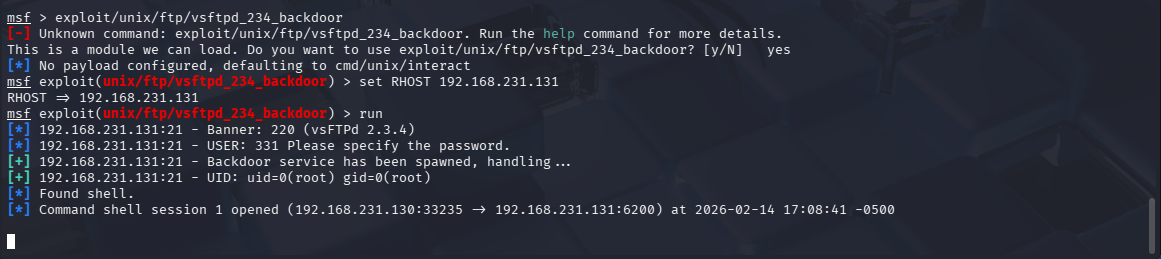
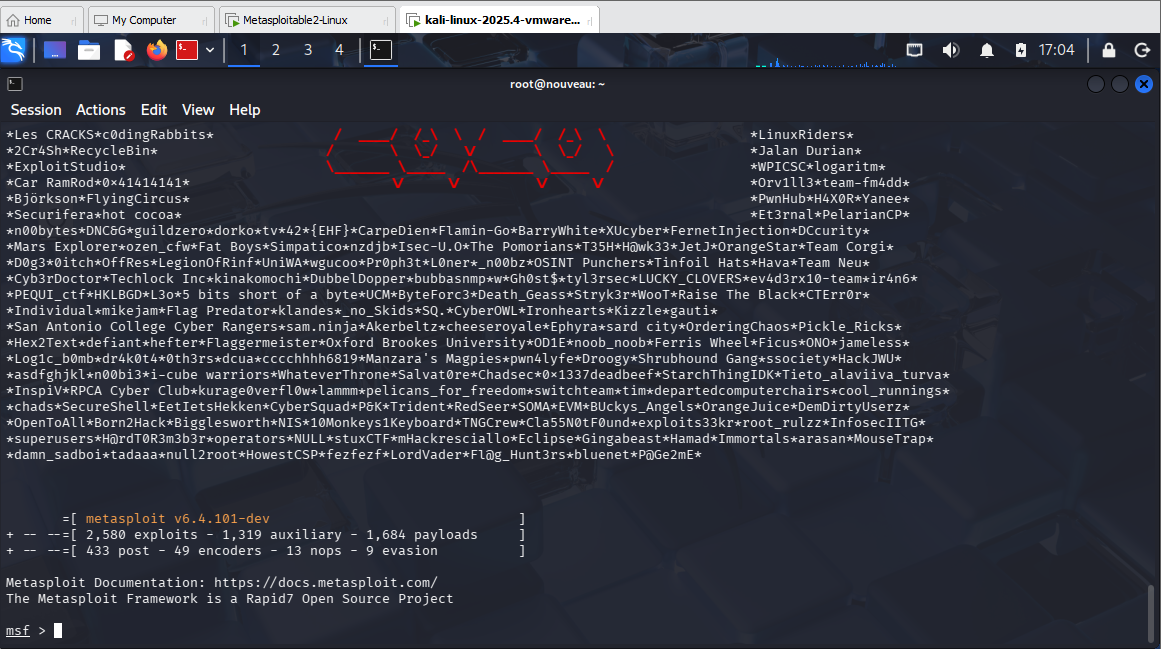
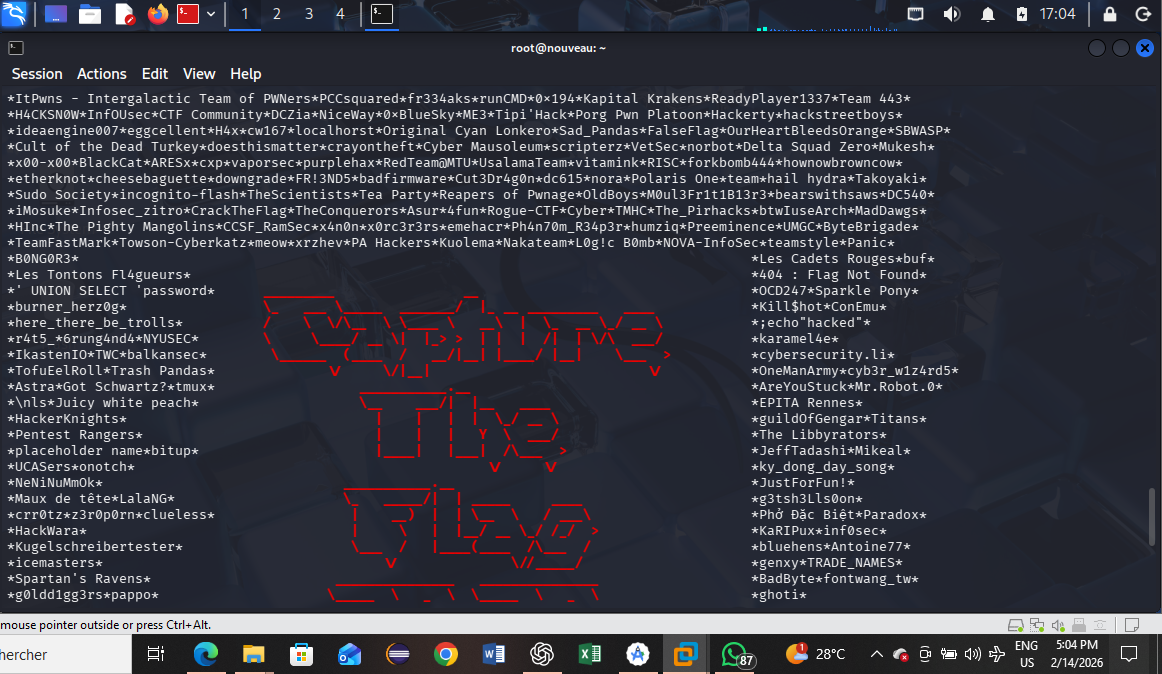
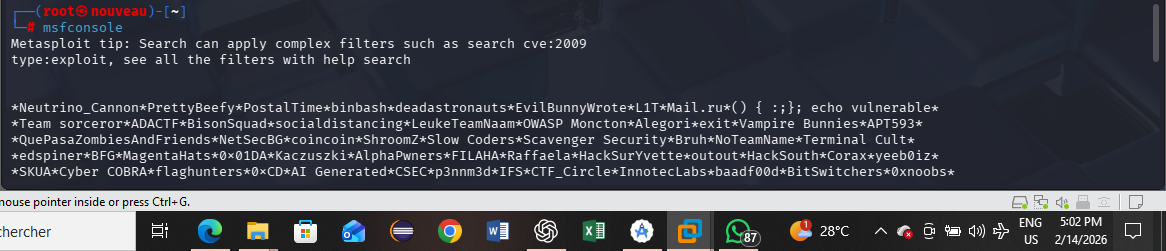
… **Telnet**

Le service Telnet (port 23) permet une connexion non chiffrée. Une simple commande Telnet 192.168.231.131 a abouti à l’invite de connexion. En utilisant les identifiants msfadmin / msfadmin, un Shell interactif a été obtenu.



1. **Exploits FTP –Metasploitable 2 via Metasploit**

**2.1** Le service FTP sur le port 21 utilise vsftpd version 2.3.4, connue pour contenir une Backdoor (CVE-2011-2523). L’exploitation a été réalisée avec Metasploit



**2.2 Scanner TCP**



**2.3 MySQL**

Le serveur MySQL (port 3306) est configuré avec un compte root sans mot de passe (ou root/root). Le module auxiliaire MySQL login de Metasploit a permis de valider cette vulnérabilité :



**2.4 PostgreSQL**

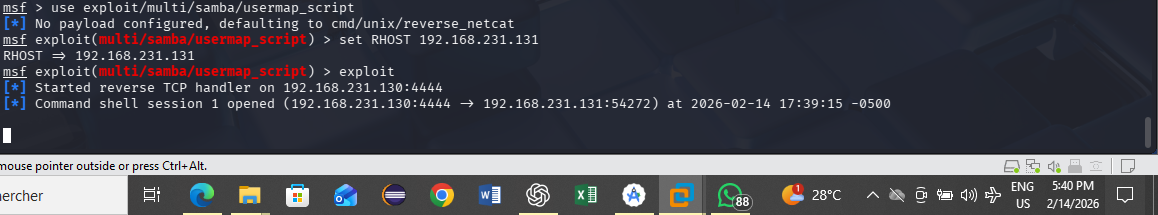
Le service PostgreSQL (port 5432) peut être exploité via le module postgres\_payload qui permet d’exécuter du code sur le serveur :



Pour la commande use auxiliary /admin /postgres / postgres\_payload on me dit no result from search failed to load search il me semble que ma machine ne supporte pas ce port

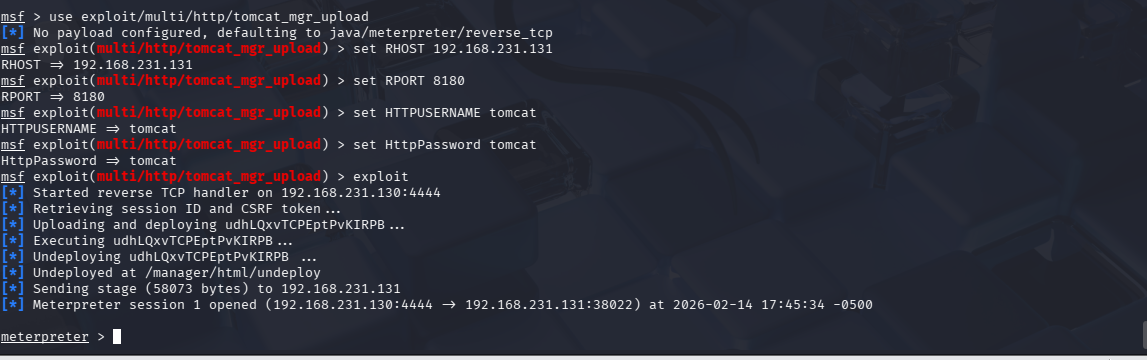
**2.5 Samba**

Samba (port 445) est vulnérable à une injection de commande via le script usermap (CVE-2007-2447). Exploit correspondant dans Metasploit a été utilisé:



**2.6 Apache Tomcat**

Le serveur Tomcat écoute sur le port 8180. Les identifiants par défaut tomcat/tomcat donnent accès au gestionnaire d’applications. Le module tomcat\_mgr\_upload permet de déployer une application malveillante (fichier WAR) et d’exécuter du code :



**Conclusion** Ce TP a permis de mettre en évidence plusieurs failles de sécurité classiques dans un système non maintenu :

· Mots de passe par défaut (msfadmin, root sans mot de passe, tomcat/tomcat) ;

· Services obsolètes (vsftpd 2.3.4, Samba ancien) ;

· Protocoles non sécurisés (Telnet en clair) ;

· Mauvaises configurations (accès au gestionnaire Tomcat sans restriction).

Chaque exploitation a abouti à l’obtention d’un accès, parfois avec les plus hauts privilèges. Ces résultats illustrent l’importance d’une politique de durcissement des systèmes : mise à jour régulière, suppression des services inutiles, utilisation de mots de passe forts et de protocoles chiffrés (SSH au lieu de Telnet), et restriction des interfaces d’administration.

En environnement réel, ces vulnérabilités pourraient être découvertes par un attaquant via un simple scan et conduire à une compromission totale du système. Ce TP souligne donc la nécessité d’audits de sécurité réguliers et de l’application des correctifs.