Cybersécurité

Pentesting

Projet de cybersécurité du semestre 3 - IUT de La Rochelle

Matthias DUMAS - 2025

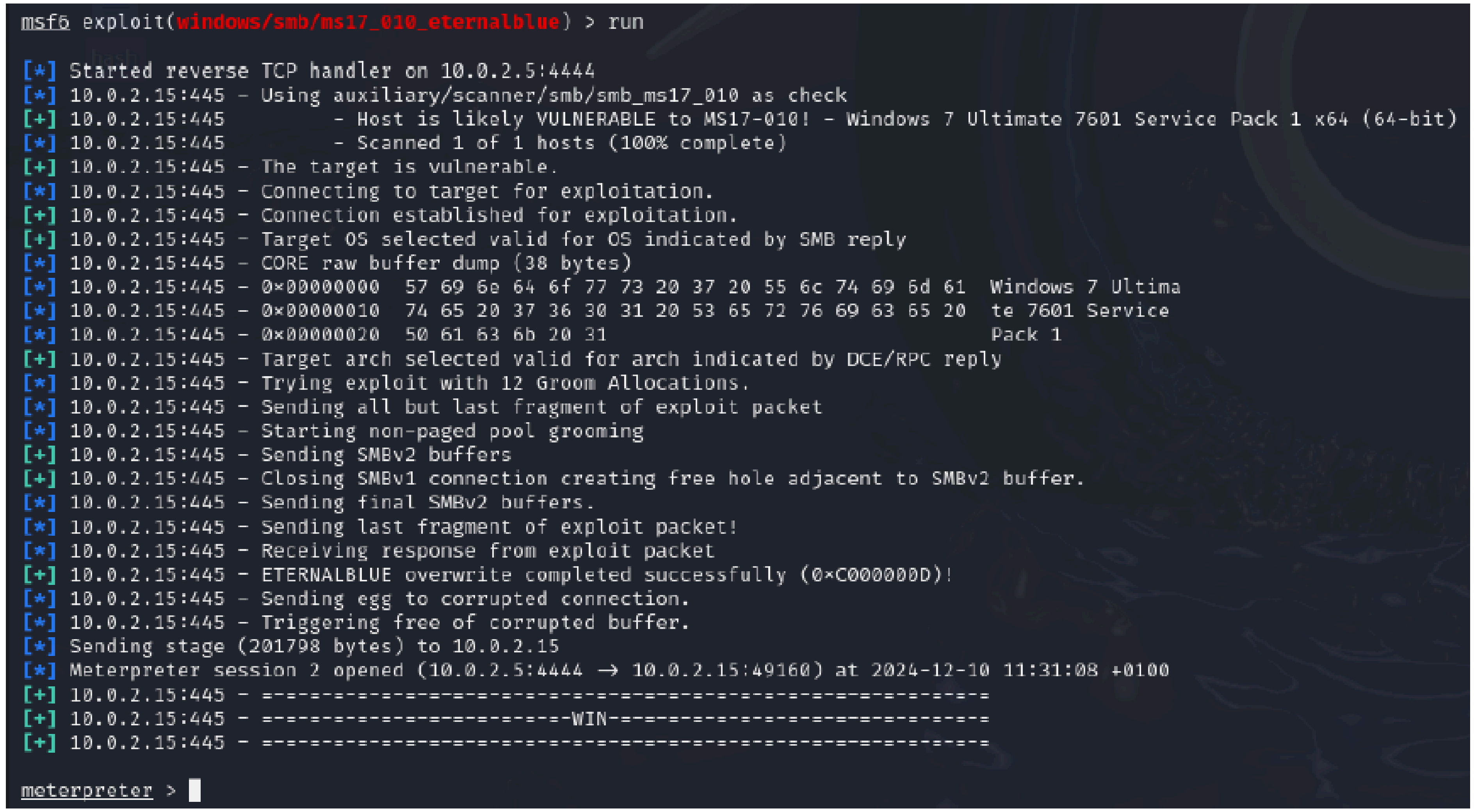
Introduction

La SAE de cybersécurité du semestre 3 a pour but de découvrir les différentes méthodes de pentesting. Ce projet, réalisé en binôme, nous permet de nous familiariser avec les différentes failles couramment trouvées sur des systèmes Windows et Linux.

Le pentesting, ou test d'intrusion, vise à reproduire une attaque sur un système informatique afin de détecter ses vulnérabilités. Cela permet d'identifier les failles de sécurité avant qu'elles ne puissent être exploitées par des individus malveillants. Cette démarche aide les entreprises à améliorer leur sécurité en anticipant les risques. Le projet s'est concentré sur l'analyse de 5 machines vulnérables fournies par TCM Security.

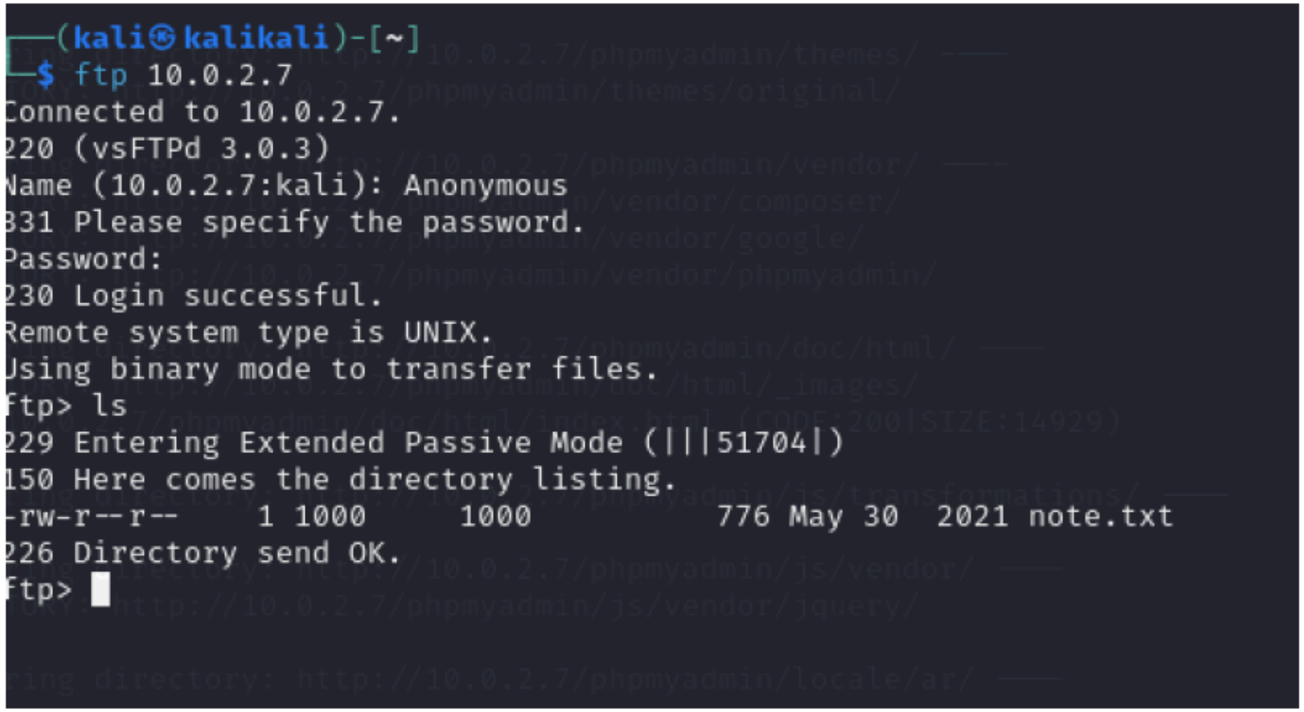
Présentation des attendus

Il nous a été demandé de prendre l'accès administrateur sur 5 machines virtuelles (2 Windows, 3 Linux) à partir d'une machine d'attaque Kali Linux.
Nous avons dû utiliser les 7 étapes de la Cyber Kill Chain afin d'avoir une marche à suivre.



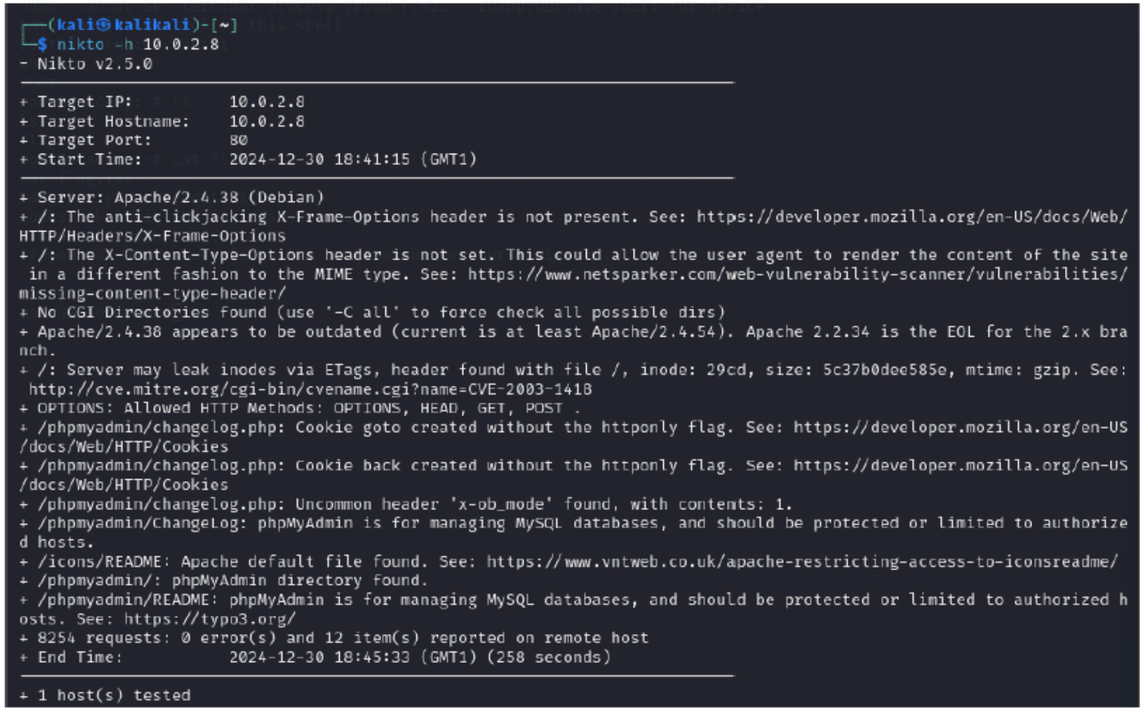
Connaissances exploitées

Nous avons pu exploiter nos connaissances acquises lors des cours de pentesting du semestre 3. Nous avons également dû beaucoup utiliser Internet afin de faire des recherches précises concernant les différente failles découvertes afin de mieux comprendre le fonctionnement de ces dernières.
Nous avons utilisé les différents outils de Kali (Nmap, Hydra, Metasploit, BurpSuite) pour arriver à nos fins.



Difficultés rencontrées

La difficulté était de réussir à obtenir l'accès des 5 machines virtuelles dans le temps imparti. En effet, nous avions assez peu de séances de travail pour faire nos recherches et éditer un rapport complet.
Aussi, nous n'avions pas suffisamment de connaissances pour être efficace dans nos recherches.
Nous avons tout de même pu finir en avance le projet.



Compétences développées

Cette SAE nous a permis de développer nos compétences dans le domaine du pentesting et de la recherche de failles. Nous nous sommes rendus compte que beaucoup de failles différentes pouvaient exister, et que certaines étaient très facilement détectables pour un attaquant.
Enfin, nous avons pu approfondir nos connaissances sur le fonctionnement de certaines failles et de la méthodologie d'attaque des hackers.