Лабораторна робота №1

Основи етичного хакінгу та тестування на проникнення. Мережеве сканування за допомогою Nmap

Мета роботи:

1. Ознайомлення з основними поняттями етичного хакінгу та тестування на проникнення.
2. Вивчення основних етапів тестування на проникнення.
3. Набуття практичних навичок роботи з інструментом мережевого сканування Nmap.

Хід роботи

Завдання 1. Реєстрація на платформах.

1. Зареєструватися на платформі TryHackMe (https://tryhackme.com/)

Для реєстрації на платформі TryHackMe рекомендується використовувати особисту електронну пошту, щоб забезпечити збереження результатів після деактивації університетської пошти.

2. Зареєструватися на платформі LabEx (https://labex.io)

Завдання 2. Проходження кімнати TryHackMe.

Кімната для проходження - Pentesting Fundamentals: https://tryhackme.com/room/pentestingfundamentals

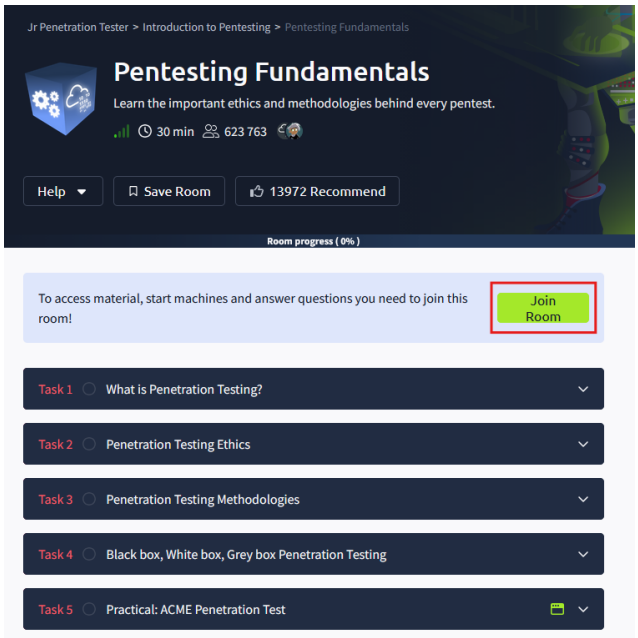

Рисунок 1 – Кімната Pentesting Fundamentals на платформі TryHackMe

Щоб розпочати проходження кімнати, необхідно натиснути кнопку «Join Room», після чого з’явиться можливість вводити відповіді.

Під час проходження:

1. Уважно ознайомитися з теоретичним матеріалом.
2. Відповісти на всі питання кімнати (разом з практичною частиною в останньому завданні).
3. Отримати статус Completed.
4. Оформити скріншот успішно пройденої кімнати у звіт.

Завдання 3. Ознайомлення з інструментом для мережевого сканування Nmap.

Інструмент Nmap (Network Mapper) є одним з базових засобів етичного хакінгу та тестування на проникнення і використовується на етапі мережевого сканування та розвідки (Scanning & Enumeration). За допомогою Nmap визначаються активні хости в мережі, відкриті порти, запущені сервіси, а також особливості конфігурації мережевих захисних механізмів.

З метою отримання практичних навичок роботи з інструментом Nmap необхідно виконати навчальні кімнати на платформі LabEx:

1. Learn Nmap Fundamentals for Network Scanning: https://labex.io/labs/nmap-learn-nmap-fundamentals-for-network-scanning-415922
2. Use Nmap to Detect and Bypass Firewall Restrictions: https://labex.io/labs/nmap-use-nmap-to-detect-and-bypass-firewall-restrictions-415921
3. Perform Stealth Network Scanning with Nmap: https://labex.io/labs/nmap-perform-stealth-network-scanning-with-nmap-415933

Виконання завдання здійснюється без використання локальної віртуальної машини Kali Linux, оскільки платформа LabEx забезпечує доступ до попередньо налаштованого віртуального навчального середовища з необхідними інструментами.

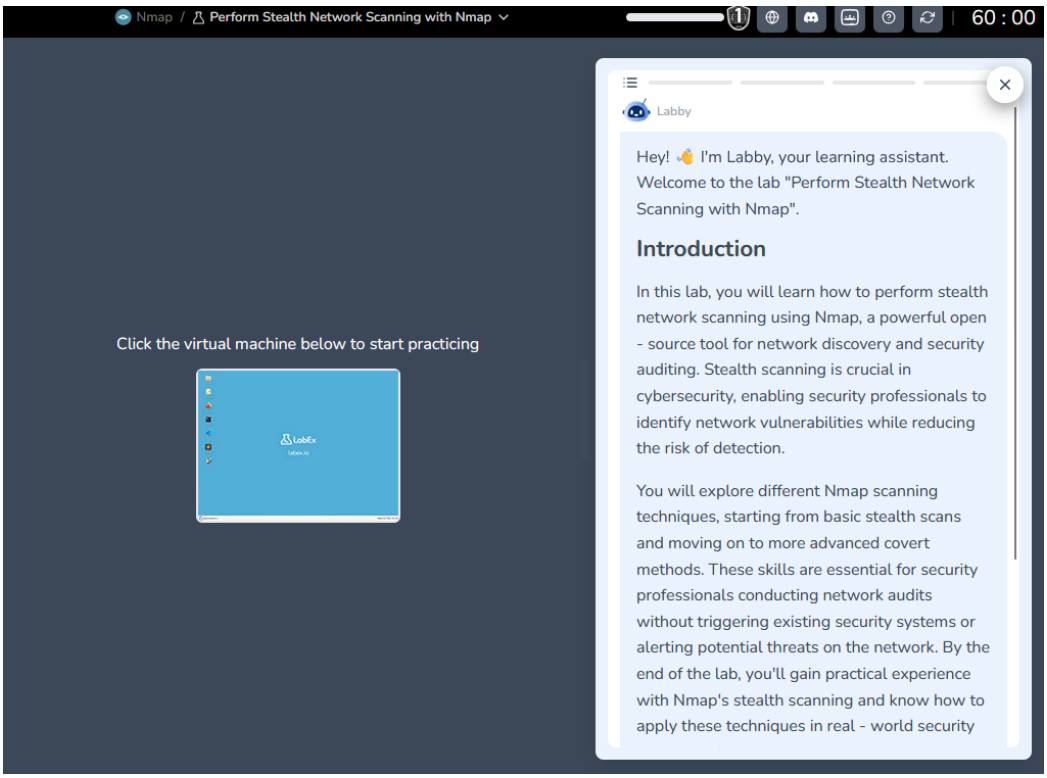

Рисунок 2 – Приклад навчальної кімнати на платформі LabEx

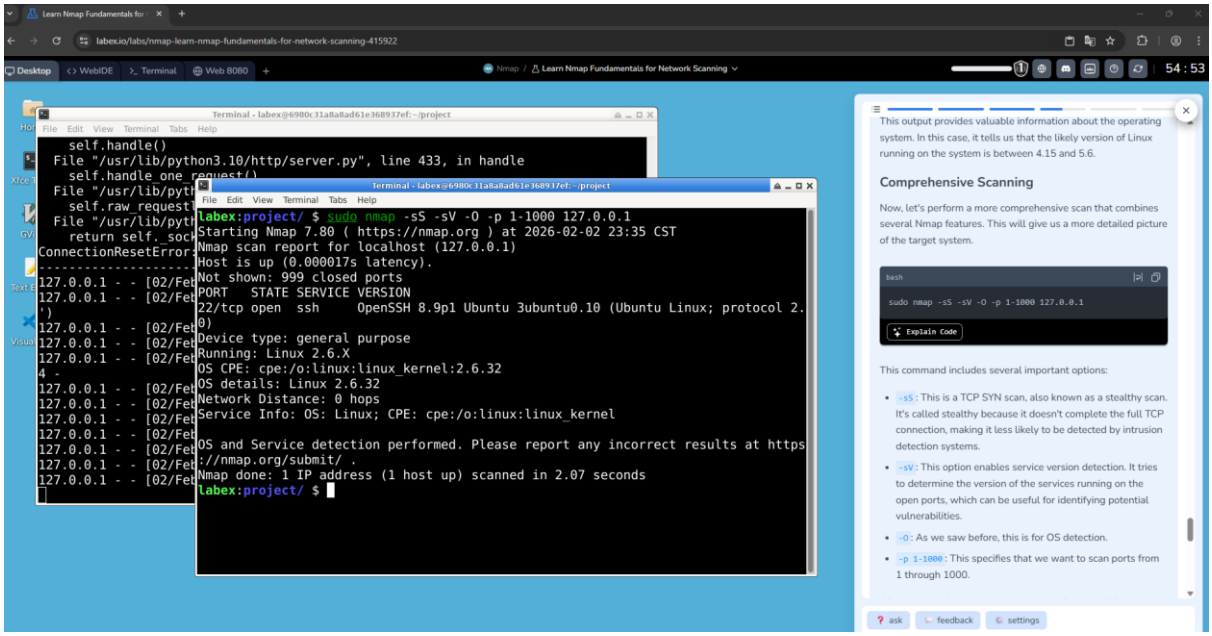

Рисунок 3 – Приклад виконання завдання на платформі LabEx

Під час виконання навчальних кімнат необхідно зробити скріншоти результатів виконання кожного завдання (завершення завдання, виконані кроки або отриманий статус). Скріншоти виконаних завдань мають бути додані до звіту з лабораторної роботи з відповідними короткими поясненнями.