**UNIVERSITE DE TECHNOLOGIE D’HAÏTI**

**FACULTE DES SCIENCES DE GENIE CIVIL ET D’ARCHITECTURE**

**DEPARTEMENT DES SCIENCE INFORMATIQUE**

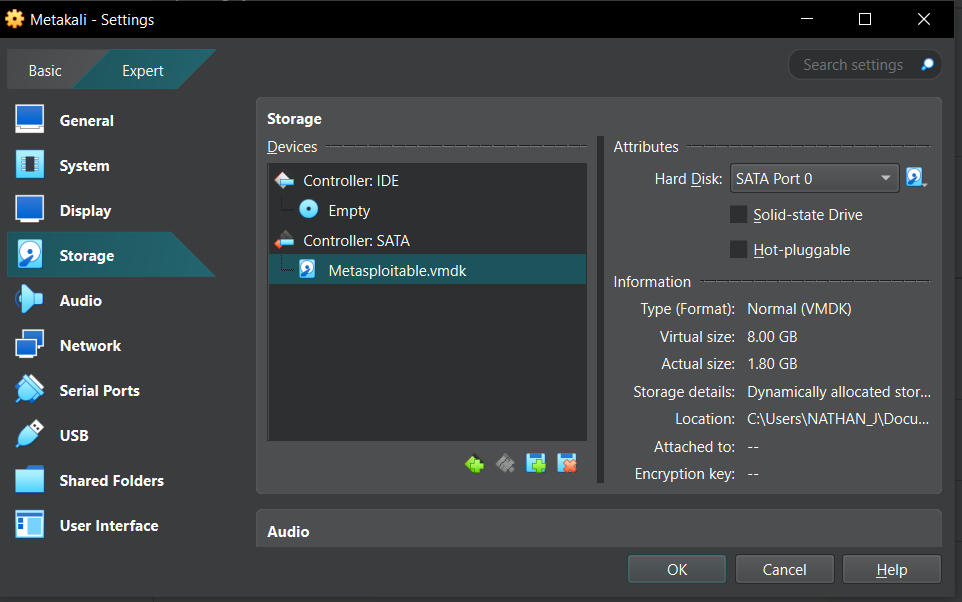
53, Avenue N, Port-au-Prince

Niveau: IV

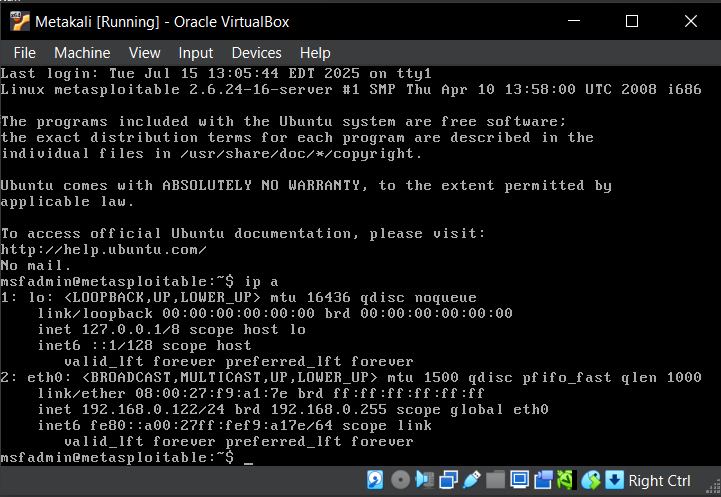
**Préparer par:** Jonathan JACQUES

**Soumis au professeur:** ING Ismaël Saint Amour dans le cadre du cours cyber sécurité.

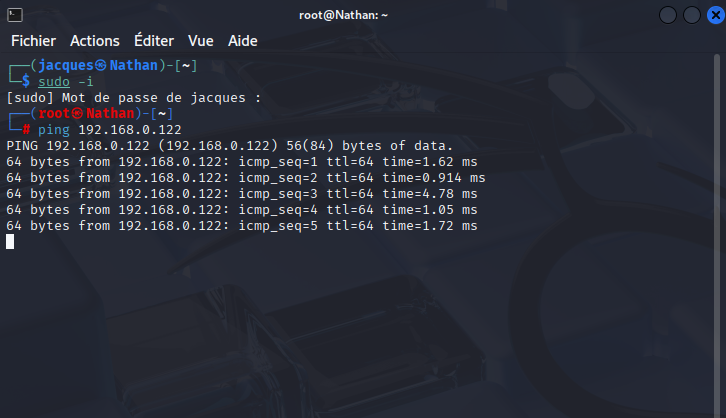
Le 15 Juillet 2025

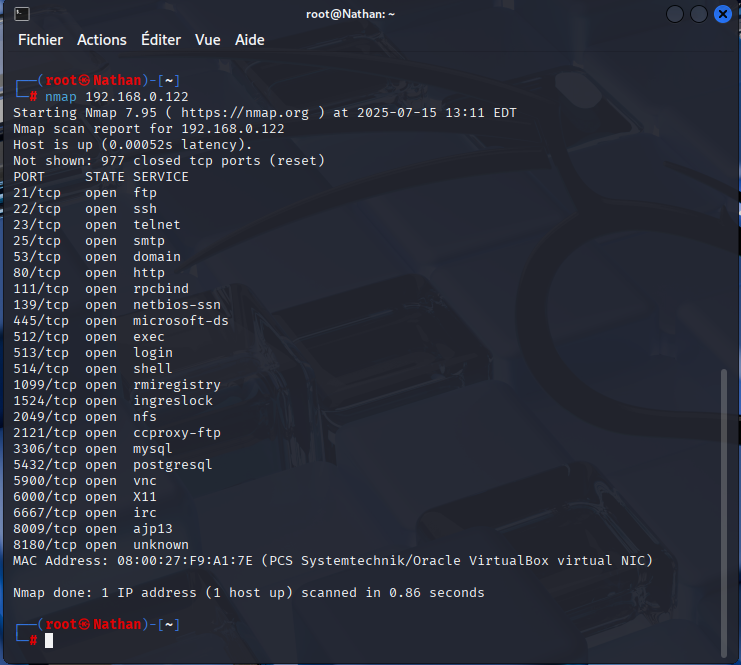
Importation Metasploitable 

Configuration Metasploitable

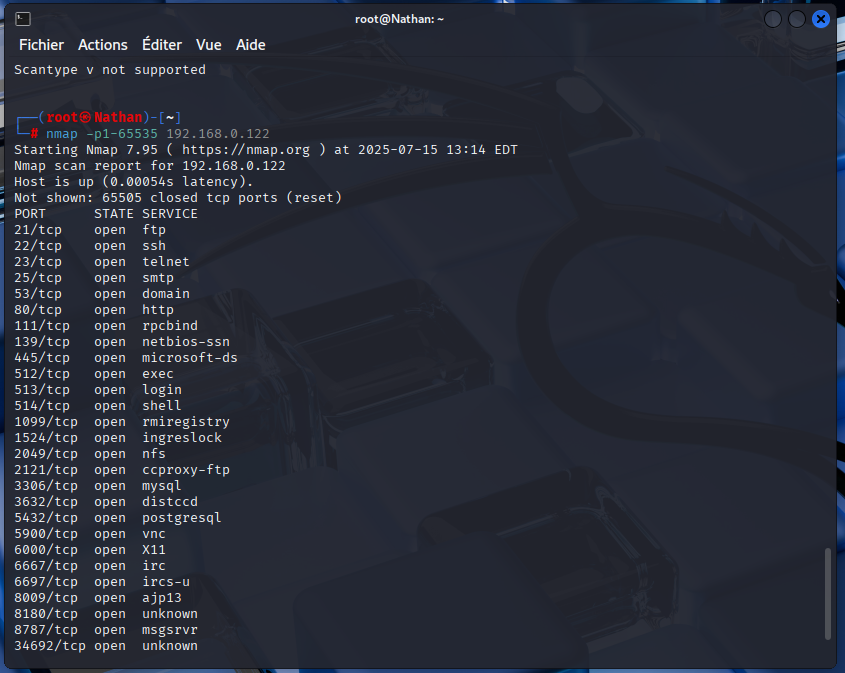


Scan de vulnérabilités

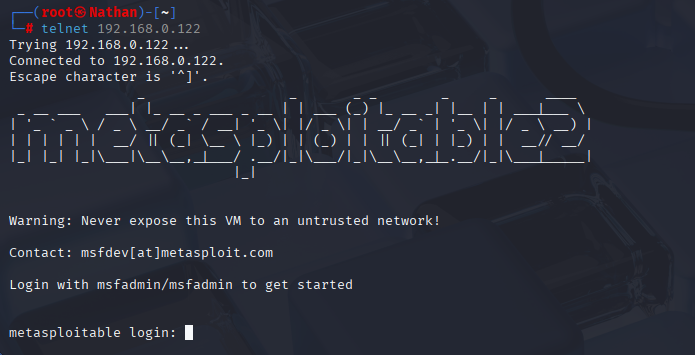


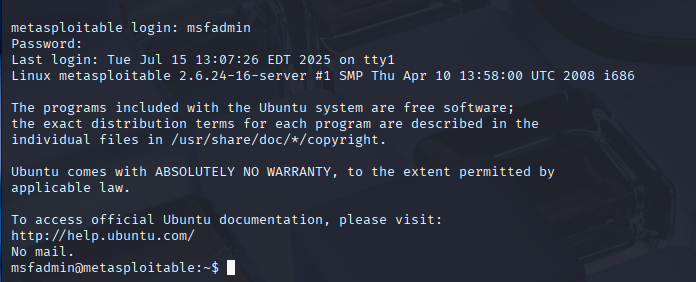


Analyser tous les ports TCP



Exploits telnet

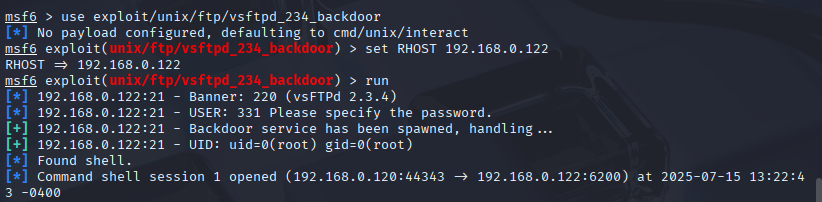




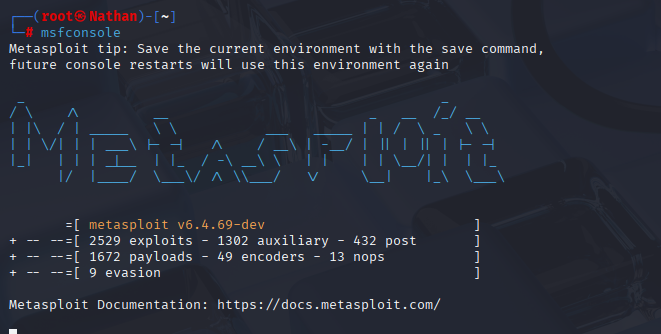
Exploits FTP – Metasploitable 2 via Metasploit

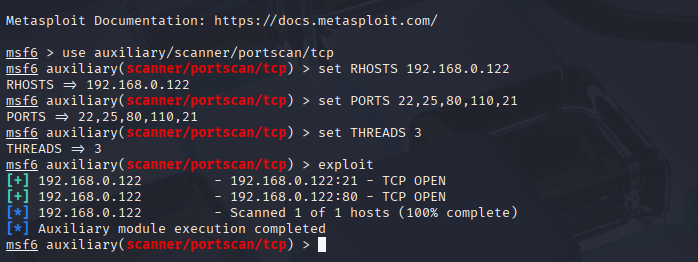
Backdoor Command Execution

\



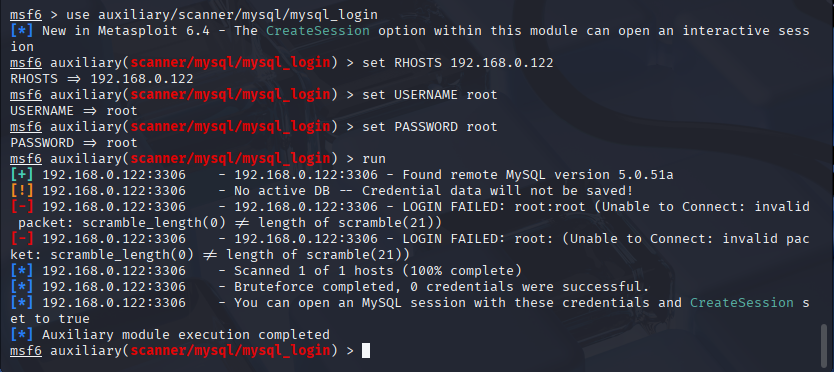
Scanner TCP





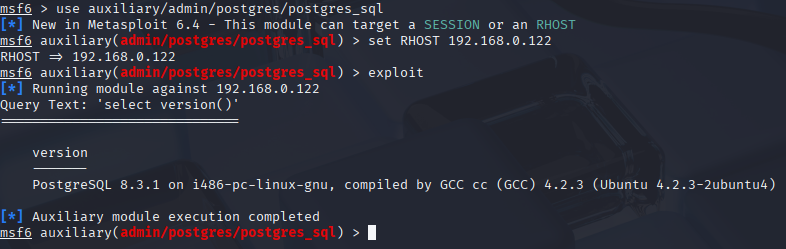
MySQL

Port : 3306



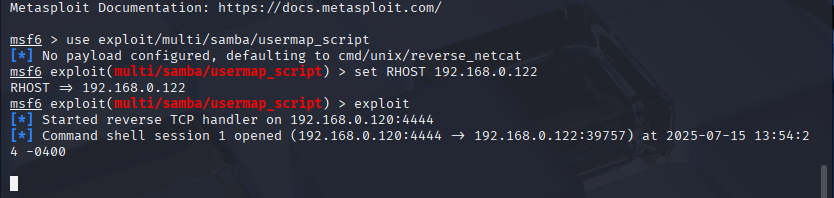
PostgreSQL

Port : 5432



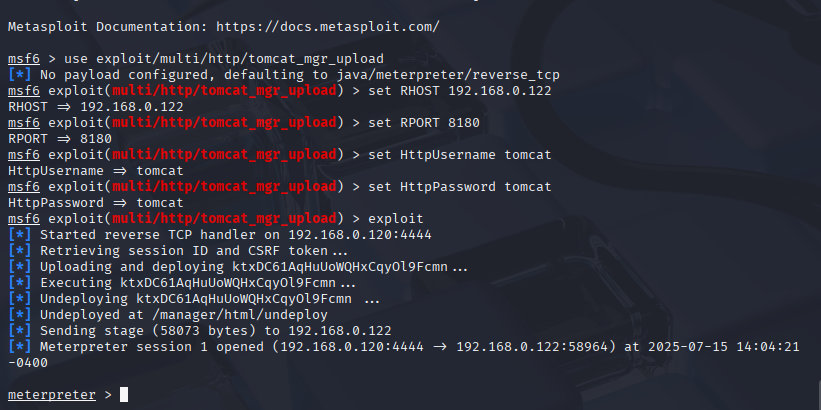
Samba

Port : 445



Apache Tomcat

Port : 8180



Description des résultats de la tâche

La tâche consistait à :

1. Importer et configurer la machine virtuelle Metasploitable 2 dans un environnement virtuel.

2. Réaliser un scan de vulnérabilités à l’aide d’outils comme Nmap.

3. Identifier les ports ouverts et les services associés.

4. Exploiter certaines vulnérabilités connues sur des services spécifiques : Telnet, FTP, MySQL, PostgreSQL, Samba, Apache Tomcat, etc., en utilisant Metasploit Framework.

Résultats de l'exécution des commandes (captures d'écran)

Le document contient plusieurs sections où des captures d’écran sont attendues, mais elles ne sont pas intégrées dans le fichier. Ces sections incluent :

Scan des ports TCP avec Nmap

Exploits Telnet

Exploitation FTP via Metasploit

Command Execution via Backdoor

Scanner TCP

Accès aux bases de données (MySQLcar le PostgreSQL ne voulait pas marcher)

Exploitation de Samba (port 445)

Exploitation d’Apache Tomcat (port 8180)

Conclusions sur la tâche accomplie

L’environnement virtuel Metasploitable 2 a été correctement importé et configuré.

Un scan complet des ports TCP a permis de recueillir des informations précieuses sur les services exposés.

Plusieurs services vulnérables ont été identifiés et des exploits ont été réalisés avec succès grâce à Metasploit, notamment sur Telnet, FTP et les bases de données.

Le test démontre l'importance de la sécurité réseau et du renforcement des systèmes vulnérables.