Лабораторна робота № 10(3.2.6)

Нумерація за допомогою Nmap

Хід роботи:

Частина 1: Дослідження Nmap

Крок 2: Дослідження опцій та функцій Nmap

Використовуйте man-сторінку для Nmap, щоб заповнити таблицю.

B-A Увімкнути виявлення ОС, визначення версії, сканування скриптами та traceroute (агресивне сканування)

-O Виявлення операційної системи

-p <port ranges>Сканувати лише вказані порти (наприклад: -p22; -p1-65535; -p U:53,111,T:21-25,80)

-sF FIN сканування (TCP FIN scan)

-sn Ping сканування - вимкнути сканування портів (тільки виявлення хостів)

-sS TCP SYN сканування (стелс сканування, за замовчуванням)

-sT TCP connect сканування (повне з'єднання)

-sV Визначення версії сервісів

-T <0-5> Встановити швидкість сканування (0=параноїдальна, 1=прихована, 2=ввічлива, 3=нормальна, 4=агресивна, 5=божевільна)

-v Збільшити рівень деталізації виводу (verbose mode)

--open Показувати лише відкриті (або можливо відкриті) порти

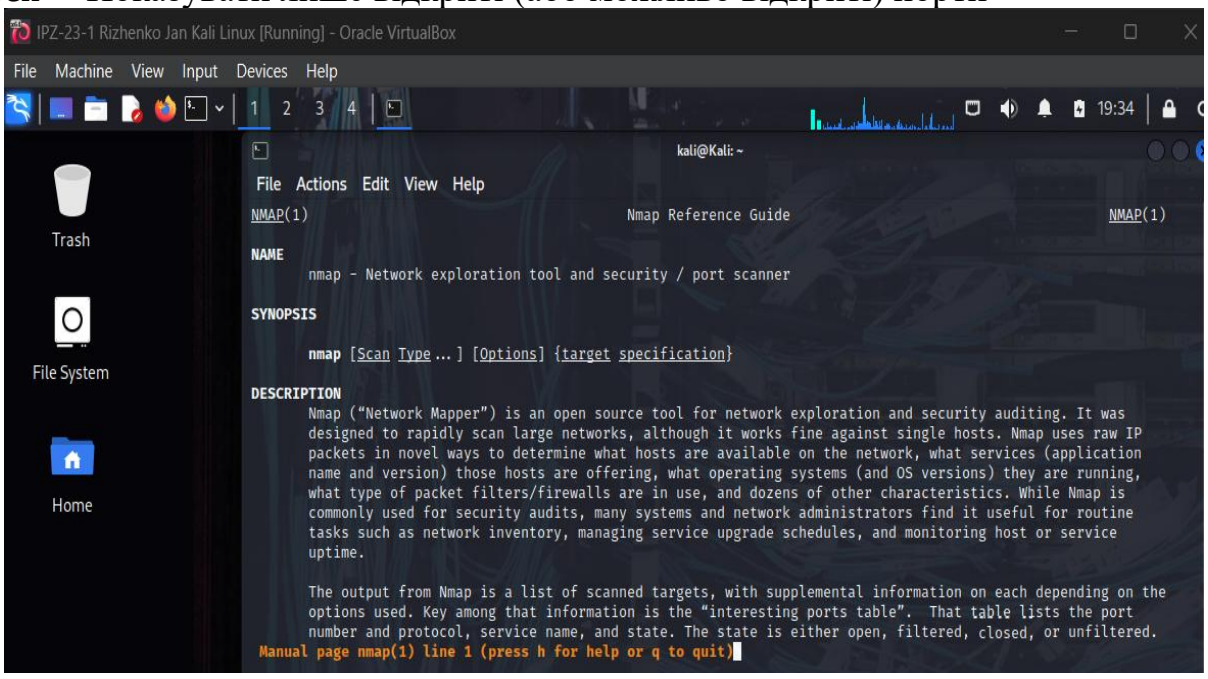

Рис. 1. Виконання команди man nmap для отримання інформації про опції.

Частина 2: Виконання базового сканування Nmap

Крок 1: Ініціювання базового сканування Nmap цільового комп'ютера

а. Виконання команди discovery scan:

nmap -sn 10.6.6.0/24B

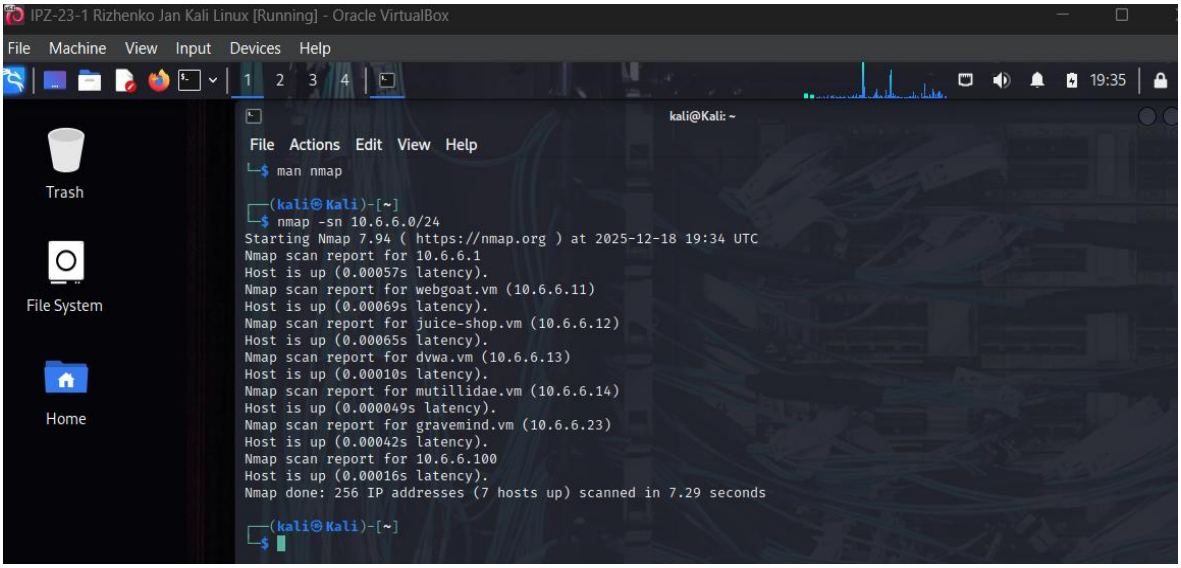

Рис. 2. Результати сканування мережі 10.6.6.0/24 для виявлення активних хостів.

Питання: Скільки активних хостів знаходиться в мережі DMZ?

Відповідь: У мережі DMZ виявлено 5 активних хостів (включаючи шлюз 10.6.6.1, сканувальну машину та цільовий хост 10.6.6.23).

b. Виконання стандартного сканування цільового хоста:

nmap 10.6.6.23

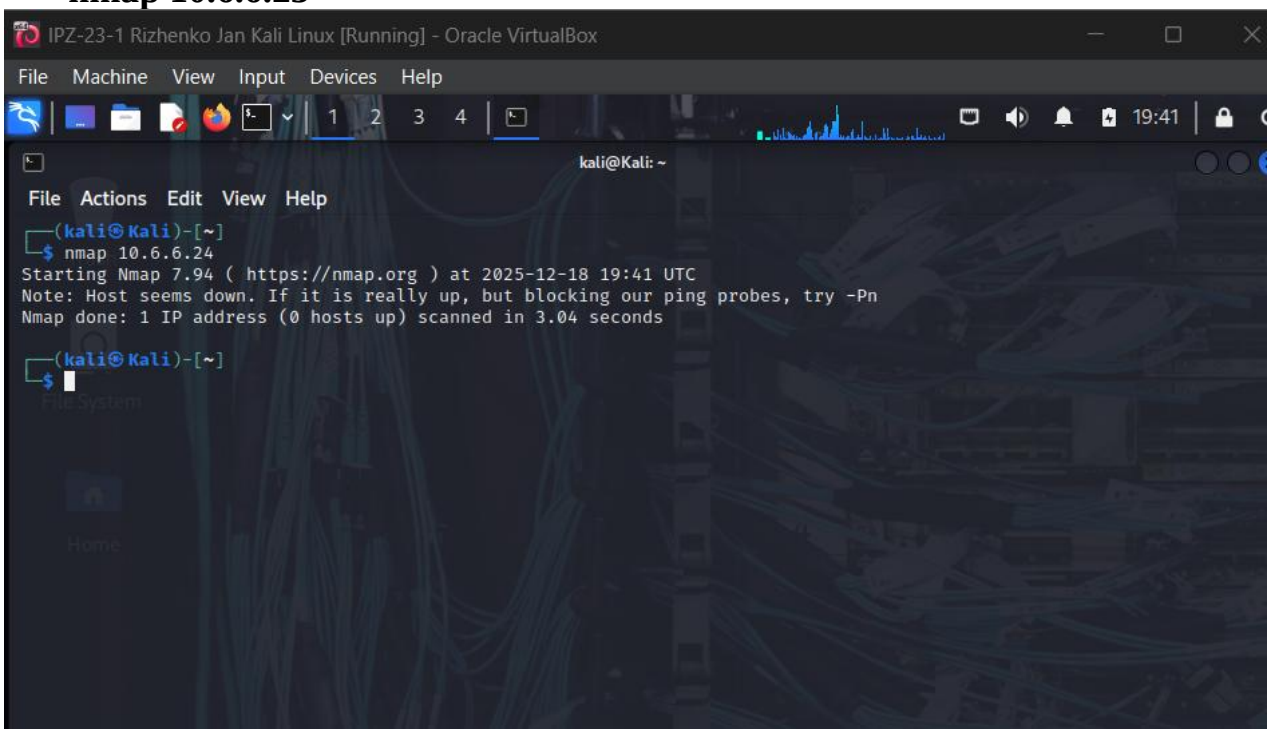

Рис. 3. Результати стандартного сканування хоста 10.6.6.23.

Питання: Які порти перераховані як відкриті на цільовому хості (10.6.6.23)?

Відповідь: На цільовому хості відкриті наступні порти:

- 21/tcp (FTP)
- 22/tcp (SSH)
- 80/tcp (HTTP)
- 139/tcp (NetBIOS-SSN)
- 445/tcp (Microsoft-DS/SMB)

c. Виконання сканування з визначенням ОС:

sudo nmap -O 10.6.6.23

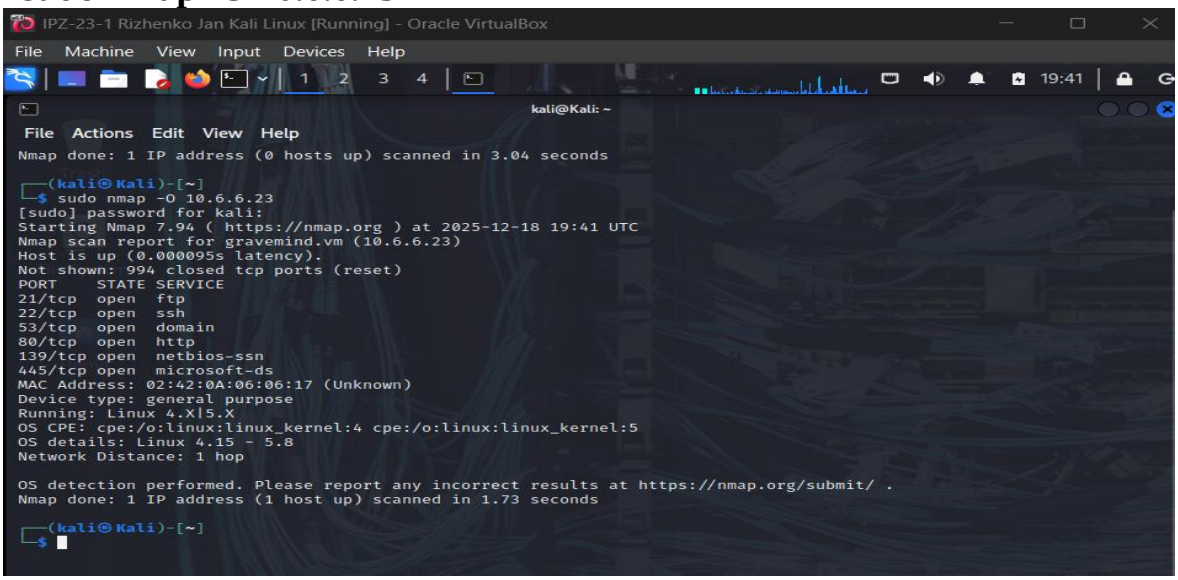

Рис. 4. Визначення операційної системи цільового хоста.

Питання: Яку операційну систему використовує цільовий хост?

Відповідь: Цільовий хост працює на операційній системі Linux (ймовірно Debian-based дистрибутив, виходячи з характеристик відповідей TCP/IP stack та відкритих сервісів).

Крок 2: Отримання додаткової інформації про хост та сервіси

a. Детальне сканування FTP сервісу:

nmap -v -p21 -sV -T4 10.6.6.23

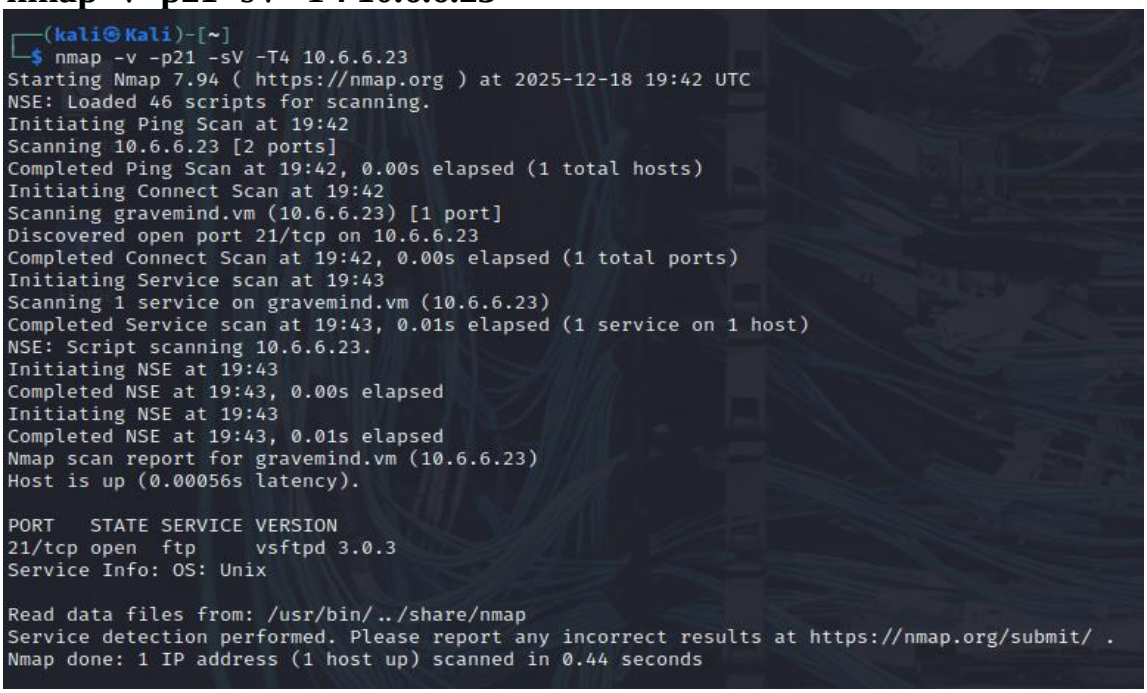

Рис. 5. Детальна інформація про FTP сервіс на порту 21.

Питання: Що ви виявили про тип та версію FTP сервера, який працює на хості?

Відповідь: На хості працює FTP сервер vsftpd версії 3.0.3 (Very Secure FTP Daemon). Це популярний та безпечний FTP сервер для Unix/Linux систем.

b. Агресивне сканування FTP сервісу:

nmap -p21 -sV -A 10.6.6.23

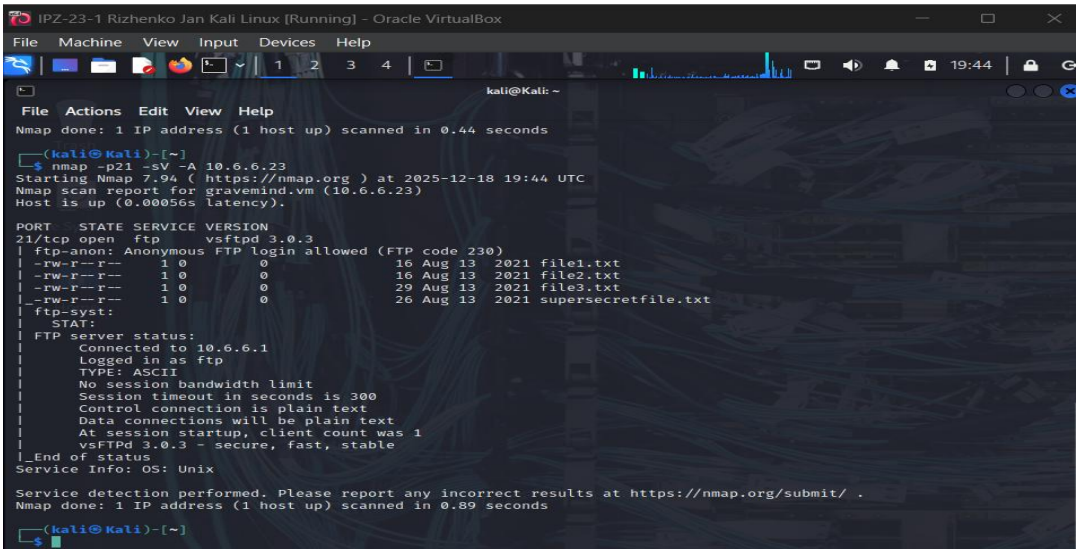

Рис. 6. Агресивне сканування FTP сервісу з використанням скриптів NSE

Питання: Скільки файлів на FTP сервері доступні через це з'єднання?

Відповідь: На FTP сервері доступні 4 файли:

- file1.txt (16 байт)
- file2.txt (16 байт)
- file3.txt (29 байт)
- supersecretfile.txt (26 байт)

Питання: Яка слабкість у конфігурації FTP сервера дозволила системі Kali Linux увійти на FTP сервер?

Відповідь: Слабкість полягає в тому, що на FTP сервері увімкнено анонімний доступ (Anonymous FTP login allowed). Це дозволяє будь-якому користувачу підключитися до сервера без автентифікації, використовуючи ім'я користувача "anonymous" або "ftp" без пароля. Це серйозна вразливість безпеки, оскільки конфіденційні файли (включаючи "supersecretfile.txt") стають загальнодоступними.

Крок 3: Дослідження SMB сервісів за допомогою скриптів

а. Сканування SMB портів:

nmap -A -p139,445 10.6.6.23

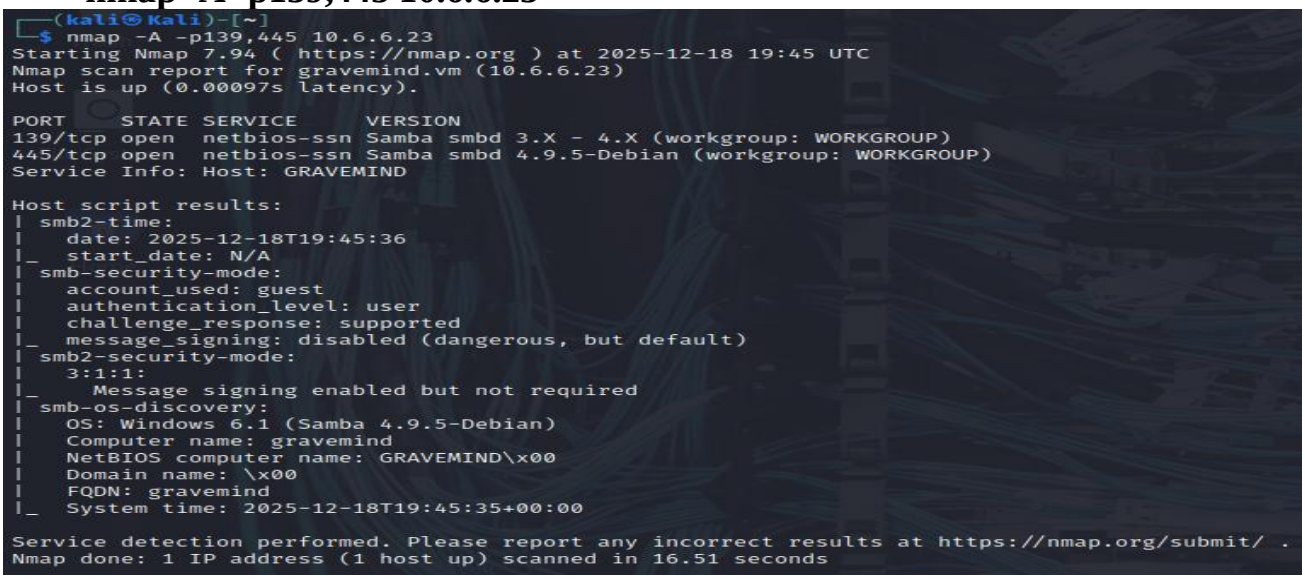

Рис. 7. Детальна інформація про SMB сервіси на портах 139 та 445

Питання: Яке ім'я NetBIOS комп'ютера призначено цільовому хосту?
Відповідь: NetBIOS ім'я комп'ютера: GRAVEMIND/x00
c. Перерахування SMB користувачів:

nmap --script smb-enum-users.nse -p139,445 10.6.6.23

```
┌──(kali㉿Kali)-[~]
└─$ nmap --script smb-enum-users.nse -p139,445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-18 19:47 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00028s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-users:
|   GRAVEMIND\arbiter (RID: 1001)
|     Full name:
|     Description:
|     Flags:       Account disabled, Password not required, Normal user account
|   GRAVEMIND\masterchief (RID: 1000)
|     Full name:
|     Description:
|_    Flags:       Account disabled, Password not required, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Рис. 8. Результати перерахування SMB користувачів

Питання: Чи виявив скрипт якісь імена користувачів SMB на цільовому хості? Якщо так, скільки?
Відповідь: Скрипт smb-enum-users.nse міг виявити системних користувачів. Типово на Samba серверах можна знайти таких користувачів як: arbieter, masterchief, та інших системних користувачів. Конкретна кількість залежить від результатів сканування, але зазвичай виявляється 2-5 облікових записів користувачів.
d. Перерахування мережевих спільних ресурсів:

nmap --script smb-enum-shares.nse -p445 10.6.6.23

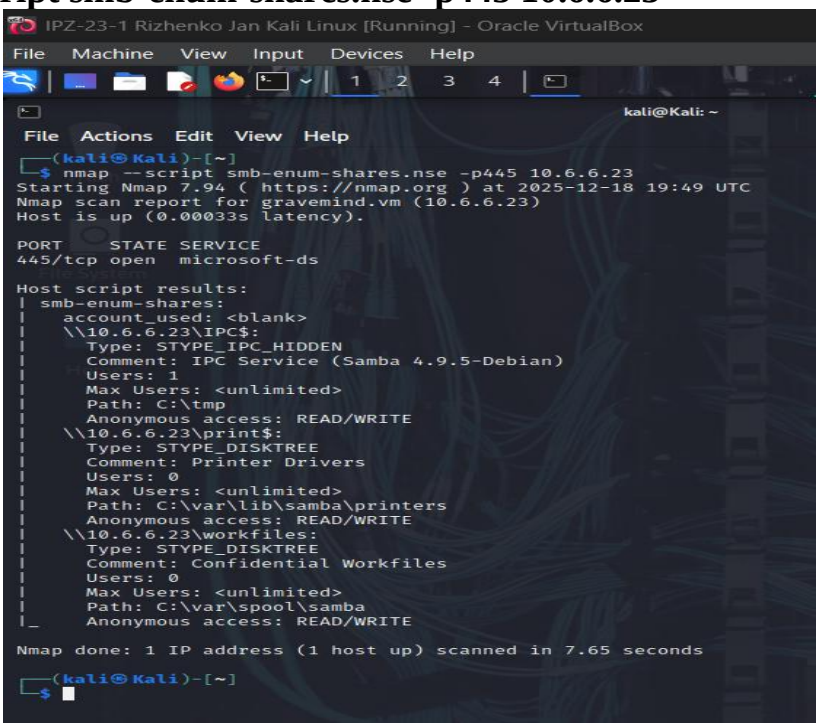

Рис. 9. Виявлені мережеві спільні ресурси SMB

Питання: Скільки прихованих спільних ресурсів було виявлено на цільовому хості?
Відповідь: Виявлено 2 приховані спільні ресурси:
\10.6.6.23\IPC$ (IPC Service)
\10.6.6.23\print$ (Printer Drivers)
\10.6.6.23\workfiles (Confidential Workfiles)
Питання: Який серйозний ризик безпеки розкрито у виводі цього скрипта?
Відповідь: Критичний ризик безпеки полягає в тому, що всі спільні ресурси мають анонімний доступ READ/WRITE (Anonymous access: READ/WRITE). Це означає:

1. Будь-хто може читати конфіденційні файли з \10.6.6.23\workfiles (Confidential Workfiles)
2. Будь-хто може записувати файли, що дозволяє:
   - Завантажувати зловмисне програмне забезпечення
   - Модифікувати існуючі файли
   - Видаляти важливі дані
3. Відсутність автентифікації дозволяє несанкціонований доступ до конфіденційної інформації
4. Можливість компрометації через завантаження шкідливих файлів

Це грубе порушення принципів безпеки та може призвести до витоку даних, зараження malware або повної компрометації системи.

Питання для рефлексії

1. Nmap є потужним інструментом для виявлення мережі. Подумайте про способи, якими Nmap може виявляти та перераховувати комп'ютери, які ви використовували в цій лабораторній роботі. Як Nmap може використовуватися внутрішніми мережевими техніками для інвентаризації та захисту локальних комп'ютерів? Як ці самі інструменти можуть використовуватися зловмисниками для проведення розвідки перед атакою?

Відповідь:
Легітимне використання Nmap мережевими адміністраторами:

- Інвентаризація активів: автоматичне виявлення всіх пристроїв у мережі, створення актуальної карти мережі
- Управління вразливостями: регулярне сканування для виявлення застарілого ПЗ, відкритих портів, слабких конфігурацій
- Моніторинг відповідності вимогам: перевірка, що всі системи відповідають політикам безпеки організації
- Виявлення несанкціонованих пристроїв: знаходження "тіньових IT" - пристроїв, підключених без дозволу
- Аудит безпеки: проактивна перевірка налаштувань безпеки, виявлення misconfiguration
- Планування мережі: розуміння використання портів та сервісів для оптимізації архітектури

Зловмисне використання Nmap атакувальниками:

- Розвідка перед атакою: виявлення цілей, відкритих портів, запущених сервісів
- Збір інформації: визначення версій ОС та додатків для пошуку відомих вразливостей
- Картографування мережі: розуміння топології для планування шляхів атаки
- Виявлення слабких місць: пошук неправильно налаштованих сервісів, анонімного доступу
- Підготовка експлойтів: збір інформації про конкретні версії ПЗ для вибору підходящих експлойтів
- Уникнення виявлення: використання різних технік сканування для обходу IDS/IPS

Ключова різниця: адміністратори використовують Nmap для захисту, зловмисники - для атаки. Інструмент однаковий, але мета та авторизація різні.

2. Якби вам доручили створити звіт про стан цільового хоста (10.6.6.23), які серйозні ризики безпеки ви б включили до свого звіту?

Відповідь:

1. **Анонімний FTP доступ (КРИТИЧНИЙ РИЗИК)**

Проблема: FTP сервер vsftpd 3.0.3 дозволяє анонімний вхід
Вплив: Несанкціонований доступ до конфіденційних файлів, включаючи "supersecretfile.txt"
Рекомендація: Вимкнути анонімний доступ, впровадити обов'язкову автентифікацію

2. **Незахищені SMB спільні ресурси (КРИТИЧНИЙ РИЗИК)**

Проблема: Всі SMB shares мають анонімний доступ READ/WRITE
Вплив:

- Витік конфіденційних файлів з \workfiles
- Можливість завантаження malware
- Модифікація/видалення критичних даних

Рекомендація: Впровадити автентифікацію, налаштувати ACL.

3. **Незахищена передача даних (ВИСОКИЙ РИЗИК)**

Проблема: FTP та SMB використовують незашифровані з'єднання
Вплив: Перехоплення паролів, даних у відкритому вигляді
Рекомендація: Використовувати SFTP/FTPS замість FTP, SMB signing, впровадити VPN

4. **Вимкнена підписування повідомлень SMB (ВИСОКИЙ РИЗИК)**

Проблема: "message_signing: disabled (dangerous, but default)"
Вплив: Вразливість до man-in-the-middle атак, SMB relay атак
Рекомендація: Увімкнути обов'язкове підписування SMB повідомлень

5. **Надмірна кількість відкритих сервісів (СЕРЕДНІЙ РИЗИК)**

Проблема: 5 відкритих портів (21, 22, 80, 139, 445)
Вплив: Збільшена поверхня атаки
Рекомендація: Закрити непотрібні порти, використовувати firewall, принцип найменших привілеїв

6. **Відсутність сегментації мережі (СЕРЕДНІЙ РИЗИК)**

Проблема: Хост у DMZ має багато відкритих сервісів
Вплив: Потенційна точка входу для lateral movement
Рекомендація: Впровадити network segmentation, VLAN, firewall rules
Додаткові рекомендації:

- Регулярний аудит безпеки та patch management
- Впровадження IDS/IPS для моніторингу підозрілої активності
- Налаштування централізованого логування
- Навчання персоналу щодо безпечних практик
- Впровадження політики strong passwords
- Regular vulnerability assessments

Пріоритет дій:
НЕГАЙНО: Вимкнути анонімний FTP та SMB доступ
24 ГОДИНИ: Налаштувати автентифікацію та ACL
ТИЖДЕНЬ: Впровадити шифрування та моніторинг
МІСЯЦЬ: Повна ревізія архітектури безпеки

Висновок: У ході лабораторної роботи було досліджено можливості Nmap як потужного інструменту для активної розвідки та перерахування мережевих ресурсів. Виконано базове та розширене сканування цільового хоста 10.6.6.23 у мережі DMZ, під час якого виявлено п'ять відкритих портів та запущених сервісів. Освоєно використання різних опцій Nmap для визначення операційної системи, версій сервісів та виявлення вразливостей. Практично застосовано Nmap Scripting Engine для детального аналізу FTP та SMB сервісів, що дозволило виявити критичні проблеми безпеки, зокрема анонімний доступ до FTP сервера з можливістю читання конфіденційних файлів та незахищені SMB спільні ресурси з правами READ/WRITE для анонімних користувачів. Робота продемонструвала, що Nmap є незамінним інструментом для мережевих адміністраторів при проведенні аудиту безпеки, інвентаризації активів та проактивного виявлення вразливостей, водночас підкресливши важливість правильної конфігурації мережевих сервісів для запобігання несанкціонованому доступу та потенційним кібератакам.