

# **ЛАБОРАТОРНА РОБОТА №1**

## **ОСНОВИ ЕТИЧНОГО ХАКІНГУ ТА ТЕСТУВАННЯ НА ПРОНИКНЕННЯ. МЕРЕЖНЕ СКАНУВАННЯ ЗА ДОПОМОГОЮ NMAP**

### **Мета роботи:**

1. Ознайомлення з основними поняттями етичного хакінгу та тестування на проникнення.
2. Ознайомлення з основними етапами проведення тестування на проникнення.
3. Ознайомлення з поняттям мережної розвідки та її роллю під час тестування на проникнення.
4. Вивчення основних можливостей інструменту Nmap.
5. Набуття практичних навичок виявлення активних хостів, відкритих портів та мережних сервісів.
6. Набуття навичок аналізу результатів мережного сканування.

**Інструменти та ПЗ:** Kali Linux, Nmap, Metasploitable2.

### **Теоретичні відомості**

Етичний хакінг – це контрольоване дослідження інформаційних систем, мереж та веб-застосунків з метою виявлення вразливостей і недоліків безпеки за наявності відповідного дозволу.

На відміну від зловмисної атаки, під час етичного хакінгу дослідження проводиться в установлених межах і має визначену мету – оцінити рівень захищеності системи та надати рекомендації щодо усунення виявлених проблем.

### **Тестування на проникнення**

Тестування на проникнення (Penetration Testing, Pentesting) – це контрольований процес моделювання дій потенційного зловмисника для перевірки захищеності інформаційної системи.

У спрощеному вигляді процес тестування можна представити такими темпами:

1. Planning/Pre-engagement – визначення цілей, меж та правил тестування.

2. Reconnaissance – збір інформації про ціль

3. Scanning & Enumeration – виявлення хостів, портів, сервісів та іншої технічної інформації.

4. Vulnerability Assessment – визначення потенційних вразливостей.

5. Exploitation – перевірка можливості експлуатації вразливостей.

6. Post-Exploitation – аналіз можливих наслідків отриманого доступу.

7. Reporting – документування результатів та рекомендацій.

### **Розвідка та мережне сканування**

Розвідка (Reconnaissance) – це процес збору інформації про цільову систему, яка може бути використана під час подальших етапів тестування.

Розвідку умовно поділяють на:

1. Пасивну.

2. Активну.

Пасивна розвідка – це процес отримання інформації без безпосередньої взаємодії з інфраструктурою цілі.

Активна розвідка – це безпосередня взаємодія з цільовою системою для отримання технічної інформації.

Окремими завданнями мережного сканування є:

1. Визначення активних хостів.

2. Визначення відкритих портів.

3. Визначення мережних сервісів.

4. Визначення версій сервісів.

5. Отримання додаткової інформації про конфігурацію цільової системи.

### **Порти та мережні сервіси**

Мережний порт – це логічна точка взаємодії із сервісом у мережі. TCP та UDP використовують номери портів від 0 до 65535.

Таблиця 1. Відповідність портів та типових сервісів

| Порт       | Типовий сервіс |
|------------|----------------|
| 21/TCP     | FTP            |
| 22/TCP     | SSH            |
| 23/TCP     | Telnet         |
| 25/TCP     | SMTP           |
| 53/TCP/UDP | DNS            |
| 80/TCP     | HTTP           |
| 443/TCP    | HTTPS          |
| 3306/TCP   | MySQL          |
| 3389/TCP   | RDP            |

Відкритий порт не означає автоматично наявність вразливості. Проте він вказує на доступний мережний сервіс, який може потребувати подальшого дослідження.

### Nmap

Nmap (Network Mapper) – це інструмент для дослідження мереж та систем, який використовується для виявлення хостів, відкритих портів, мережних сервісів та їх версій.

Загальний синтаксис:

```
nmap [параметри] <IP-адреса цілі>
```

Приклад використання інструмента Nmap:

```
nmap -sV -sC 10.0.2.15
```

Таблиця 2. Основні параметри Nmap

| Параметр | Призначення                                     |
|----------|-------------------------------------------------|
| -sn      | Виявлення активних хостів без сканування портів |
| -sS      | TCP SYN scan                                    |
| -sT      | TCP Connect scan                                |
| -sV      | Визначення версій сервісів                      |

|     |                                                                   |
|-----|-------------------------------------------------------------------|
| -sC | Запуск стандартного набору NSE-скриптів                           |
| -p  | Вказання портів для сканування                                    |
| -O  | Спроба визначення операційної системи                             |
| -A  | Комплексне сканування з визначенням версій, ОС, NSE та traceroute |

Таким чином, мережна розвідка за допомогою Nmap може виконуватися поетапно: спочатку визначаються активні хости, після чого досліджуються відкриті порти, запуснені на них сервіси та їх версії. Отримана інформація використовується для подальшого аналізу потенційних вразливостей цільової системи.

Приклади використання Nmap:

*nmap 10.0.2.15 – виконання базового сканування цільового хоста*

*nmap -sV 10.0.2.15 – додатково спроба визначення версії запусчених сервісів.*

*nmap -sV -sC 10.0.2.15 – сканування з визначенням версій сервісів та запуском стандартного набору NSE-скриптів.*

### Хід роботи

#### Завдання 1. Ознайомлення з тестуванням на проникнення.

Для виконання завдання необхідно використати навчальну кімнату Pentesting Fundamentals на платформі TryHackMe.

Посилання:

<https://tryhackme.com/room/pentestingfundamentals>

Необхідно:

1. Приєднатися до кімнати.
2. Ознайомитися з теоретичними відомостями.
3. Виконати всі завдання кімнати.
4. Отримати статус Completed.
5. Додати до звіту скріншот завершеної кімнати.

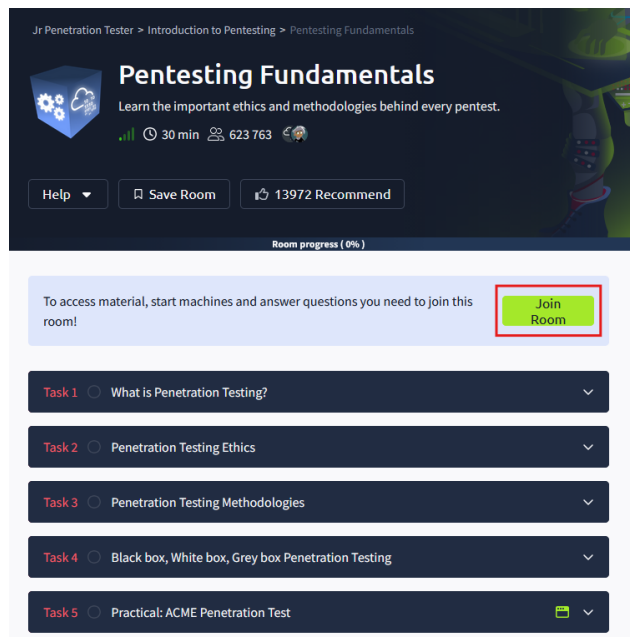


Рисунок 1 – Кімната Pentesting Fundamentals на платформі TryHackMe

## Завдання 2. Імпорт віртуальної машини Kali Linux з курсу Cisco.

1. Завантажити готовий образ віртуальної машини у форматі .ova зі сторінки дисципліни (VM Kali Linux (Cisco)).
2. Запустити середовище Oracle VM VirtualBox.
3. У головному меню обрати пункт “File” → “Import Appliance”

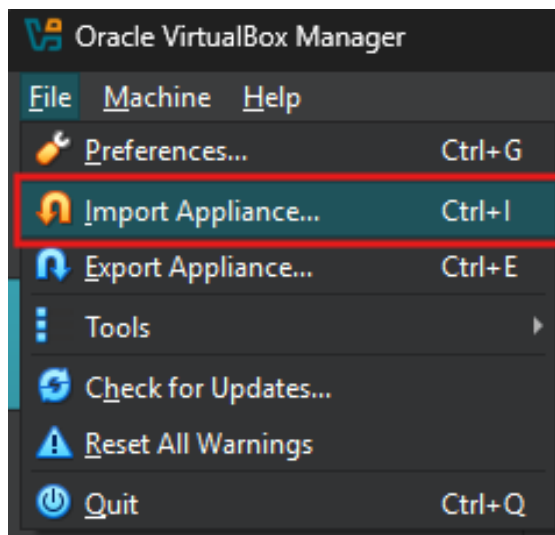


Рисунок 4 – Вкладка “File” → “Import Appliance”

4. У полі “File” обрати завантажений образ віртуальної машини.

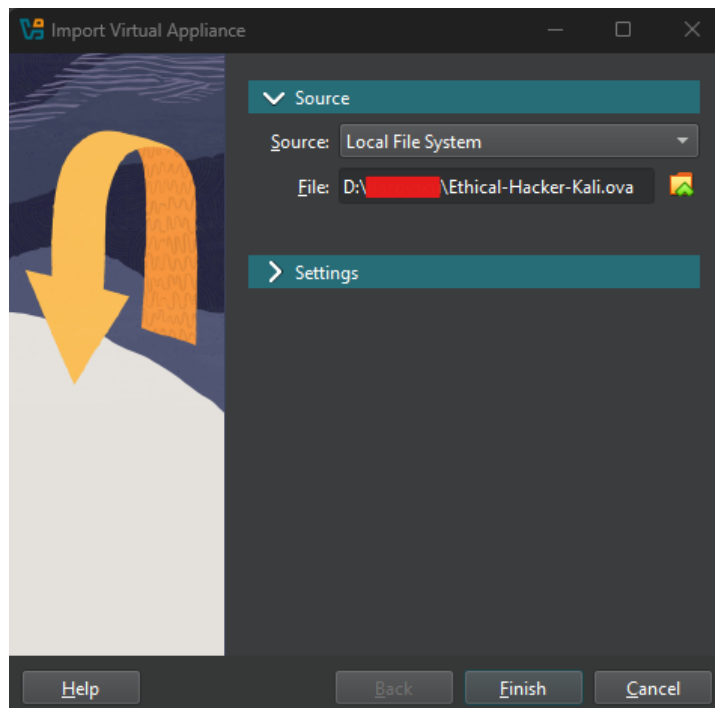


Рисунок 5 – Процес імпорту віртуальної машини Kali Linux у середовище VirtualBox

5. У вікні налаштувань змінити назву віртуальної машини, додавши **власне прізвище**, а також встановити обсяг оперативної пам'яті на рівні 4000 МБ.

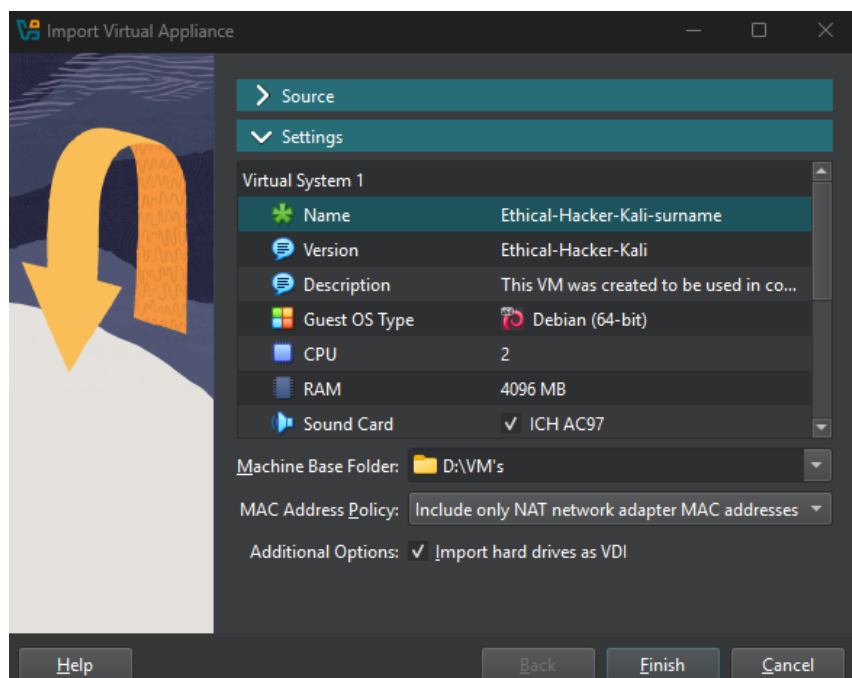


Рисунок 6 – Налаштування параметрів VM Kali Linux

6. Натиснути кнопку “Finish” та дочекатися завершення процесу імпорту віртуальної машини до середовища VirtualBox.

**Примітка.** Усі подальші практичний завдання лабораторної роботи виконуються у віртуальній машині *Kali Linux Ethical Hacker* (збірка від Cisco). Цільовим середовищем для сканування є ізольована *Docker*-мережа з адресним простором *172.17.0.0/24*.

**Завдання 3.** Визначення активних хостів в мережі.

1. Виконати сканування *Docker*-мережі *172.17.0.0/24* за допомогою *Nmap* у режимі виявлення активних хостів:

```
nmap -sn 172.17.0.0/24
```

2. На основі результатів сканування визначити:
  - Кількість активних хостів у мережі.
  - IP-адресу кожного активного хоста.
  - Ім'я хоста, якщо воно визначається *Nmap*.
3. Визначити, який із виявлених хостів відповідає цільовій системі *Metasploitable2*.

У звіті навести результати сканування та зазначити IP-адресу цільової системи *Metasploitable2*.

**Завдання 4.** Сканування відкритих портів.

1. Виконати базове сканування цільової системи *Metasploitable2*, IP-адресу якої було визначено під час виконання попереднього завдання.
2. Проаналізувати результати сканування.
3. Визначити всі відкриті TCP-порти цільової системи.
4. Для кожного відкритого порту визначити номер порту та стан.
5. Виконати TCP SYN-сканування цільової системи:

```
sudo nmap -sS 172.17.0.2
```

6. Порівняти результати базового сканування та SYN-сканування.

**Завдання 5.** Визначення мережних сервісів та їх версій.

1. Виконати сканування цільової системи з визначенням версій сервісів:

```
nmap -sV 172.17.0.2
```

2. На основі результатів сканування визначити інформацію про такі мережні сервіси:

- FTP.
- SSH.
- HTTP.
- SMB.

3. Для кожного із зазначених сервісів визначити:

- Номер порту.
- Стан порту.
- Назву сервісу.
- Версію програмного забезпечення.

4. Виконати сканування із використанням стандартних NSE-скриптів.

5. Проаналізувати додаткову інформацію, отриману NSE-скриптами для FTP, SSH, HTTP та SMB.

**Завдання 6.** Аналіз результатів мережного сканування.

На основі результатів виконання попереднього завдання:

1. Обрати один з чотирьох сервісів (FTP, SSH, HTTP, SMB).

2. Для одного з обраних сервісів за допомогою відкритих джерел знайти відомі вразливості відповідної версії програмного забезпечення.

3. Для знайденої вразливості визначити:

- Ідентифікатор CVE.
- Короткий опис вразливості.
- Версію програмного забезпечення, для якої вона актуальна.
- Тип або клас вразливості.

4. Сформулювати короткий висновок щодо того, яку інформацію про цільову систему вдалося отримати на етапі мережної розвідки та як ця інформація може бути використана для подальшого дослідження безпеки системи.

## **Контрольні запитання**

1. Що таке етичний хакінг та яка його основна мета?
2. Що таке тестування на проникнення (Penetration Testing)?
3. Які основні етапи тестування на проникнення?
4. Що таке мережна розвідка?
5. У чому полягає різниця між пасивною та активною розвідкою?
6. Що таке Nmap та для яких завдань він використовується?
7. Яка команда Nmap використовується для виявлення активних хостів без сканування портів?
8. Для чого використовується параметр -sn у Nmap?
9. Яку інформацію можна отримати за допомогою визначення версій сервісів?
10. Чому факт наявності відкритого порту сам по собі не означає наявності вразливості?