КОМП'ЮТЕРНІ МЕРЕЖІ

ЛІТНЯ ШКОЛА З КІБЕРБЕЗПЕКИ

ПРАКТИЧНЕ ЗАНЯТТЯ №1

Завдання №1. Визначення мережних параметрів системи.

Ваша мета: Навчитися отримувати базову інформацію про мережні налаштування Linux.

Команди для виконання завдання:

ip a

ip route

hostname -I

Завдання:

1. Визначити IP-адресу системи.
2. Визначити назву мережного інтерфейсу.
3. Визначити шлюз за замовчуванням.
4. Визначити адресу мережі.

Питання для обговорення:

1. Що таке IP-адреса?
2. Для чого потрібен шлюз?
3. Чим відрізняється локальна та публічна IP-адреса?

Завдання №2. Робота з IPv4 та підмережами.

Ваша мета: Навчитися визначати параметри підмережі.

Інструмент:

https://www.calculator.net/ip-subnet-calculator.html

Для адреси:

192.168.10.55/24 та *10.10.20.15/27*

Визначити:

1. Адресу мережі.
2. Broadcast-адресу.
3. Першу адресу вузла.
4. Останню адресу вузла.
5. Кількість доступних вузлів.

Питання для обговорення:

1. Для чого використовується маска підмережі?
2. Що таке broadcast адреса?
3. Чому адреси мережі та broadcast не можуть призначатися хостам?

Завдання №3. Побудова локальної мережі у VirtualBox.

Ваша мета: Створити ізольовану мережу між двома віртуальними машинами.

Теоретична інформація:

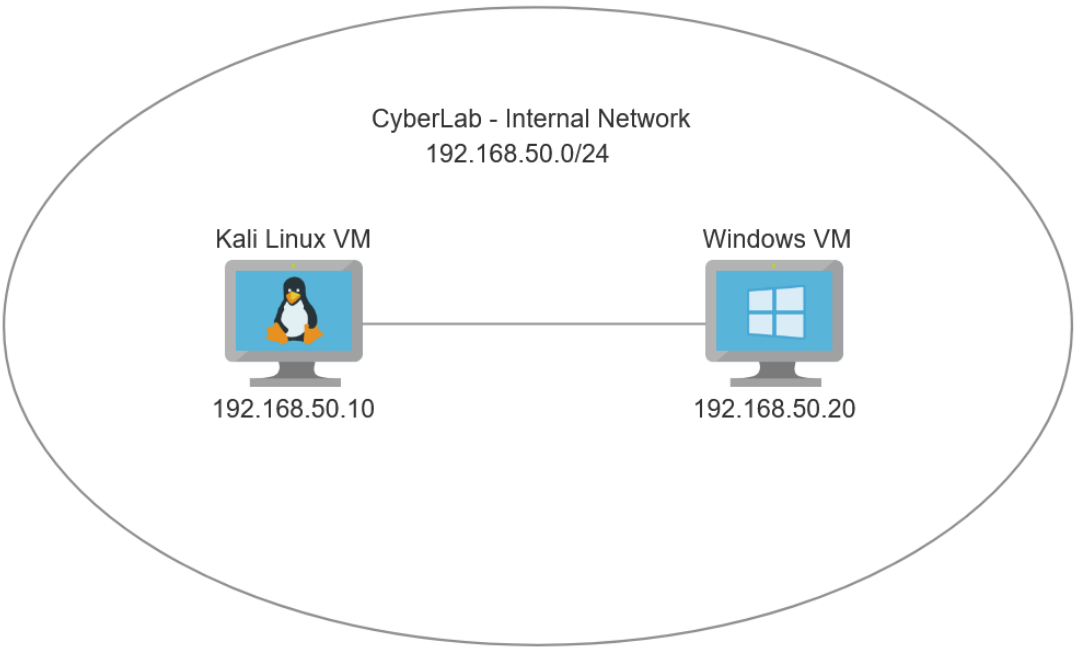
Внутрішня мережа (Internal Network) у VirtualBox дозволяє об'єднати декілька віртуальних машин в окрему мережу.

У цьому завданні буде використовуватися мережа:

Мережа: 192.168.50.0/24

Маска: 255.255.255.0

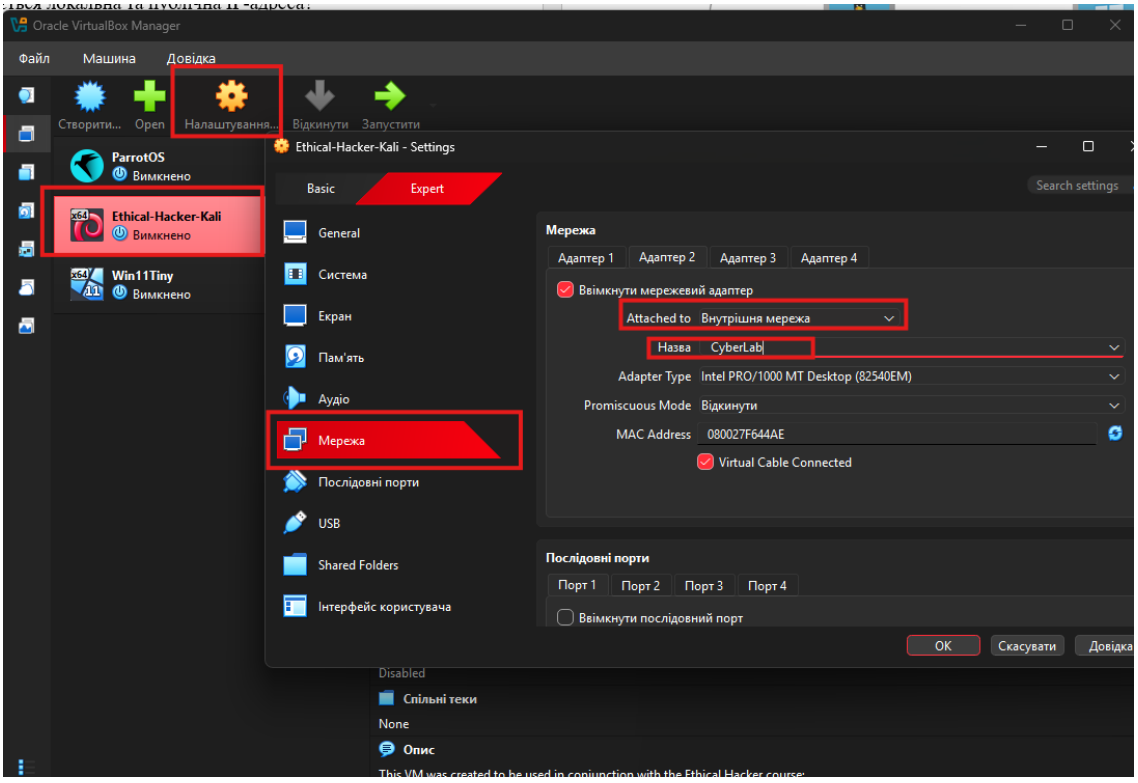
Загальна структура мережі:



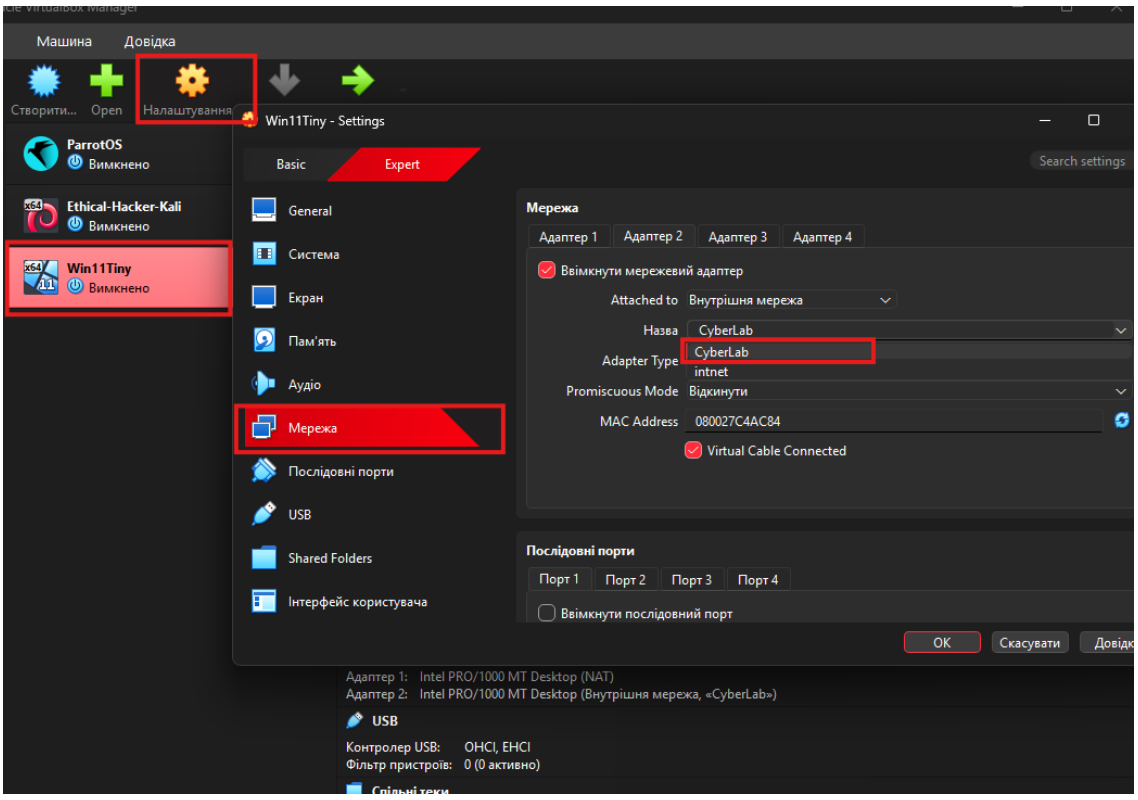
Завдання:

1. Для Адаптера №2 (Kali Linux) створити внутрішню мережу VirtualBox з назвою:

CyberLab



2. Для Адаптера №2 (Windows) обрати внутрішню мережу VirtualBox з назвою CyberLab:



3. Налаштувати статичні IP-адреси:

- Kali:

ip a – визначити назву мережного інтерфейсу

Отримати dhcp адресу на першому інтерфейсі:

sudo dhclient eth0

sudo ip link set <інтерфейс> up – увімкнення інтерфейсу

sudo ip addr add 192.168.50.10/24 dev <інтерфейс> – призначення IP-адреси

ip a – перевірка налаштувань

- Windows:

IP-адреса: 192.168.50.20

Маска: 255.255.255.0

Шлюз: не вказувати

DNS-сервер: не вказувати

4. Перевірити доступність вузлів (зв'язок між хостами):

- Kali (термінал):

ping 192.168.50.20

Ctrl+C для зупинки команди ping

- Widnows (cmd):

ping 192.168.50.10

Питання для обговорення:

1. Що таке внутрішня мережа (Internal Network) у VirtualBox?
2. Чому обидві машини можуть обмінюватися пакетами?
3. Яке призначення команди ping?

Завдання №4. Дослідження ARP-таблиці (IP → MAC відповідність).

Ваша мета: Зрозуміти, як у локальній мережі IP-адреси пов'язуються з MAC-адресами:

Команди для виконання завдання:

ping

arp -a – вивід ARP-таблиці

Завдання:

1. Виконати ping з ВМ Kali Linux до ВМ Windows:
2. Перевірити ARP-таблицю
3. Знайти відповідність: IP-адреса → MAC-адреса

Питання для обговорення:

1. Для чого використовується ARP у локальній мережі?
2. Чому без ARP неможливий обмін у LAN?

Завдання №5. Перевірка маршруту до вузла.

Ваша мета: Ознайомитися з тим, як пакети проходять через мережу.

Команди для виконання завдання:

traceroute 192.168.50.20

(або якщо немає traceroute)

tracepath 192.168.50.20

Завдання:

1. Виконати трасування з ВМ Kali Linux до ВМ Windows.
2. Визначити кількість “хопів”.
3. Пояснити отриманий результат.

Питання для обговорення:

1. Що таке hop?
2. Як traceroute допомагає в діагностиці мережі?

Завдання №6. Дослідження MAC-адрес.

Ваша мета: Ознайомитися з апаратними адресами мережних пристроїв.

Команди:

ip a

arp -a

Завдання:

1. Визначити MAC-адресу мережного інтерфейсу Kali Linux.
2. Визначити MAC-адресу мережного інтерфейсу Windows.
3. Порівняти отримані MAC-адреси з записами в ARP-таблиці.

Питання для обговорення:

1. Чому MAC-адреса потрібна навіть якщо вже існує IP-адреса?

Завдання №7. Аналіз ARP-трафіку у Wireshark.

Ваша мета: Побачити механізм ARP у реальній мережі.

Завдання:

1. Запустити Wireshark.

2. Встановити фільтр:

arp

3. Очистити ARP-кеш:

sudo ip neigh flush all

4. Виконати:

ping 192.168.50.20

5. Знайти:

- ARP Requst
- ARP Reply

6. Визначити:і

- Який вузол надсилав запит.
- Який вузол надсилав відповідь.
- Яку MAC-адресу було отримано.

Питання для обговорення:

1. Чому перед ping спочатку з’являються ARP-пакети?

Завдання №8. Фільтрація ICMP-трафіку у Wireshark.

Ваша мета: Навчитися виділяти потрібний трафік у мережевому аналізі.

Завдання:

1. На ВМ Kali Linux запустити Wireshark.
2. Використати фільтр:

icmp

3. Виконати команду:

ping 192.168.50.20

4. Знайти:
    - Echo Request
    - Echo Reply
5. Визначити:
    - IP джерела
    - IP призначення

Питання для обговорення:

1. Чому ICMP важливий у діагностиці мереж?

ПРАКТИЧНЕ ЗАНЯТТЯ №2

Завдання №1. Перехоплення HTTP-запитів.

Ваша мета: Проаналізувати реальний HTTP-трафік та зрозуміти структуру HTTP-запиту в мережі.

Контекст (CTF-підготовка):

HTTP є відкритим протоколом передачі даних. У CTF і пентесті він використовується для перехоплення запитів і відповідей, аналізу параметрів форм, виявлення переданих у відкритому вигляді даних (credentials, tokens).

Інструменти:

Wireshark

браузер

Завдання:

1. Запустити Wireshark.
2. Обрати активний мережний інтерфейс.
3. Відкрити веб-браузер та перейти за URL-адресою:

http://testasp.vulnweb.com/Register.asp?RetURL=%2FDefault%2Easp%3F

4. Запустити захоплення пакетів у Wireshark перед взаємодією з сайтом.
5. На сторінці реєстрації ввести тестові дані та натиснути “Register me”.
6. Зупинити захоплення пакетів у Wireshark.
7. Встановити фільтр HTTP:

http

8. Знайти та проаналізувати:

- HTTP-запити (GET/POST).
- User-Agent.
- URL запиту.
- Поле Host.

9. У HTTP-запиті знайти відкриті облікові дані, введені при реєстрації.

Питання для обговорення:

1. Які дані передаються у HTTP-запиті при відправці форми?
2. Чому HTTP не забезпечує конфіденційність?

Завдання №2. Порівняння HTTP та HTTPS у мережному трафіку.

Ваша мета: Зрозуміти принципову різницю між HTTP та HTTPS на рівні мережевого трафіку та навчитися визначати, які дані можна/не можна перехопити.

Інструменти:

Wireshark

браузер

Завдання:

1. Запустити захоплення трафіку у Wireshark.
2. У веб-браузері відкрити будь-який HTTPS-сайт, наприклад:

https://www.calculator.net/ip-subnet-calculator.html

3. Виконати будь-яку взаємодію з веб-сайтом.
4. Зупинити захоплення трафіку у Wireshark.
5. У Wireshark змінити фільтр:

tls

6. Дослідити зашифрований HTTPS-трафік.

Питання для обговорення:

1. Які дані можна побачити в HTTPS-трафіку?
2. Чому Wireshark не показує тіло HTTPS-запиту?

Завдання №3. Аналіз DNS-запитів у мережі.

Ваша мета: Навчитися аналізувати DNS-запити та розуміти механізм перетворення доменів у IP-адреси.

Інструменти:

Wireshark

ping

Завдання:

1. Відкрити Wireshark та обрати інтерфейс для захоплення трафіку.
2. Згенерувати трафік, шляхом виконання команди:

ping google.com

3. У Wireshark встановити фільтр:

dns

4. Проаналізувати DNS-пакети та знайти:

- DNS Query
- DNS Response
- Запитуваний домен
- IP-адресу у відповіді

Питання для обговорення:

1. Навіщо потрібен DNS?
2. Що відбувається під час DNS query?

Завдання №4. Перехоплення FTP-трафіку.

Ваша мета: Навчитися перехоплювати автентифікаційні дані, які передаються у відкритому вигляді за протоколом FTP.

Примітка:

Завдання виконується в межах розгорнутої вразливої машини Metasploitable2 всередині Kali Linux.

Команда для визначення IP-адреси контейнера Metasploitable2:

docker inspect -f '{{range.NetworkSettings.Networks}}{{.IPAddress}}{{end}}' metasploitable2

Завдання:

1. Запустити Wireshark на Kali Linux.
2. У списку інтерфейсів для захоплення обрати docker0 або any.
3. Відкрити новий термінал на Kali та підключитися до FTP-сервера:

ftp IP-address

Приклад: ftp 192.168.1.20

4. Для входу використати стандартні вразливі облікові дані Metasploitable:

Логін: msfadmin

Пароль: msfadmin

5. Після успішно входу ввести команду bye для виходу.
6. Зупинити захоплення у Wireshark та виставити фільтр *ftp*.
7. Знайти пакети, які містять команди USER та PASS

Питання для обговорення:

1. Чи вдалося побачити логін та пароль у відкритому форматі?

2. Чому передача даних через FTP є небезпечною в реальних мережах?

Завдання №5. Дослідження шифрованого трафіку SSH.

Ваша мета: Переконатися у перевагах шифрування, проаналізувавши трафік протоколу SSH у порівнянні з FTP.

Завдання:

1. Переконатися, що у Wireshark запущено нове захоплення трафіку на інтерфейсі docker0.

2. У терміналі Kali підключитися до контейнера, використовуючи SSH:

ssh msfadmin@IP-address

Пароль: msfadmin

Якщо з'явиться попередження про ключ безпеки, ввести yes, а потім пароль msfadmin.

3. Виконати кілька команд всередині SSH-сесії (наприклад, whoami, uname -a) та прописати exit.

4. У Wireshark зупинити захоплення трафіку та встановити фільтр *ssh*.

5. Знайти будь-який пакет із даними, натиснути правою кнопкою миші -> Follow -> TCP Stream.

6. Дослідити захоплений мережний пакет.

Питання для обговорення:

1. Чи можна розібрати введені в SSH-сесії команди (логін чи пароль)?

ПРАКТИЧНЕ ЗАНЯТТЯ №3

Ваша мета:

Навчитися виявляти активні хости в мережі, визначати відкриті порти та сервіси, а також проводити базову мережеву розвідку в ізольованому середовищі.

Контекст (CTF-підготовка):

У CTF і пентесті першим етапом є reconnaissance (розвідка): визначення активних вузлів, відкритих портів та сервісів. Це основа для подальших атак і аналізу.

Інструменти:

nmap

Завдання №1. Визначення активних хостів у локальній мережі.

Ваша мета: Знайти всі активні пристрої у локальній мережі.

Команда для виконання завдання:

nmap -sn 192.168.50.0/24, де:

-sn – режим без сканування портів (тільки визначення хостів)

Завдання:

1. Виконати сканування мережі 192.168.50.0/24.
2. Знайти всі активні хости.
3. Визначити IP-адресу ВМ Windows.
4. Визначити Docker-інтерфейс та IP на ВМ Kali Linux:

ip a

5. Виконати сканування Docker-мережі:

nmap -sn docker_subnet

Приклад:

nmap -sn 172.17.0.0/16

Питання для обговорення:

1. Чим відрізняється host discovery від port scanning?

Завдання №2. Сканування одного хоста (port scanning).

Ваша мета: Виявити відкриті порти на цільовій системі.

Контекст (CTF-підготовка): Відкриті порти = потенційні точки входу в систему.

Команда для визначення IP-адреси контейнера Metasploitable2:

docker inspect -f '{{range.NetworkSettings.Networks}}{{.IPAddress}}{{end}}' metasploitable2

Команди:

nmap IP-address – базове сканування хоста.

nmap -sS IP-address, де

-sS – TCP SYN Scan (безшумне напіввідкрите сканування)

Завдання:

1. Виконати базове сканування хоста Metasploitable2.
2. Виконати SYN-сканування хоста Metasploitable2.
3. Порівняти результати обох сканів.
4. Визначити відкриті порти в межах ВМ Metasploitable2.

Питання для обговорення:

1. Чому SYN scan швидший і менш “шумний”?
2. Що означає “open port” у контексті атаки?

Завдання №3. Сканування сервісів та визначення версій.

Ваша мета: Отримати інформацію про сервіси та їх версії.

Команди:

nmap -sV IP-address

nmap -sV -sC IP-address, де:

-sv – визначення версій сервісів.

-sC – запуск стандартних NSE скриптів.

Завдання:

1. Просканувати Metasploitable2.
2. Визначити версії FTP, SSH, HTTP.
3. Зафіксувати:
   - Сервіс.
   - Версію.
   - Порт.

Питання для обговорення:

1. Навіщо потрібне визначення версій?

2. Чому стара версія сервісу = ризик?

Завдання №4. HTTP service enumeration.

Ваша мета: Проаналізувати веб-сервіси на цільовій машині (Metasploitable2), використовуючи nmap.

Команди:

nmap -p 80 --script http-title IP-address, де:

-p 80 – сканується тільки порт 80 (HTTP)

--script http-title – NSE-скрипт, який витягує HTML title сторінки з HTTP-відповіді (дозволяє швидко зрозуміти, що це за веб-сервіс).

nmap -p 80 --script http-enum IP-address, де:

--script http-enum – NSE-скрипт для перебору типових HTTP-ресурів. Шукає стандартні шляхи типу: /admin, /login, /backup, /phpMyAdmin тощо.

Завдання:

1. Визначити наявність HTTP сервера.
2. Отримати title сторінки.
3. Виконати перебір директорій в межах вебсайту:

nmap -p 80 --script http-enum IP-address

4. Визначити потенційні кінцеві точки (директорії) на основі результатів із п. 3.

Питання для обговорення:

1. Що таке directory enumeration?
2. Чому веб-сервер часто перша точка входу?

Завдання №5. Аналіз вразливих сервісів (CTF mapping).

Ваша мета: Навчитися визначати потенційні точки експлуатації.

Завдання:

1. На основі результатів nmap -sV:
   - Знайти 2-3 підозрілі сервіси.
2. Для кожного сервісу визначити:
   - Відомі CVE (використовуючи браузер та відкриті джерела).
3. Пояснити чому цей сервіс може бути небезпечним.

Питання для обговорення:

1. Що таке CVE?
2. Чому важливо знати версію сервісу?
3. Як Nmap допомагає на етапі розвідки?