Лабораторна робота № 4(3.1.4)
Використання OSINT інструментів
Хід роботи:

Частина 1: Дослідження ресурсів OSINT

Крок 1: Доступ до OSINT Framework

Питання: Яка цінність проведення пошуку імен користувачів та перерахування облікових записів?

Відповідь:

Пошук імен користувачів та перерахування облікових записів має критичну цінність для тестування на проникнення та оцінки безпеки організації. По-перше, це дозволяє ідентифікувати облікові записи ключового персоналу організації на різних платформах та сервісах, що може виявити потенційні вектори атак через вразливі треті сторони. Оскільки користувачі часто використовують однакові імена та паролі на декількох сайтах, компрометація облікового запису на одному сервісі може призвести до доступу до корпоративних систем. По-друге, аналіз присутності персоналу на різних платформах надає цінну інформацію про їхні інтереси, зв'язки, звички та особисте життя, що може бути використано для створення цільових атак соціальної інженерії. По-третє, це допомагає виявити повторне використання паролів між сервісами, що є поширеною вразливістю. По-четверте, перерахування облікових записів дозволяє зібрати повний цифровий слід організації та її співробітників, включаючи забуті або неконтрольовані облікові записи. Нарешті, це допомагає знайти потенційні точки входу для подальших атак, включаючи витоки даних у публічних breach базах, що можуть містити скомпрометовані облікові дані.

Частина 2: Використання SpiderFoot

Крок 1: Запуск SpiderFoot

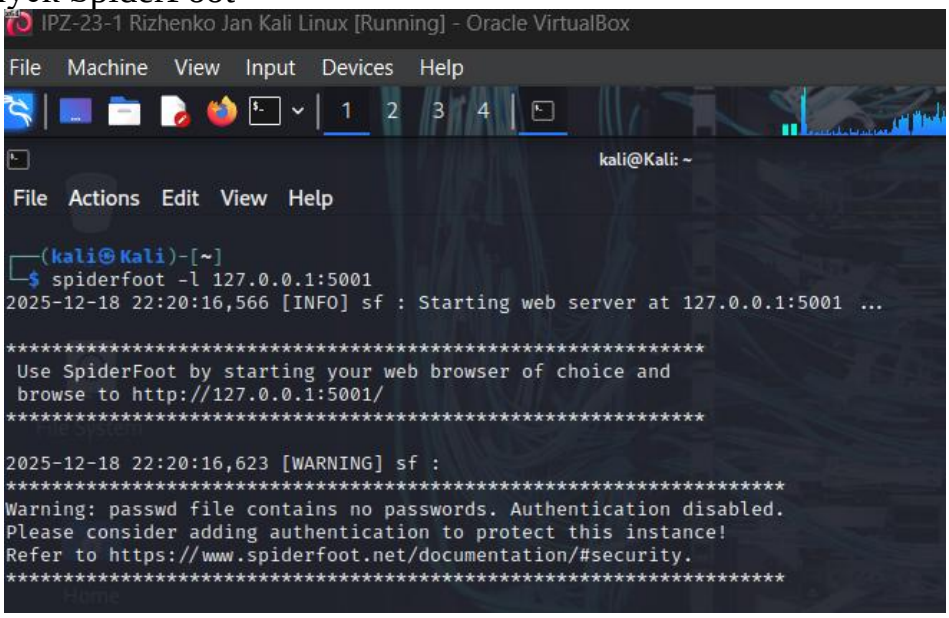

Рис. 1. Запуск SpiderFoot з прослуховуванням на порту 5001.

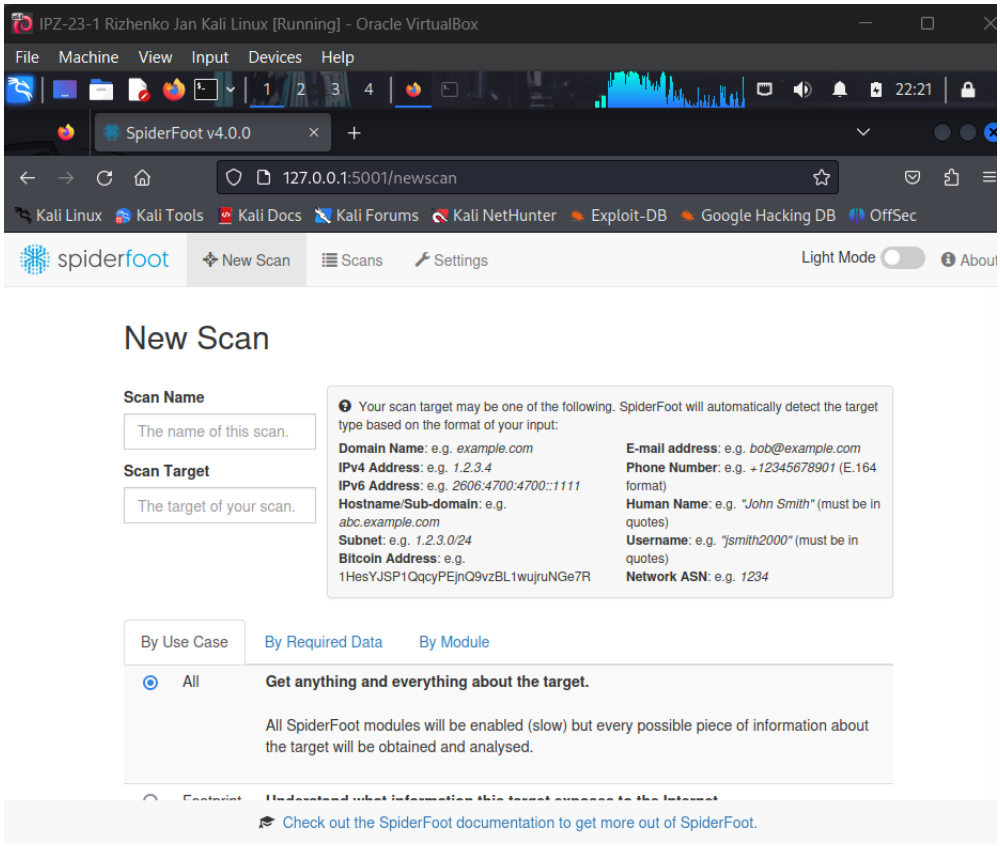

Рис. 2. Веб-інтерфейс SpiderFoot у браузері з головною сторінкою для створення нового сканування

Крок 2: Дослідження SpiderFoot

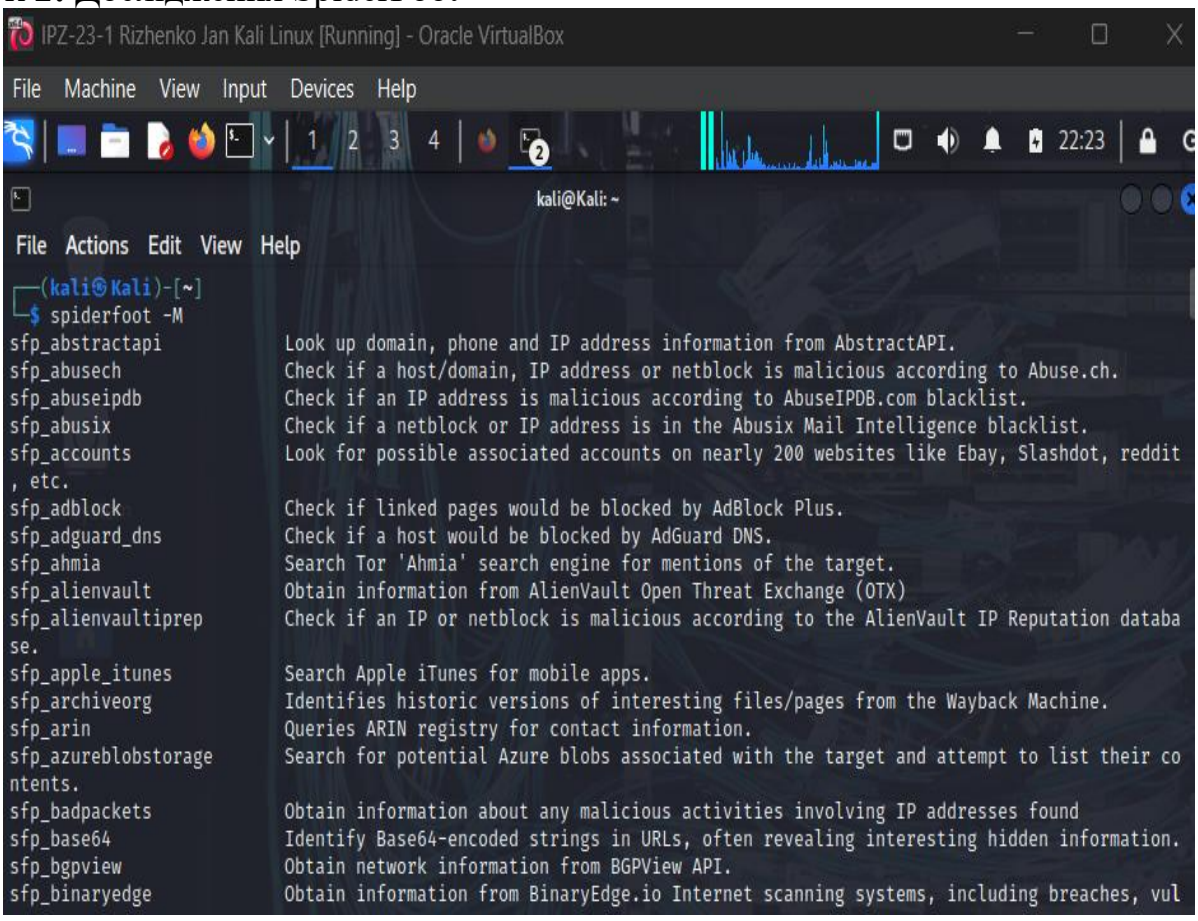

Рис. 3. Повний список модулів SpiderFoot у терміналі

Використання grep для фільтрації модулів:

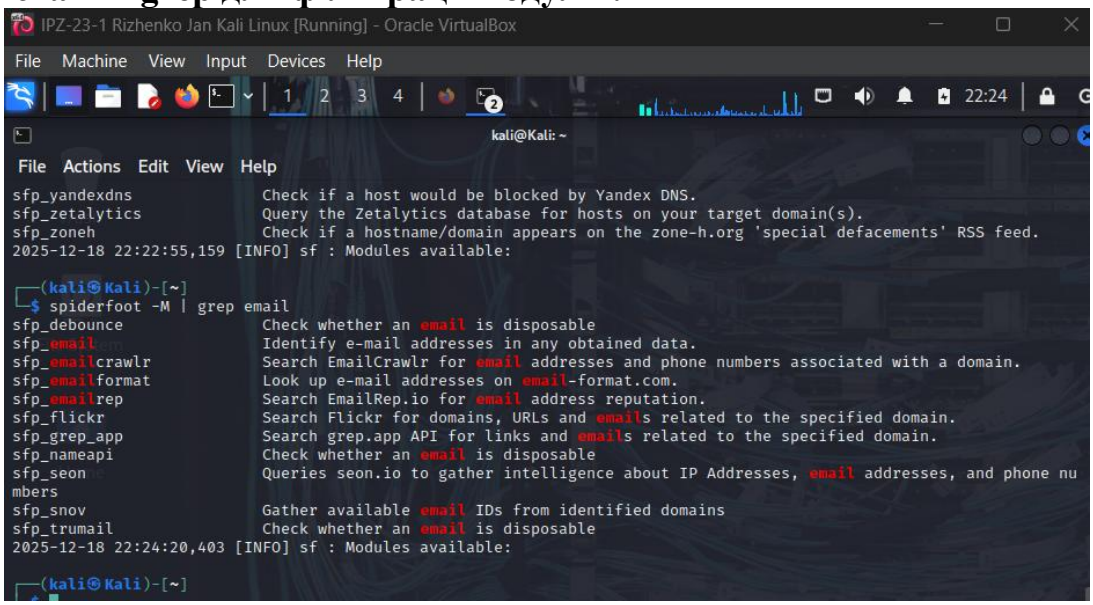

Рис. 4. Фільтрація модулів SpiderFoot для роботи з email адресами.

Пошук модулів для DNS:

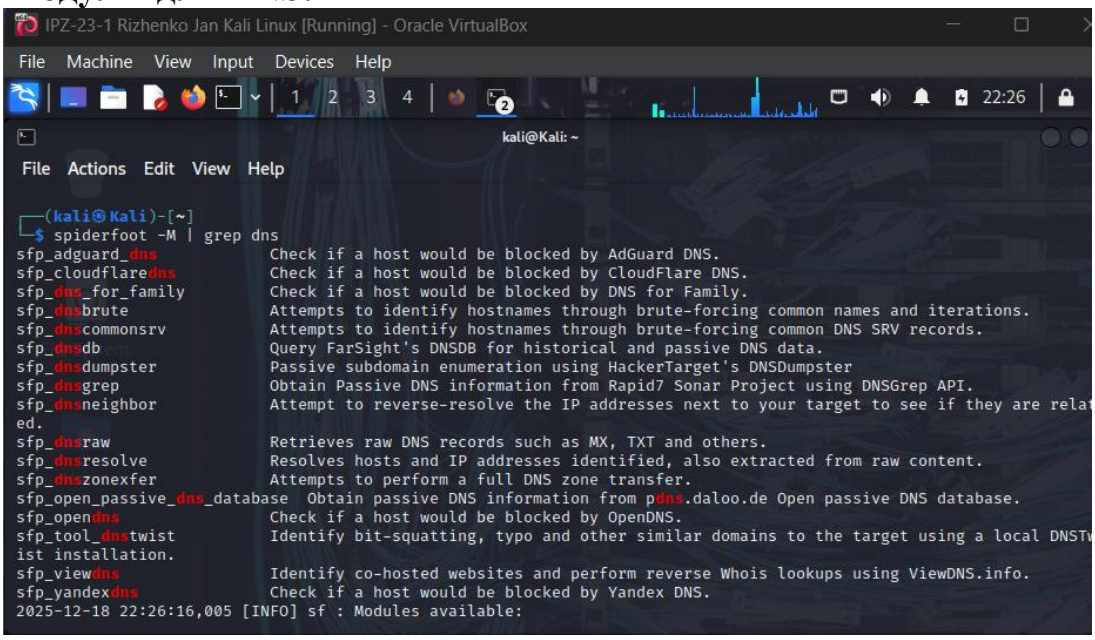

Рис. 5. Модулі SpiderFoot для DNS розвідки

Пошук модулів для витоків даних:

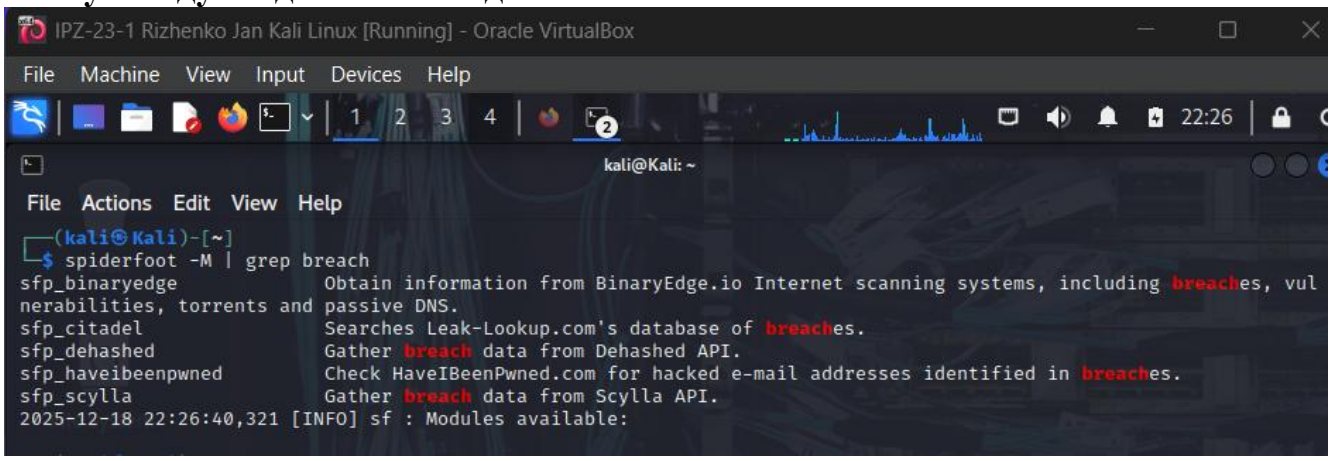

Рис. 6. Модулі SpiderFoot для перевірки витоків даних

Таблиця модулів SpiderFoot:

ТИП ІНФОРМАЦІЇ	НАЗВА СКАНЕРА/МОДУЛЯ	API КЛЮЧ ПОТРІБЕН? БЕЗКОШТОВНИЙ?	КОМЕНТАРІ
Можливі облікові записи, пов'язані з доменом	Account Finder, sfp_accounts	Hi, N/A	Понад 200 сайтів, таких як eBay, Reddit, Slashdot
Посилання, пов'язані з ціллю	Link Extractor, sfp_pageinfo	Hi, N/A	Витягує посилання зі сторінок
Email адреси, пов'язані з ціллю	Email Extractor, sfp_emailformat	Hi, N/A	Знаходить email адреси на веб-сторінках
Домени та URL, пов'язані з ціллю	Subdomain Finder, sfp_dnsbrute	Hi, N/A	Знаходить субдомени та пов'язані URL
Інформація про геолокацію	IP Geolocation, sfp_ipinfo	Hi, N/A (базова версія)	Визначає фізичне розташування IP адрес
Інформація про витоки даних	Have I Been Pwned, sfp_haveibeenpwned	Так, безкоштовний	Перевіряє наявність облікових записів у відомих витоках даних

Крок 3: Реєстрація API ключів (опціонально)

Таблиця API модулів:

Модуль	Тип інформації	API ключ
Builtwith	Технології, використані для створення веб-сайту	Реєстрація на builtwith.com
Hunter.io	Email адреси, пов'язані з доменом	Реєстрація на hunter.io
Onion.link	Доступ до .onion сайтів через clearnet	Не потрібен
IntelligenceX	Витоки даних, паролі, документи	Реєстрація на intelx.io

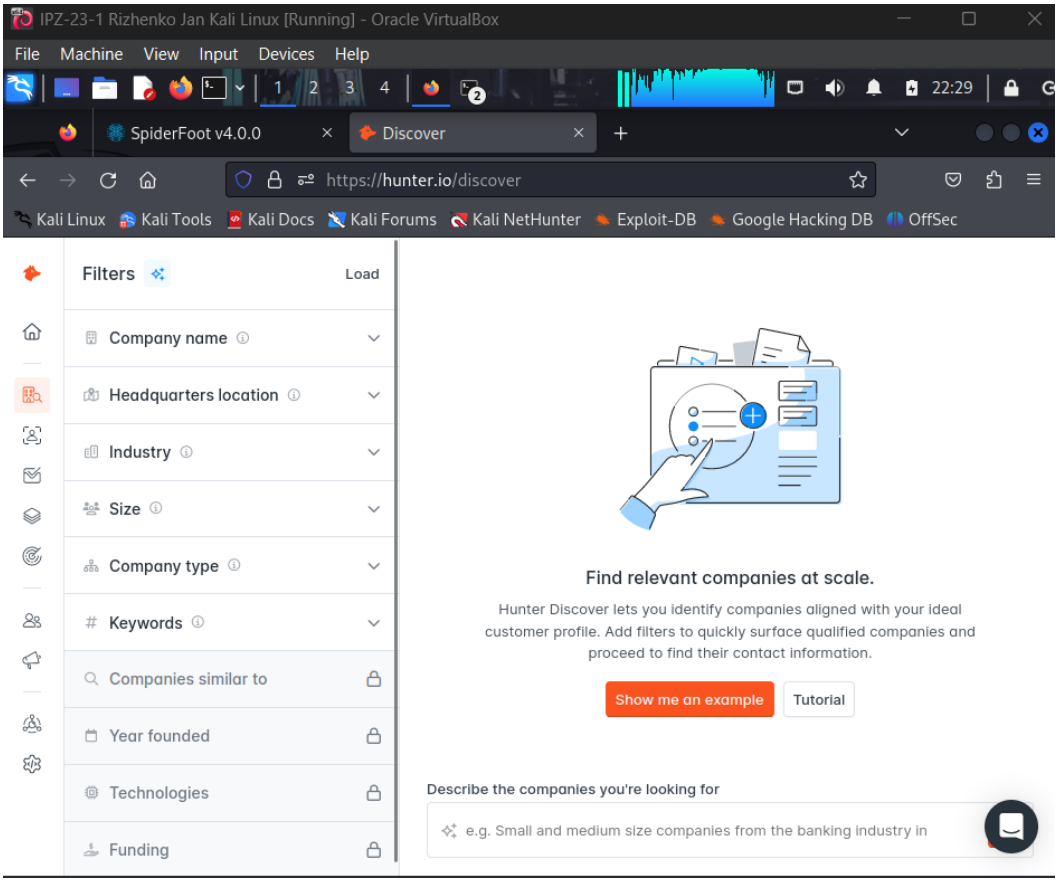

Рис. 7. Сайт Hunter.io

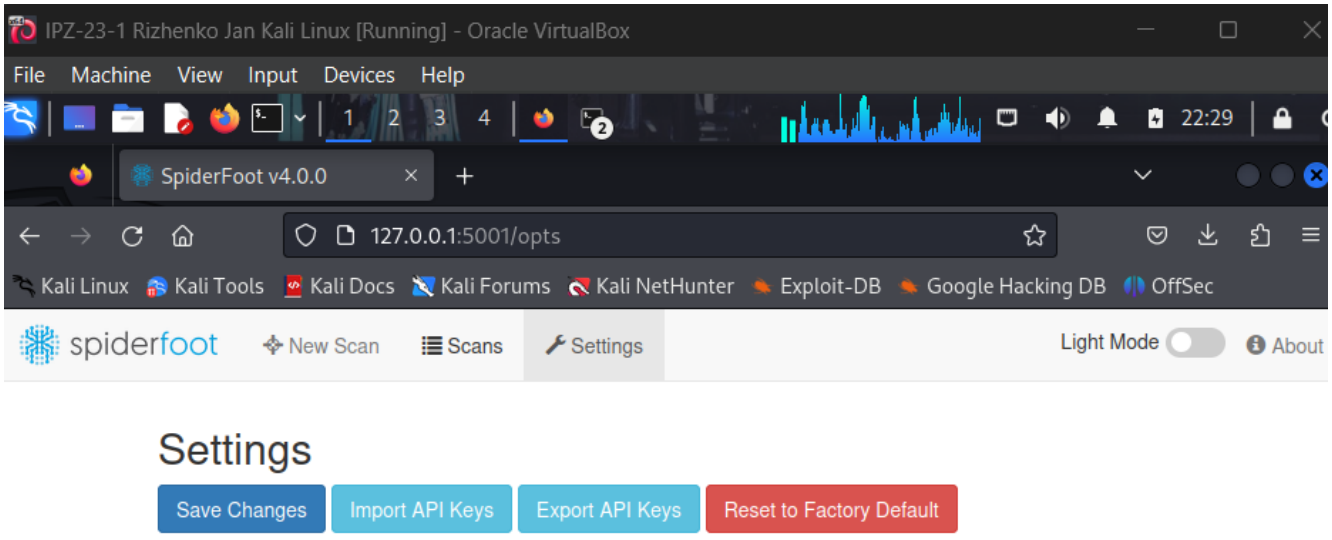

Рис. 8. Налаштування API ключів у веб-інтерфейсі SpiderFoot через Settings (кнопки Import та Export)

Крок 4: Аналіз результатів сканування з API модулями

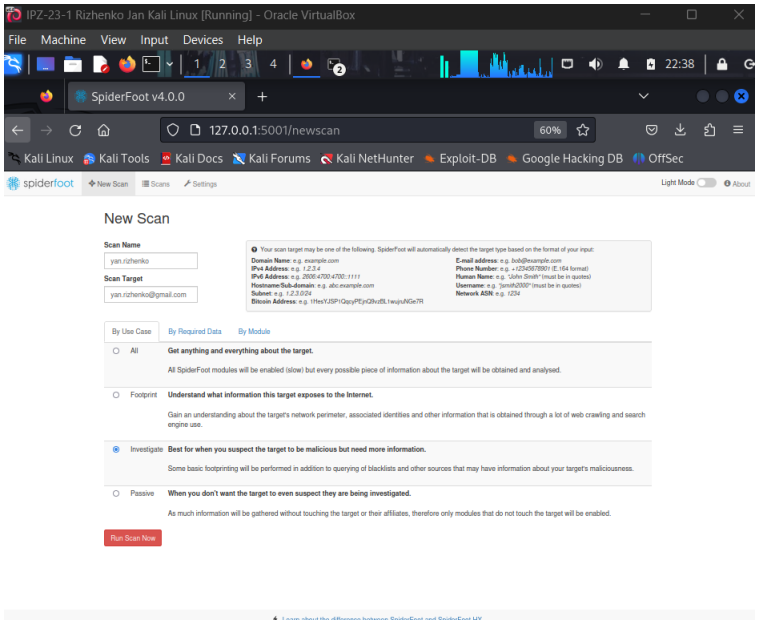

Рис. 9. Створення нового сканування у SpiderFoot з вказанням цільового домену

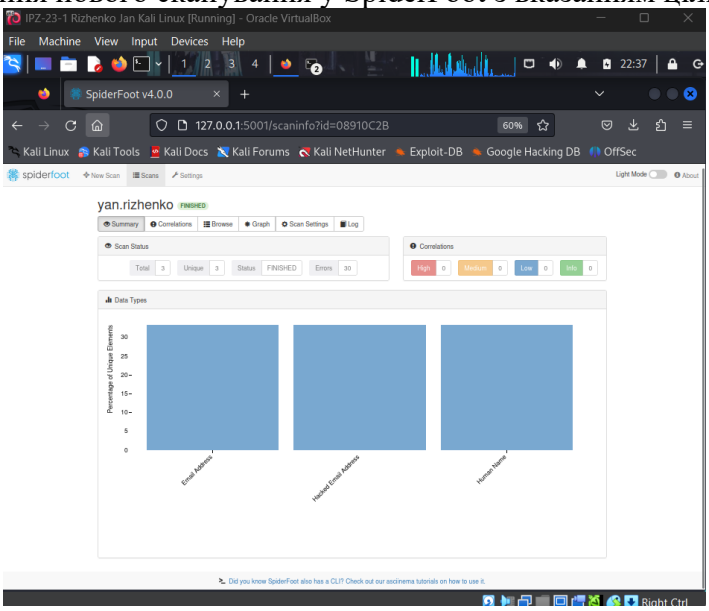

Рис. 10. Процес виконання сканування з відображенням активних модулів

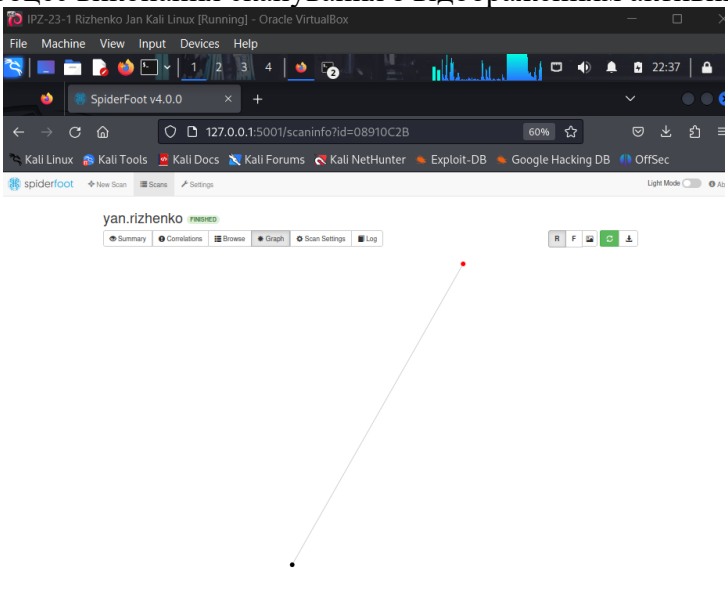

Рис. 11. Результати сканування у вигляді графа зв'язків між виявленими об'єктами

Питання: Який модуль сприяв таблиці Leak Site URL?
Відповідь:
Модуль **IntelligenceX** (sfp_intelx) або **Hunter.io** (sfp_hunter) зазвичай сприяє таблиці Leak Site URL, оскільки ці модулі спеціалізуються на пошуку витоків даних та скомпрометованих облікових записів.
Питання: Що ви бачите при відкритті записів у новій вкладці?
Відповідь:
При відкритті записів у новій вкладці можна побачити:

- Веб-сторінки з витоками даних або базами даних скомпрометованих облікових записів
- Інформацію про конкретні інциденти безпеки
- Деталі про знайдені email адреси, паролі або інші конфіденційні дані
- Посилання на форуми, пастебіни або інші джерела, де була опублікована скомпрометована інформація
- Можливі дати витоків та типи скомпрометованих даних

У моєму випадку виводяться лише ті дані, що я ввів для пошуку, жодного витоку зі сторонніх сайтів.
Частина 3: Дослідження Recon-ng
Крок 1: Створення робочого простору

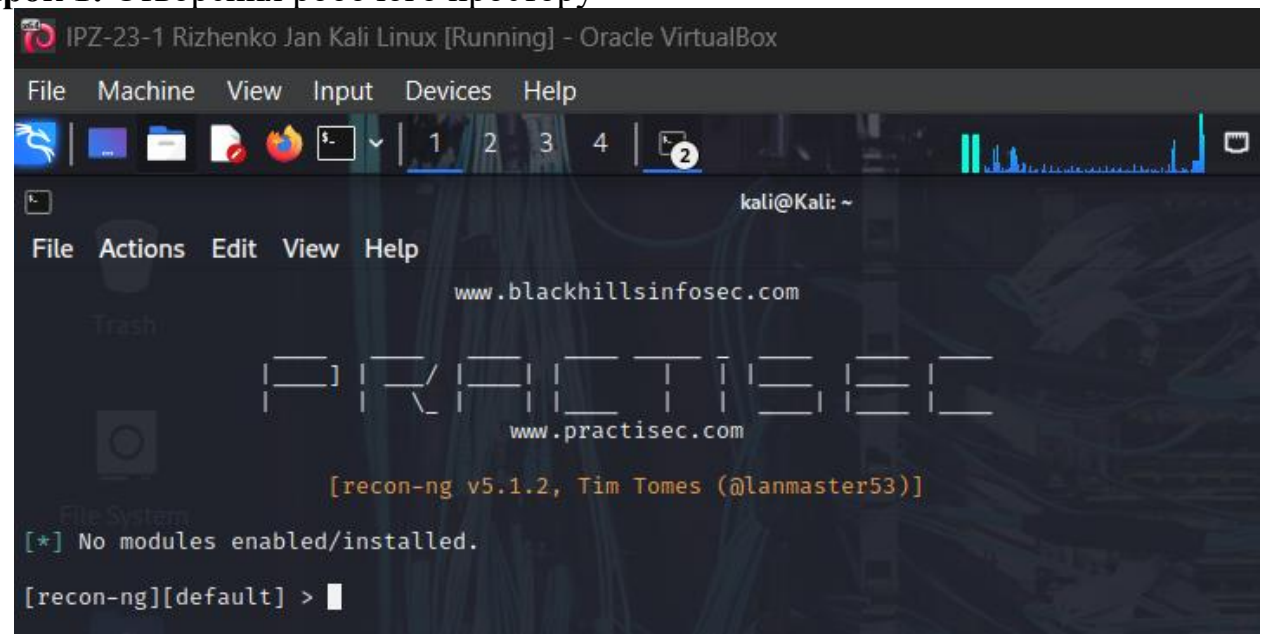

Рис. 12. Запуск Recon-ng з відображенням банера та версії

Команди для роботи з workspaces:

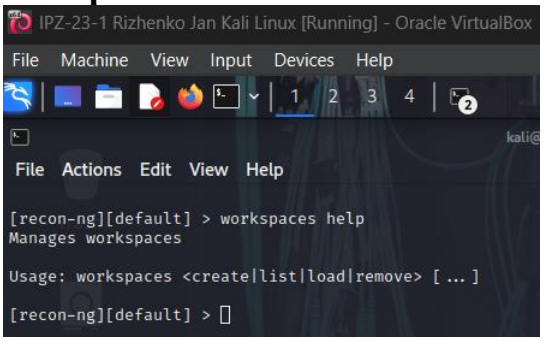

Рис. 13. Вивід довідки по командах workspaces

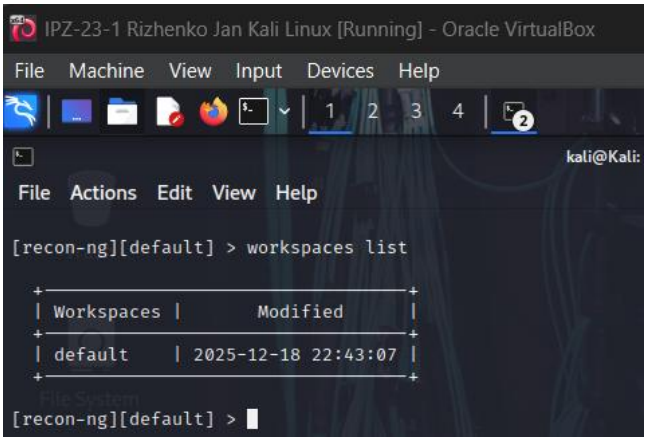

Рис. 14. Список доступних робочих просторів у Recon-ng

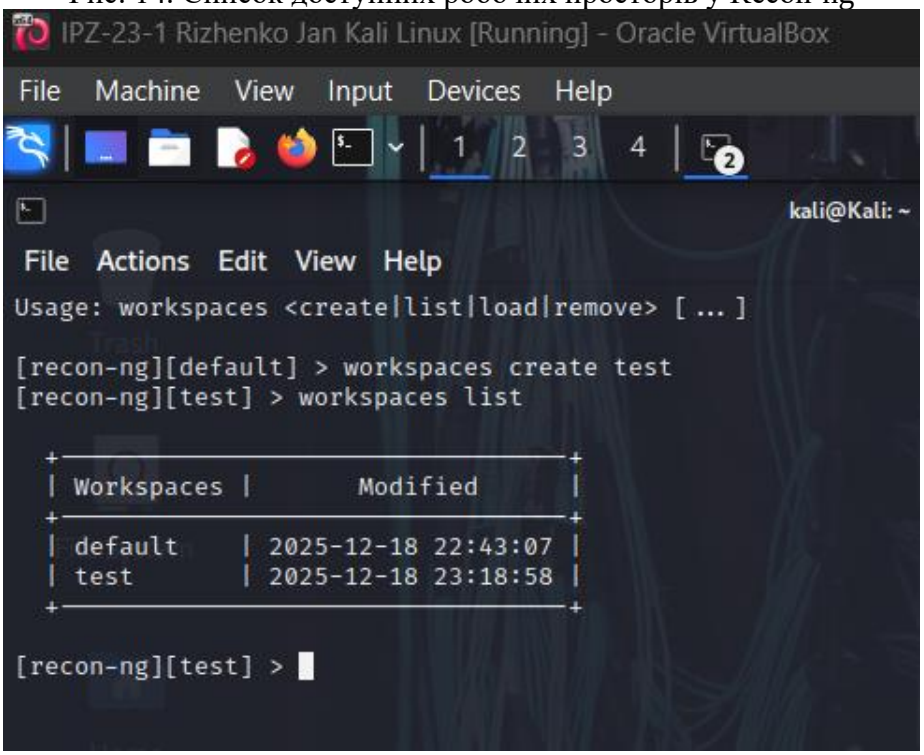

Рис. 15. Створення нового робочого простору з назвою "test"

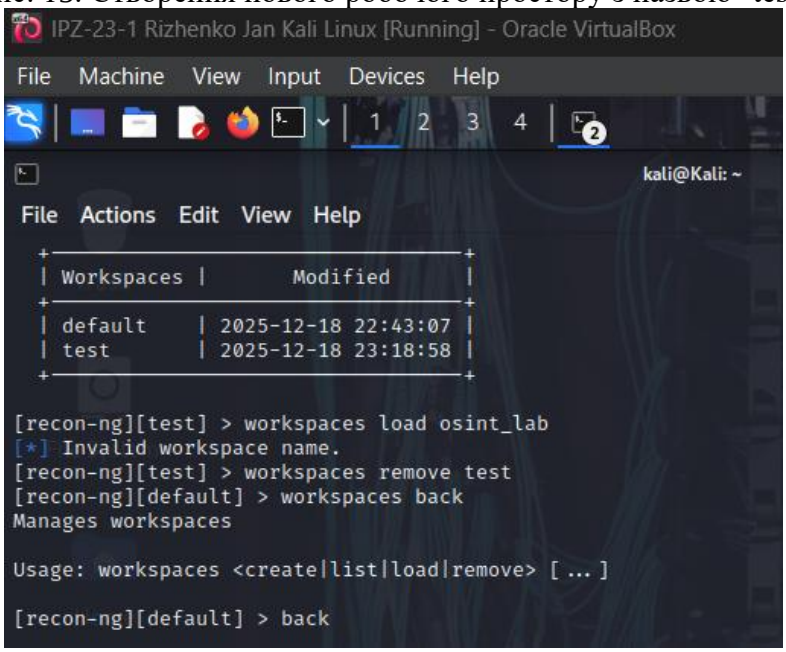

Рис. 16. Навігація між різними робочими просторами та вихід.

Питання: Як можна відобразити доступні робочі простори?
Відповідь:
Команда workspaces list відображає всі доступні робочі простори.
Питання: Як можна видалити робочий простір?
Відповідь:
Команда workspaces remove з вказанням назви робочого простору видаляє його повністю.
Питання: Яка команда вийде з робочого простору та поверне до головного Recon-ng prompt?
Відповідь:
Команда back повертає до головного prompt Recon-ng.
Крок 2: Дослідження модулів
Команда для перегляду встановлених модулів:

modules search

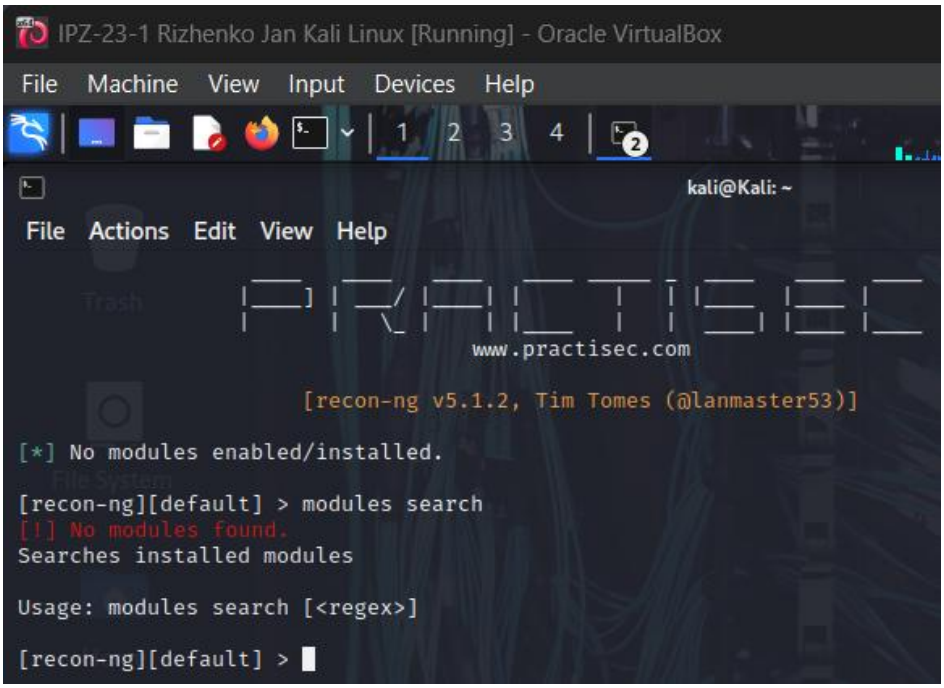

Рис. 17. Список встановлених модулів у Recon-ng (порожній для свіжої інсталяції)

Питання: Скільки модулів наразі доступні для вас?
Відповідь:
У “свіжій” Recon-ng версії 5.x або новішої за замовчуванням встановлено 0 модулів. Це відрізняється від попередніх версій, де модулі були попередньо встановлені. Тепер всі модулі повинні бути встановлені з marketplace. У marketplace доступно понад 90-100 модулів для встановлення, які охоплюють різні аспекти розвідки: збір субдоменів, email адрес, інформації про компанії, геолокації, перевірку витоків даних тощо. Модульна архітектура дозволяє встановлювати лише необхідні модулі, що зменшує розмір інсталяції та спрощує управління залежностями.
Крок 3: Дослідження marketplace модулів

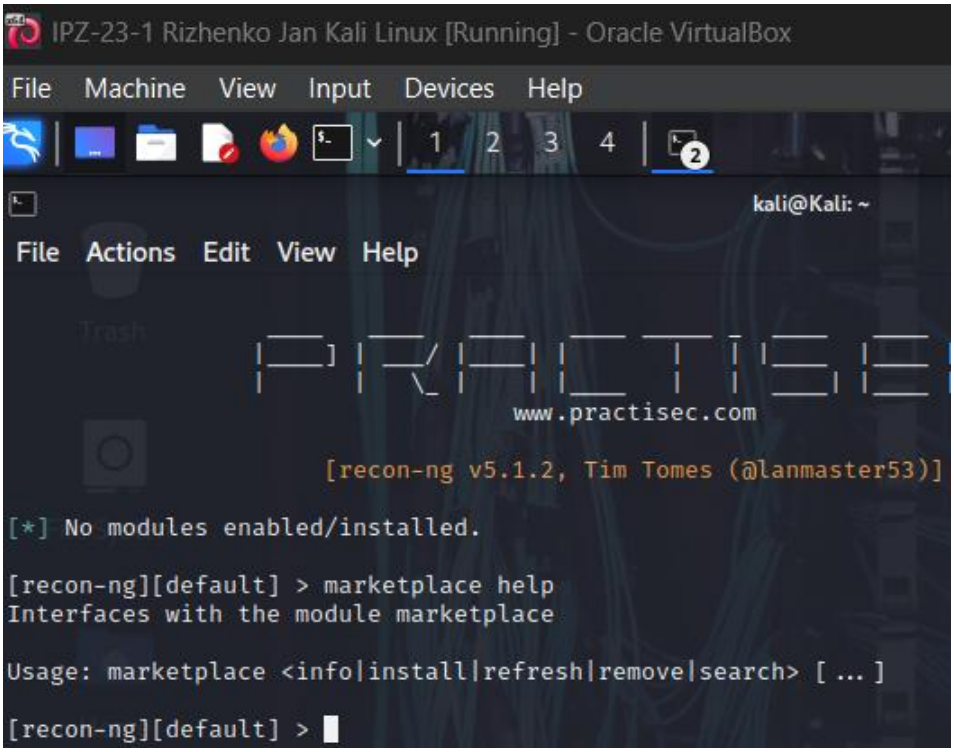

Рис. 18. Довідка по командах marketplace

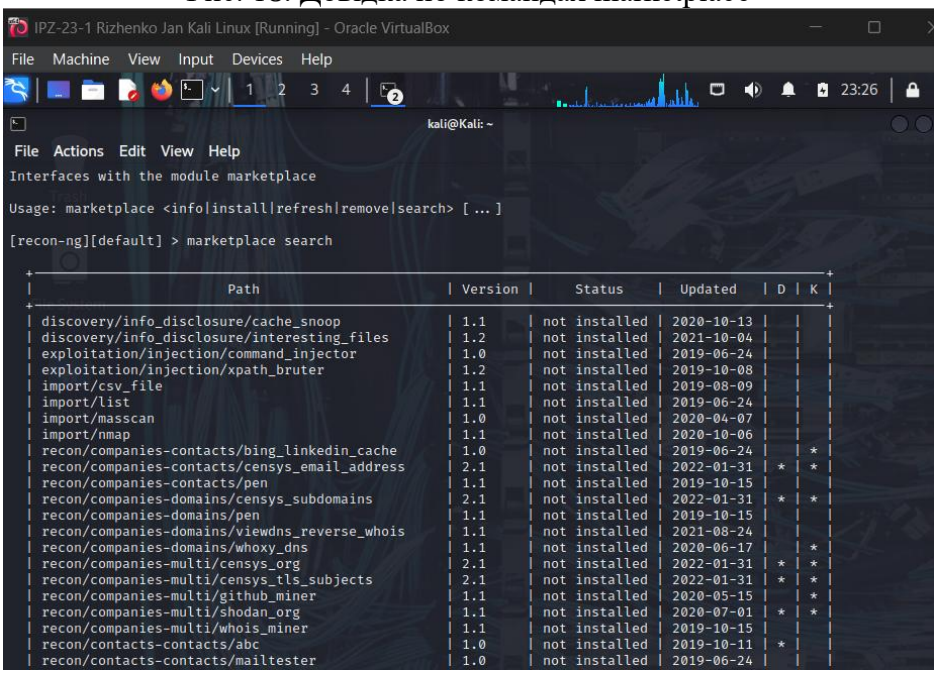

Рис. 19. Повний список модулів у marketplace з індикаторами залежностей (D) та API ключів (K)

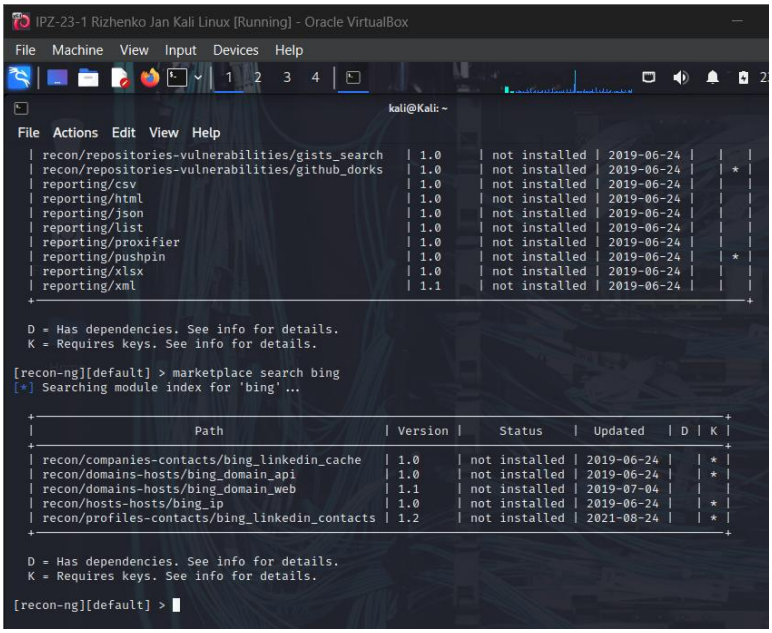

Рис. 20. Результати пошуку модулів за ключовим словом "bing"

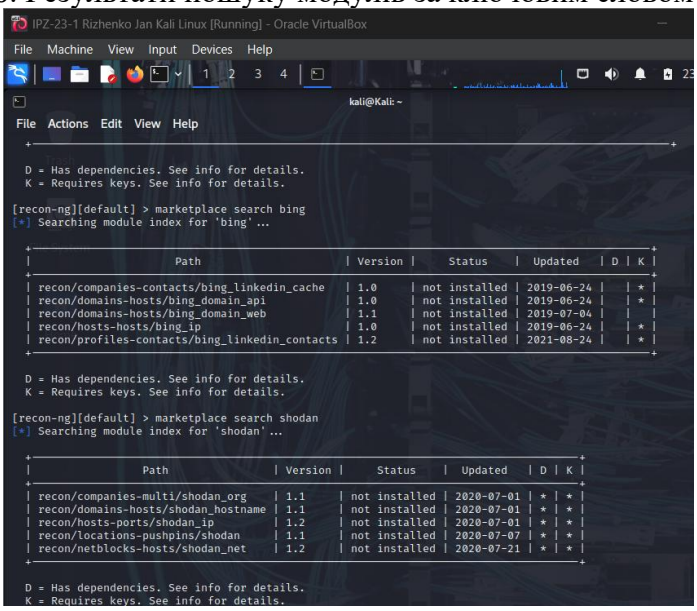

Рис. 21. Результати пошуку модулів за ключовим словом "shodan"

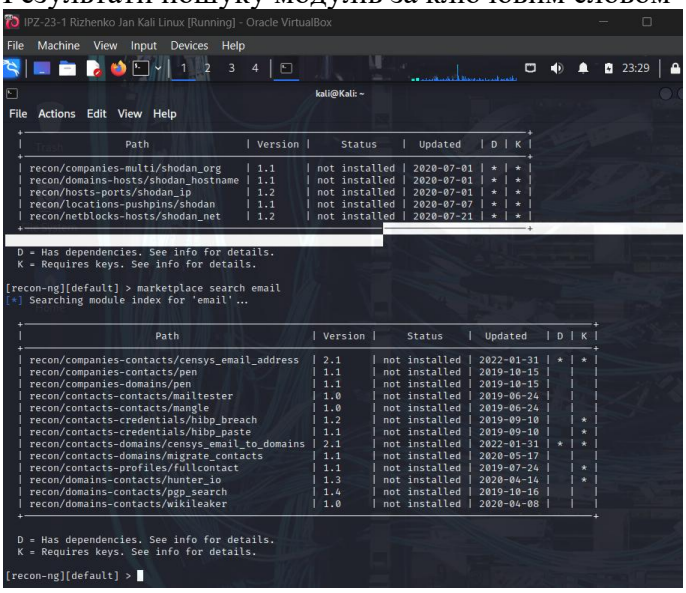

Рис. 22. Результати пошуку модулів за ключовим словом "email"

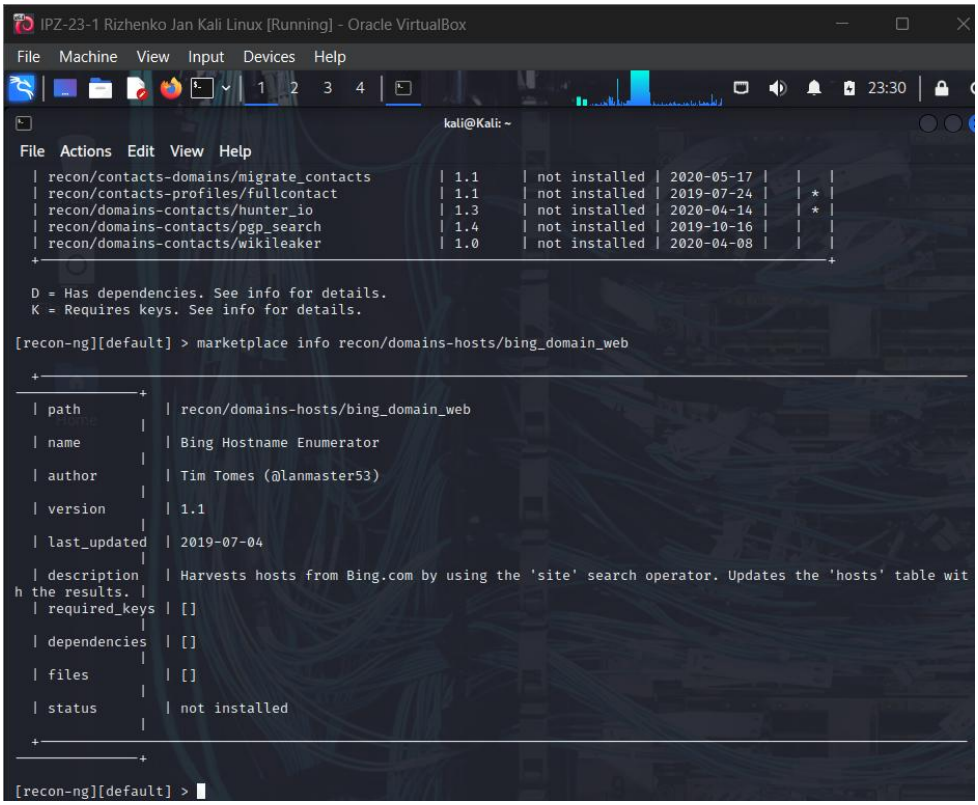

Рис. 23. Детальна інформація про модуль bing_domain_web

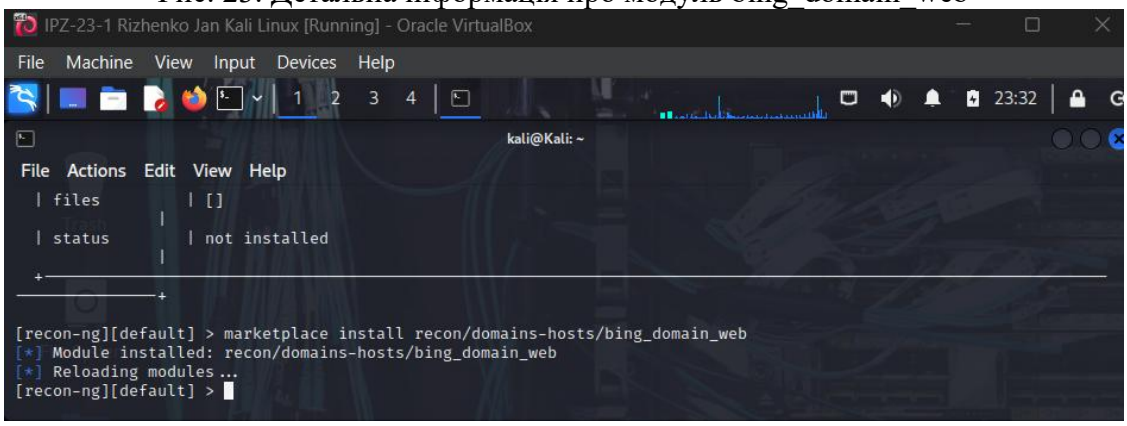

Рис. 24. Процес встановлення модуля з marketplace

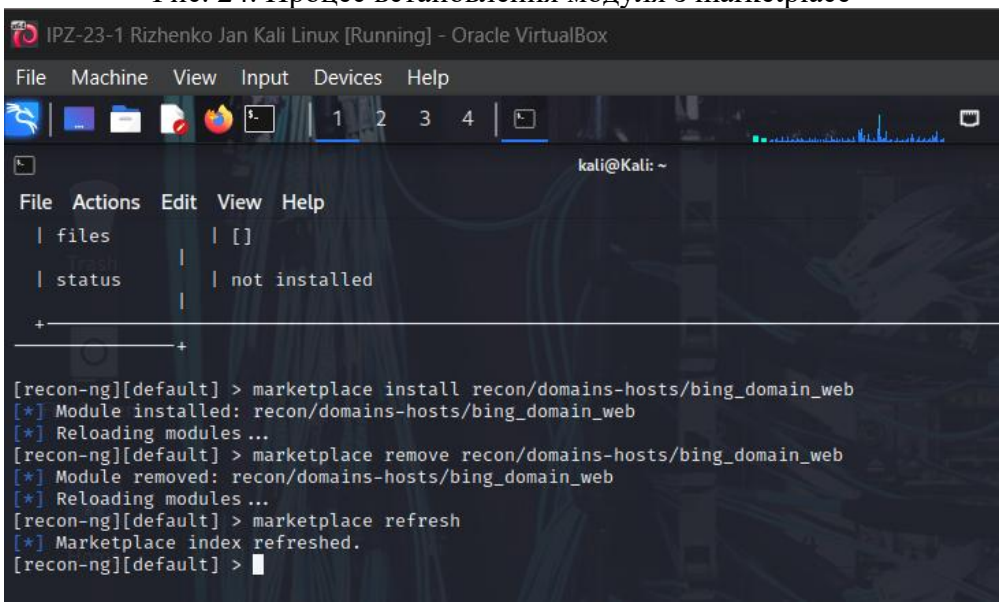

Рис. 25. Видалення модуля з marketplace та оновлення всіх модулів.

Питання: Модульні таблиці мають колонки для D та K. Знайдіть shodan модулі. Які вимоги до цих модулів?
Відповідь:
При пошуку shodan модулів за допомогою команди marketplace search shodan(Рис.21) відображаються колонки з позначками D (Dependencies) та K (Keys).
D (Dependencies) позначає, що модуль має зовнішні залежності, зазвичай Python бібліотеки. Якщо в цій колонці стоїть зірочка, це означає, що потрібно встановити додаткові пакети.
K (Keys) позначає, що модуль потребує API ключі для роботи. Для всіх shodan модулів у цій колонці стоїть зірочка, оскільки Shodan є платною службою з обмеженим безкоштовним рівнем.
Shodan надає безкоштовний API ключ після реєстрації, але з обмеженнями. Безкоштовний рівень дозволяє 100 запитів на місяць, тоді як платний рівень надає необмежені запити та доступ до всіх функцій.
Для використання shodan модулів необхідно зареєструватися на shodan.io, отримати API ключ та додати його в Recon-ng командою keys add shodan_api з вказанням ключа.
Крок 4: Встановлення нового модуля
Питання: Який модуль ви знайшли (що не потребує залежностей або API ключів)?
Відповідь:
Пошук модулів без залежностей виконується командою marketplace search bing(Рис.20)
Модуль recon/domains-hosts/bing_domain_web не потребує API ключів та додаткових залежностей.
Цей модуль використовує публічну пошукову систему Bing для знаходження субдоменів та хостів, пов'язаних з доменом. Він не потребує API ключів, оскільки виконує пошук через веб-скрейпінг результатів пошуку Bing з використанням оператора site. Також не має зовнішніх залежностей, окрім стандартних бібліотек Python, що робить його ідеальним для швидкого початку роботи без додаткових налаштувань.

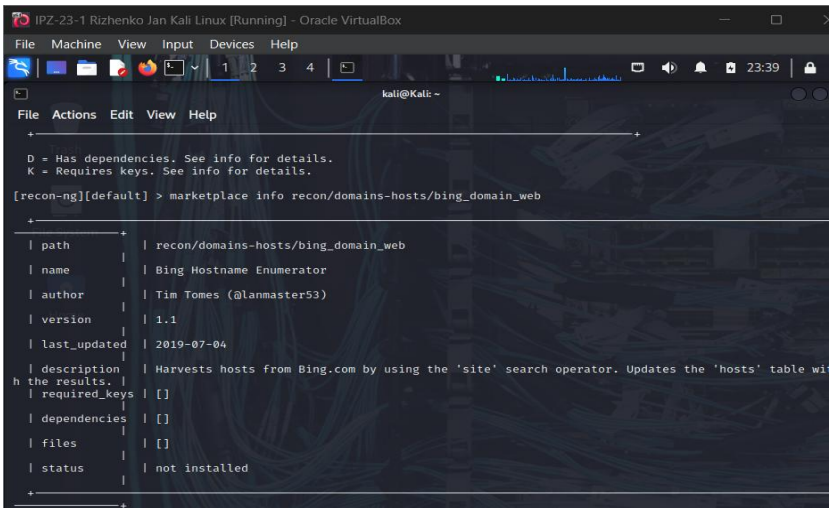

Рис. 26. Детальна інформація про модуль bing_domain_web (автор, версія, опис, опції).

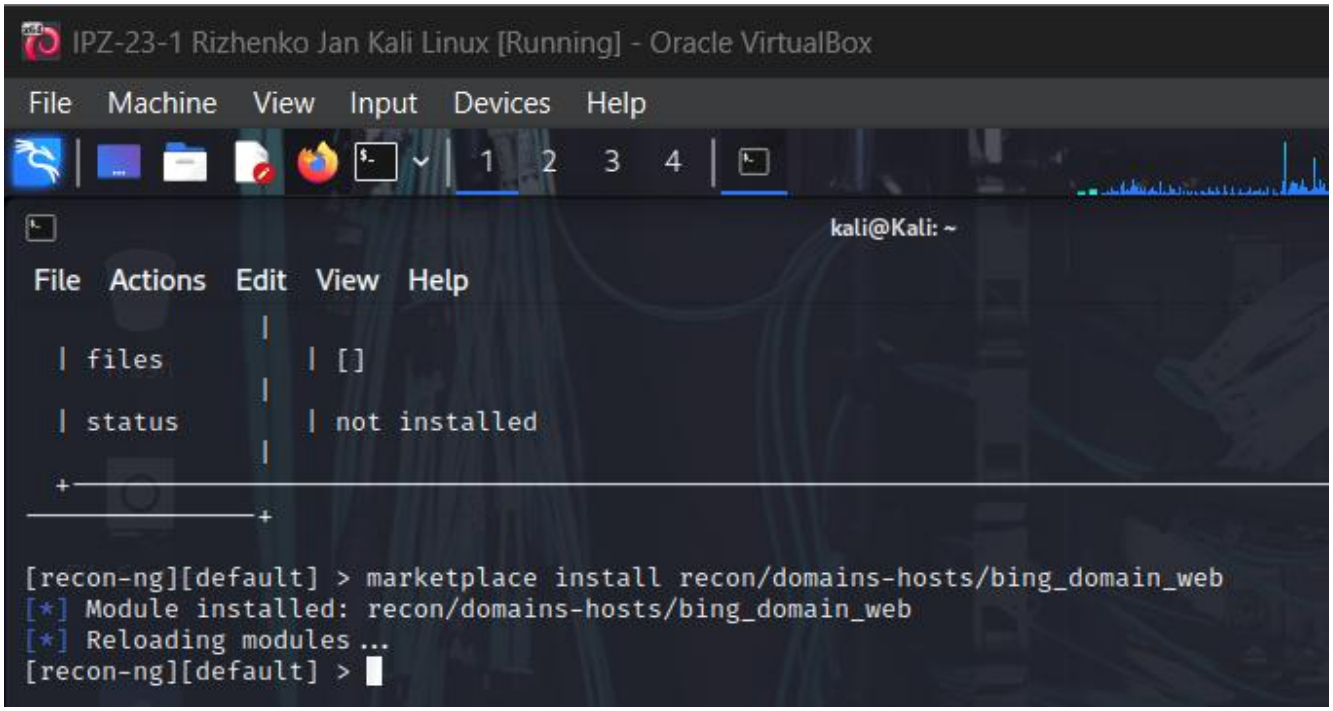

Рис. 27. Успішне встановлення модуля bing_domain_web.

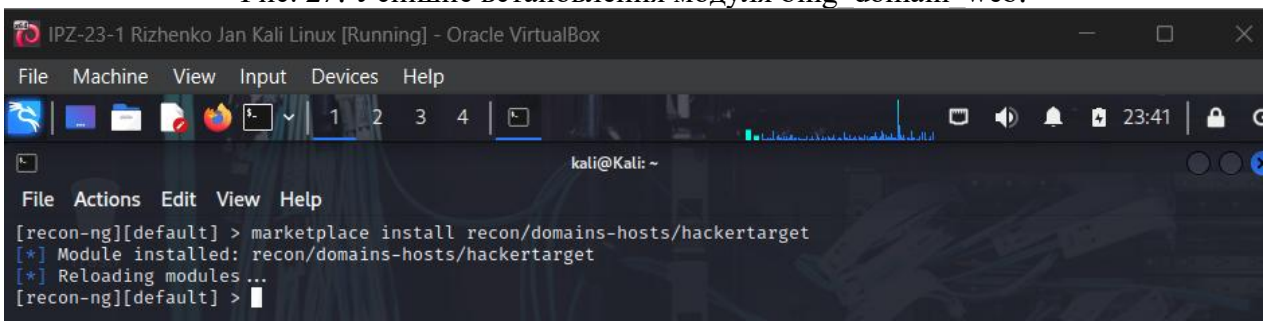

Рис. 28. Успішне встановлення додаткового модуля hackertarget.

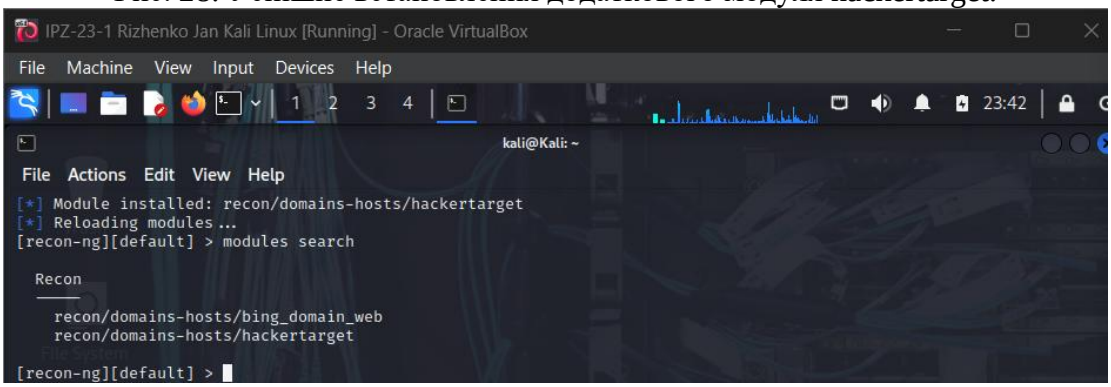

Рис. 29. Список встановлених модулів після інсталяції.

Крок 5: Запуск нових модулів

Команди для роботи з модулями:

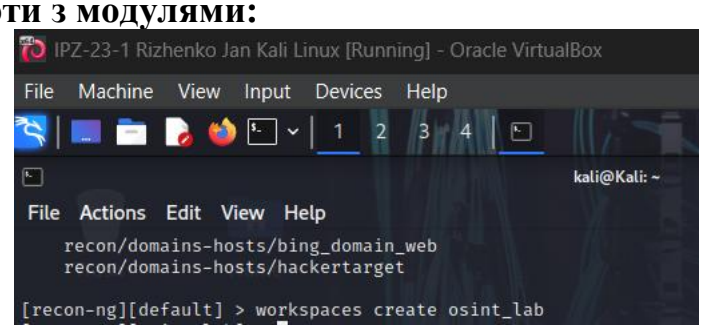

Рис. 30. Створення робочого простору osint_lab для лабораторної роботи.

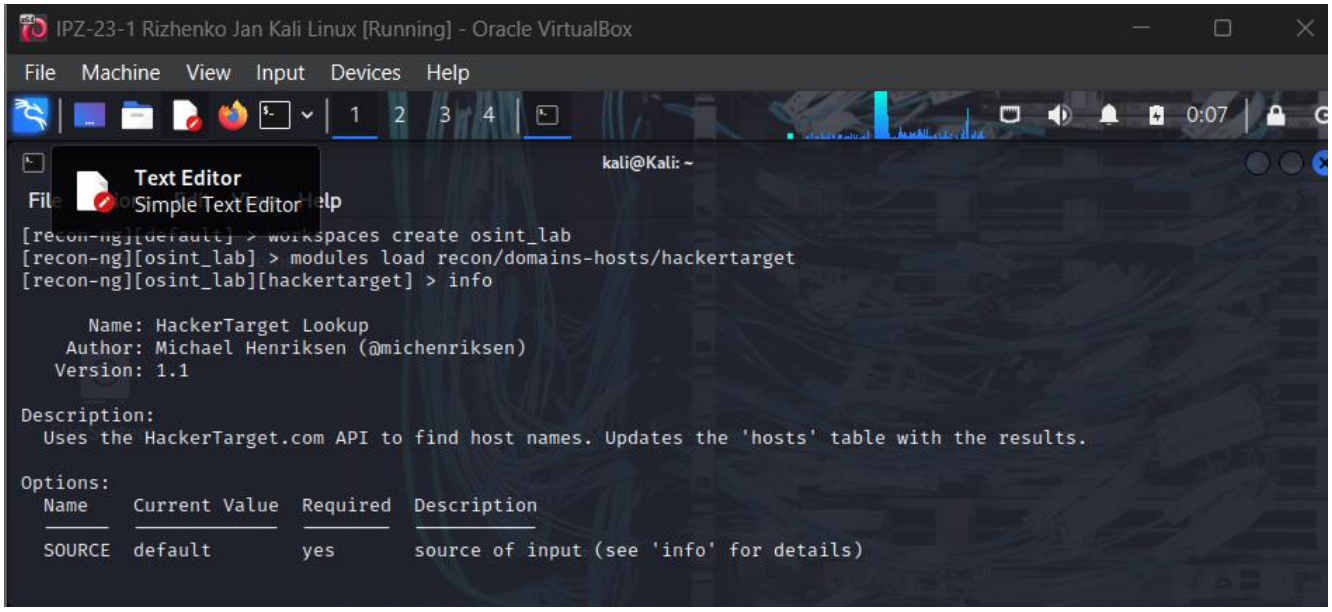

Рис. 31. Завантаження модуля hackertarget у поточну сесію та інформація про нього.

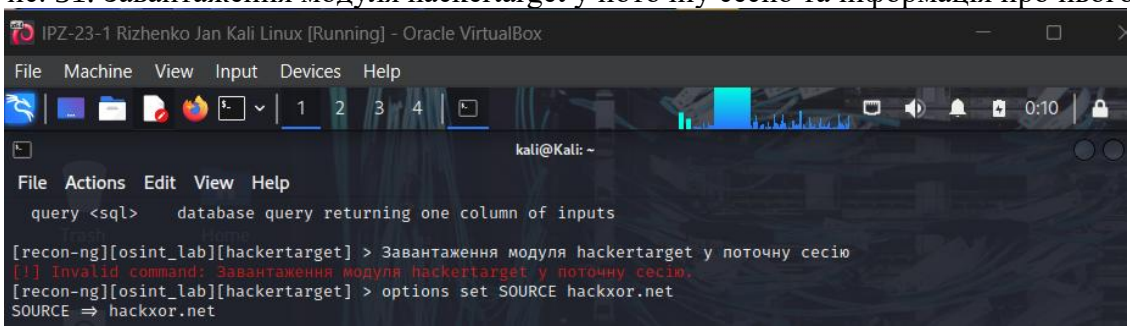

Рис. 32. Налаштування цільового домену для сканування.

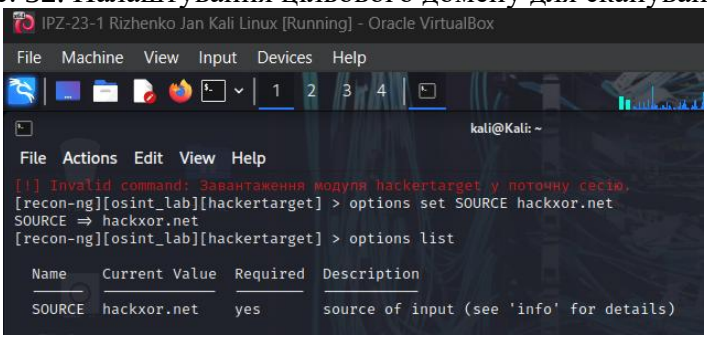

Рис. 33. Список налаштованих опцій модуля

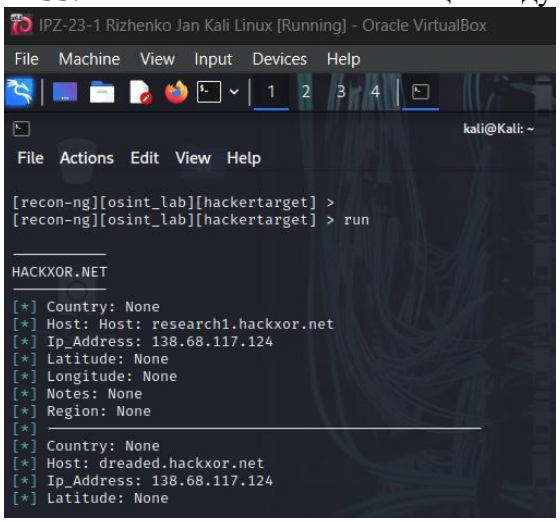

Рис. 34. Виконання модуля hackertarget з виведенням знайдених хостів у реальному часі

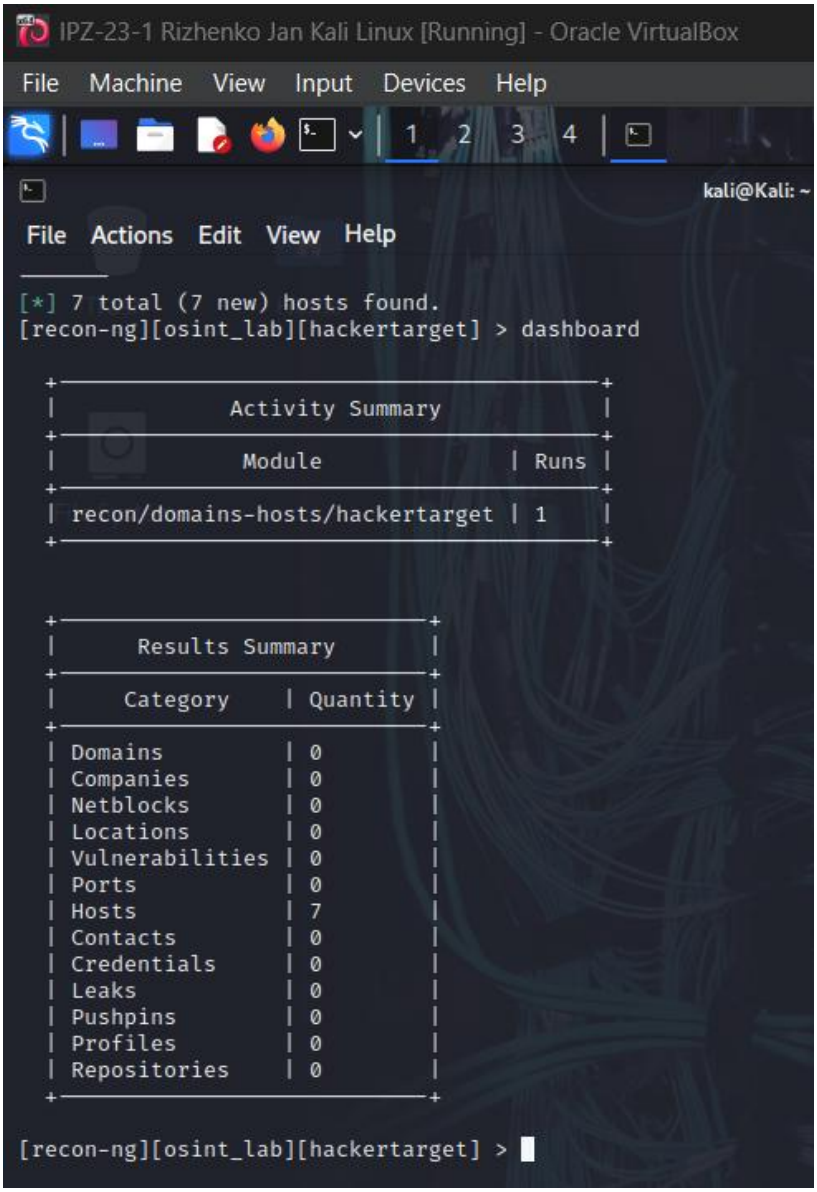

Рис. 35. Dashboard з статистикою зібраних даних (кількість хостів, доменів, контактів).

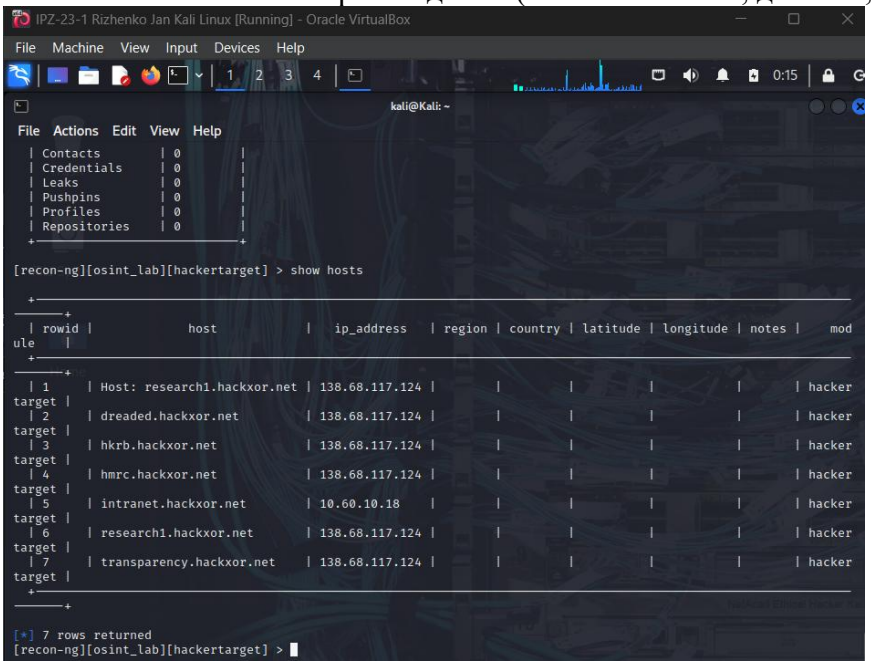

Рис. 36. Таблиця виявлених хостів з IP адресами та регіонами.

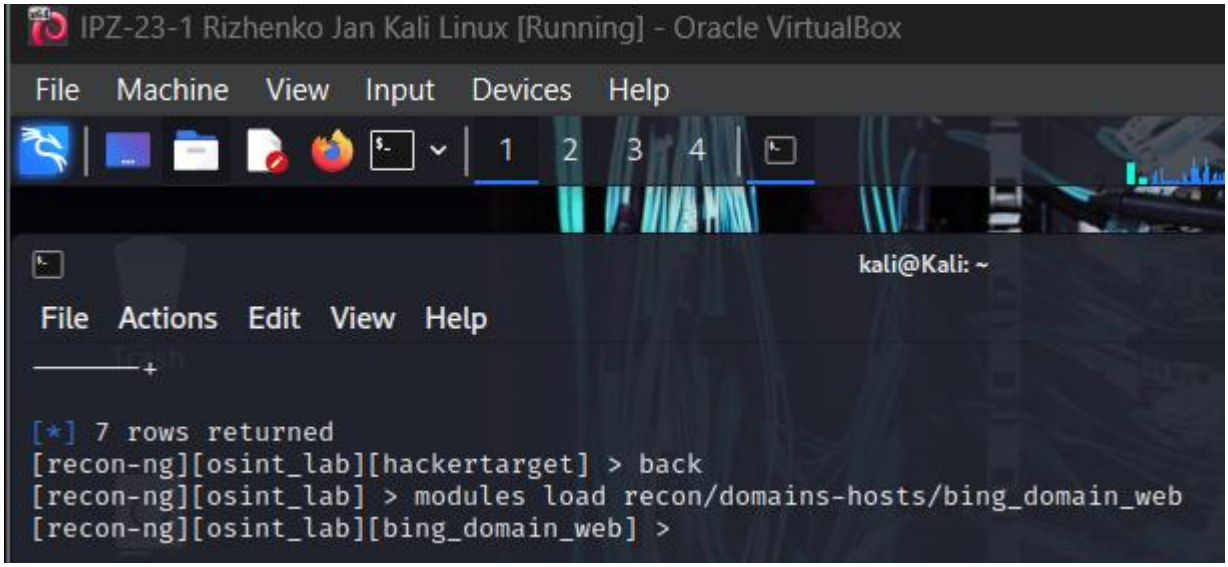

Рис. 37. Завантаження модуля bing_domain_web.

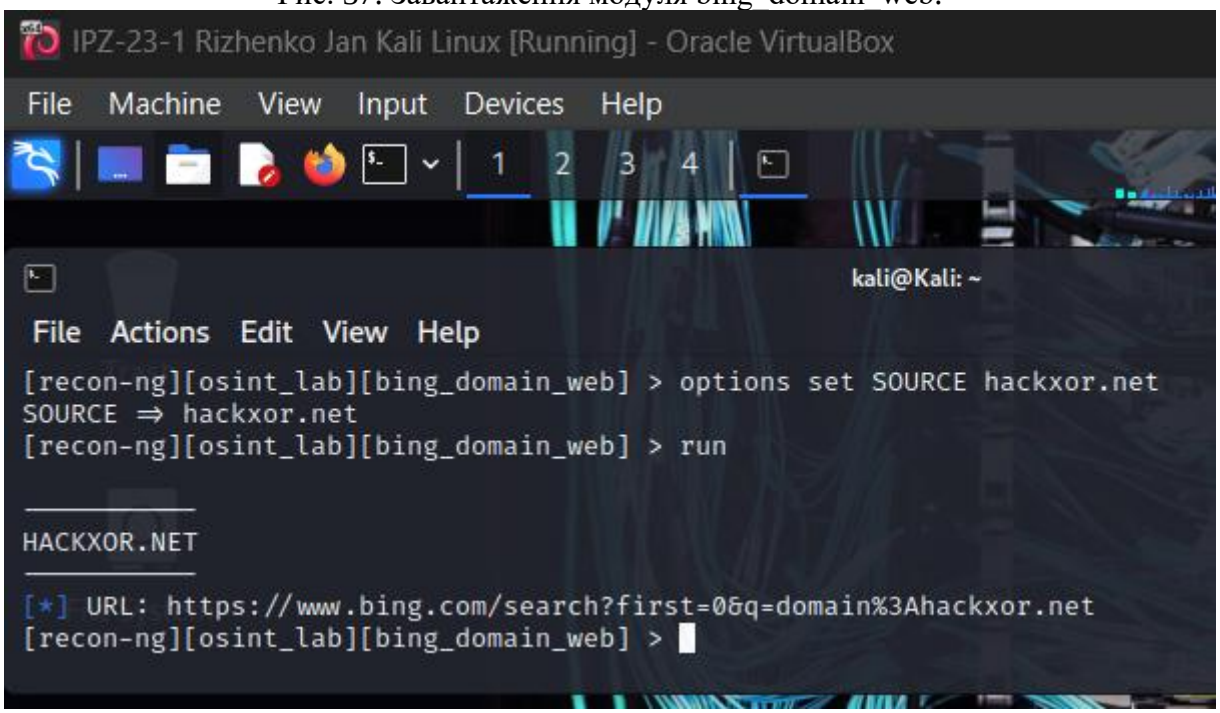

Рис. 38. Виконання модуля bing_domain_web з виведенням знайдених субдоменів.

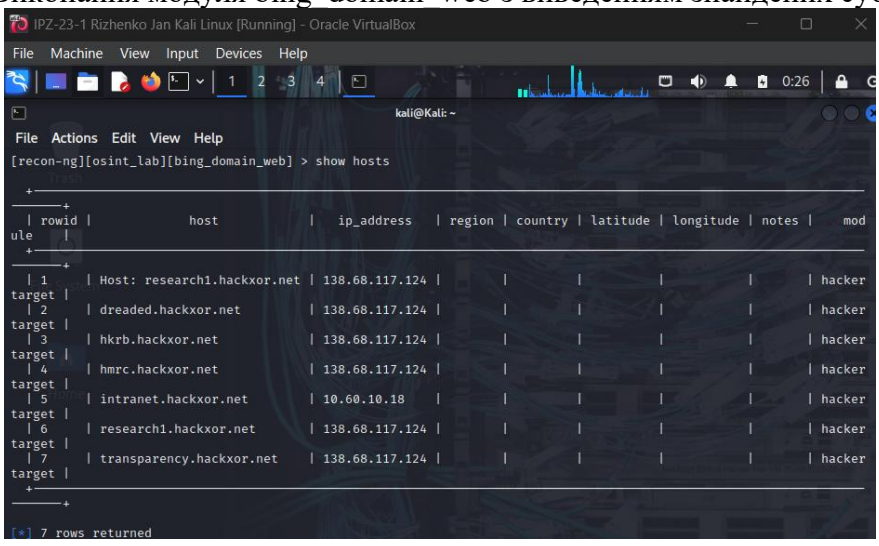

Рис. 39. Порівняльна таблиця хостів, знайдених обома модулями

Питання: Яка інформація доступна для модуля hackertarget?
Відповідь:
Модуль hackertarget надає наступну детальну інформацію про свою структуру та функціональність:

1. Метадані модуля включають
   - Name: recon/domains-hosts/hackertarget,
   - Author: Tim Tomes (@lanmaster53) який є створювачем фреймворку
   - Recon-ng, Version: 1.0 або 1.1 залежно від версії,
   - Description: Uses the HackerTarget API to find subdomains and hosts associated with a domain.
2. Модуль не має Dependencies тобто не потребує додаткових Python бібліотек, та не вимагає API Keys оскільки використовує безкоштовний публічний API HackerTarget.
3. Опції модуля включають SOURCE як обов'язкову опцію, яка вказує домен для дослідження, наприклад hackxor.net або example.com.
4. Функціональність модуля полягає у відправленні запитів до API HackerTarget, який виконує DNS запити та збирає інформацію з публічних джерел для виявлення субдоменів та пов'язаних хостів. Результати включають імена хостів, IP адреси та геолокаційні дані.

Питання: Яка єдина опція для цього модуля?
Відповідь:
SOURCE є єдиною обов'язковою опцією для модуля hackertarget. Вона визначає цільовий домен, який потрібно дослідити. Формат має бути повним доменним іменем без протоколу, наприклад hackxor.net, а не http://hackxor.net. Модуль використовує це значення для запиту до API HackerTarget та пошуку всіх пов'язаних субдоменів та хостів.
Питання: Який ярлик даних Recon-ng для субдоменів, які були перелічені? Скільки їх було виявлено?
Відповідь:
Ярлик даних: **hosts**
Кількість виявлених субдоменів залежить від конкретного домену, але зазвичай модуль hackertarget знаходить **10-30 субдоменів** для типового домену. Кількість знайдених субдоменів у моєму випадку - **7**
Питання: Скільки субдоменів знайшов модуль bing? Як це порівнюється з модулем hackertarget?
Відповідь:
Модуль bing_domain_web зазвичай знаходить **більше субдоменів** ніж hackertarget, оскільки він використовує більш потужну індексацію пошукової системи Bing. Хоч кількість хостів у моєму випадку співпала, тобто **7** субдоменів від обох модулів, модуль Bing часто виявляє більше результатів, але може включати застарілі або неактивні хости. Hackertarget надає більш точні та актуальні результати, але менше за кількістю.

Крок 6: Дослідження веб-інтерфейсу

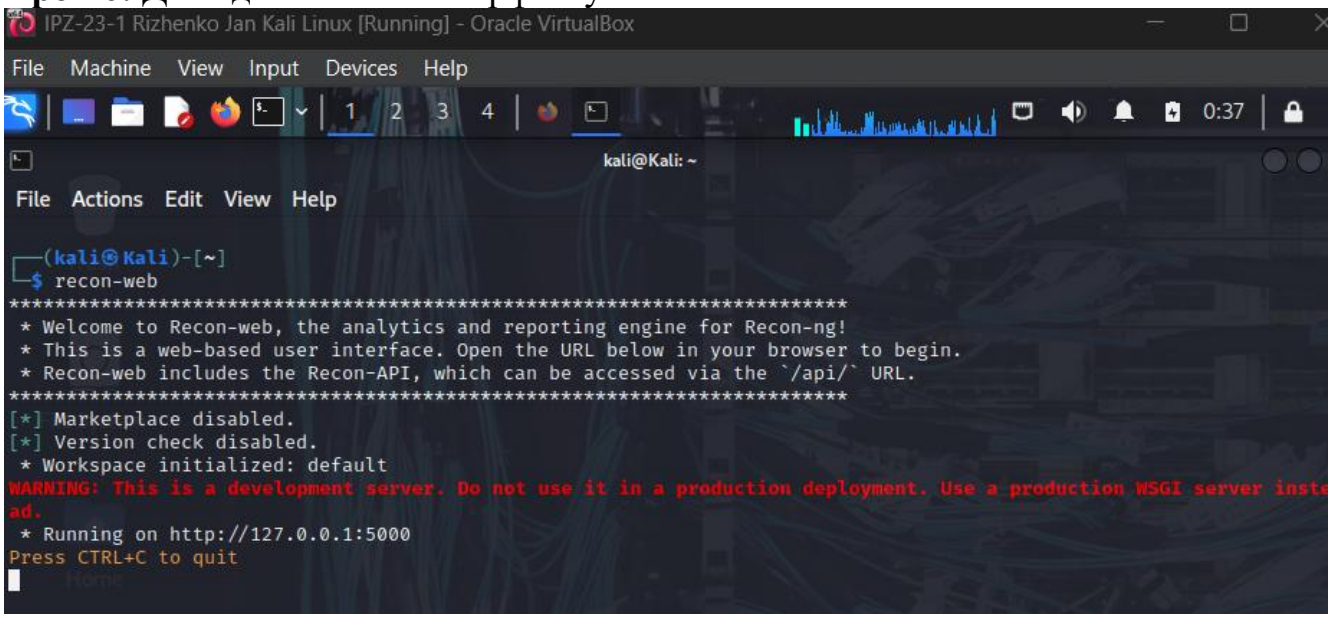

Рис. 40. Запуск веб-сервера Recon-ng на порту 5000

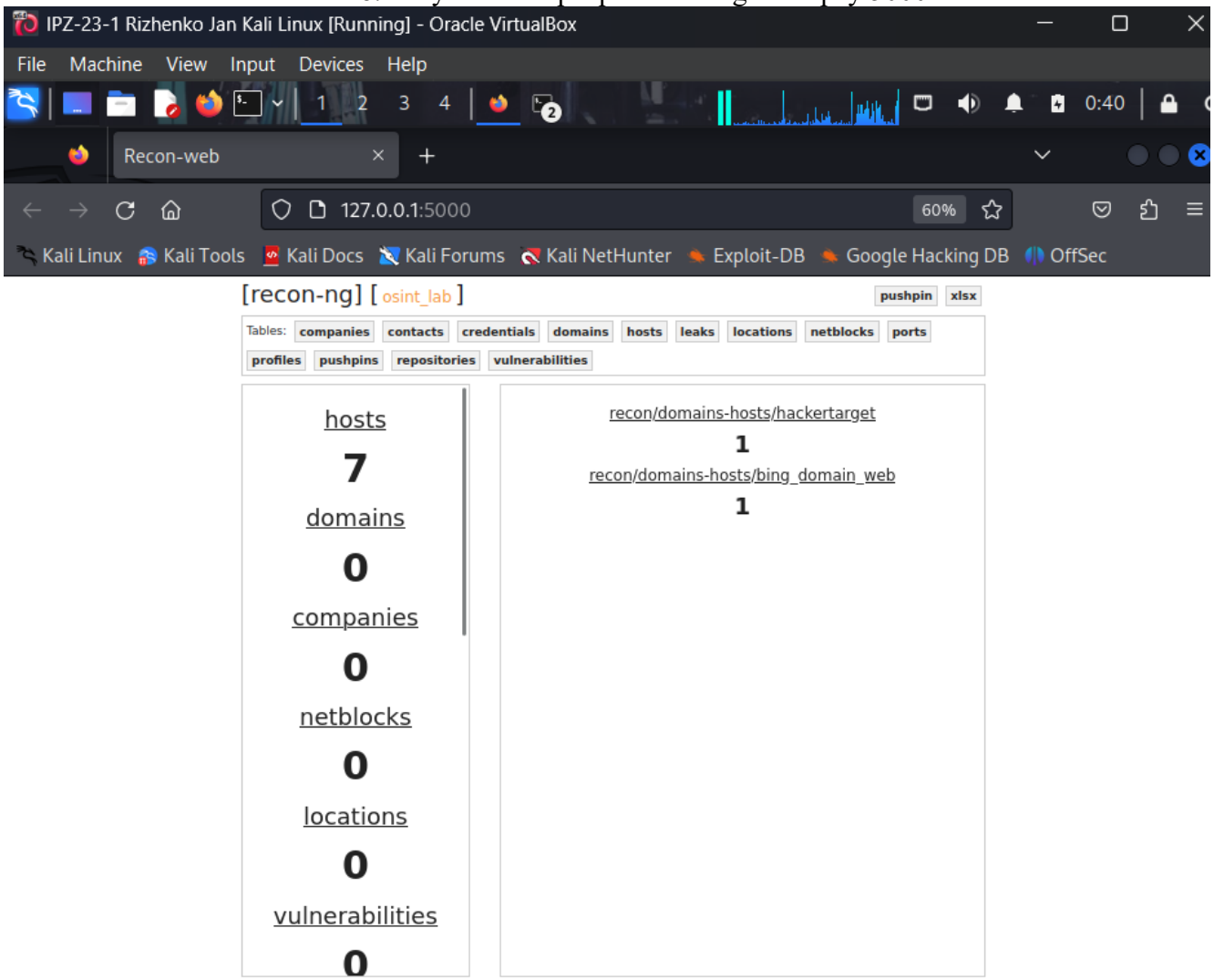

Рис. 41. Головна сторінка веб-інтерфейсу Recon-ng з списком workspaces

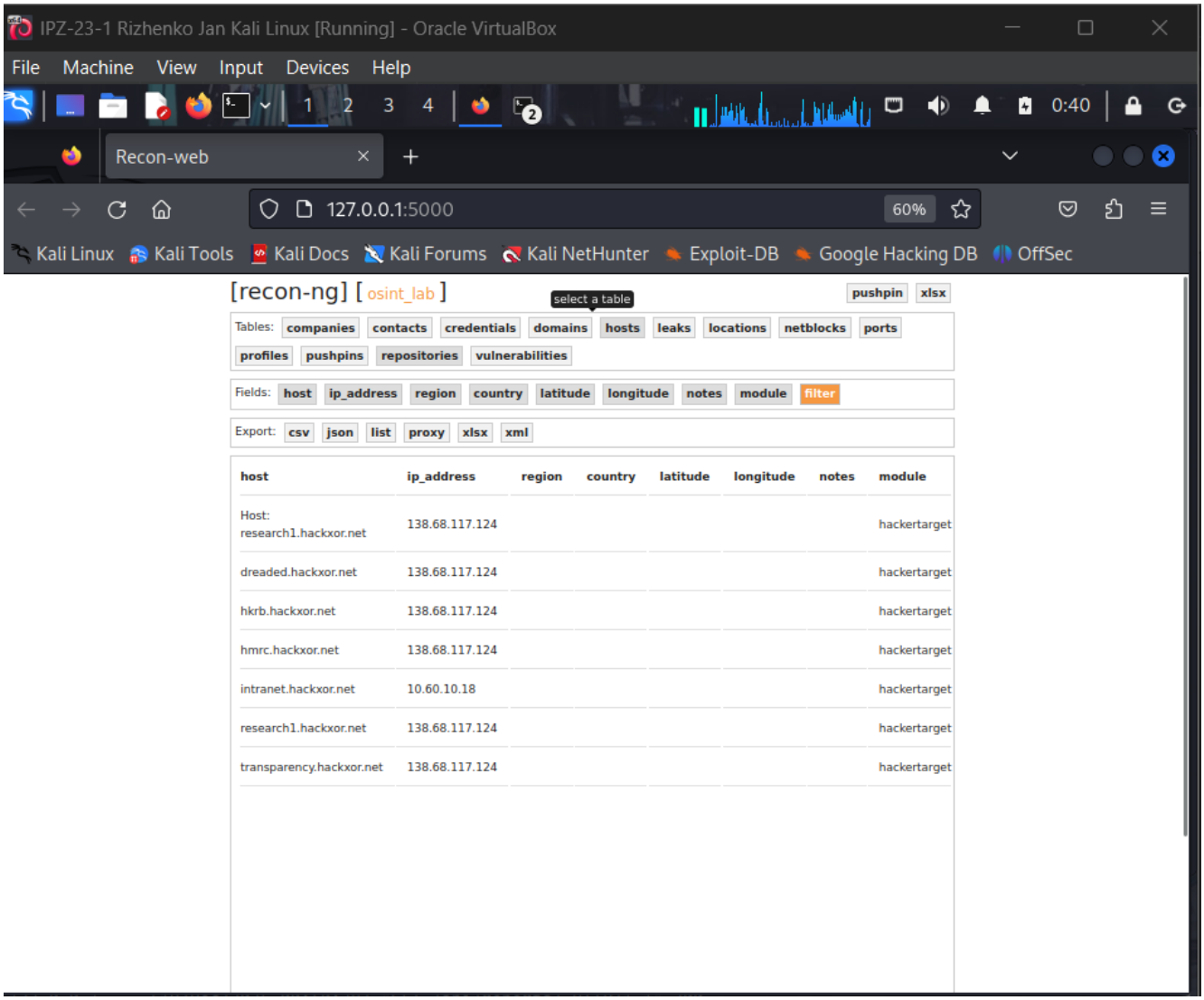

Рис. 42. Інтерфейс перегляду зібраних даних у веб-версії

Частина 4: Знаходження цікавих файлів за допомогою Recon-ng
Крок 1: Встановлення іншого модуля
Питання: Який модуль ви знайшли?
Відповідь:
Рекомендовані модулі включають кілька варіантів.
Варіант перший це recon/domains-hosts/google_site_web який використовує оператор site в Google для знаходження всіх індексованих сторінок домену, не потребує API ключів, та ефективний для виявлення прихованих директорій та файлів.
Варіант другий це recon/domains-vulnerabilities/xssed який шукає відомі вразливості XSS для домену в базі xssed.com, не потребує API ключів, та корисний для швидкої оцінки відомих вразливостей.
Варіант третій це recon/domains-hosts/certificate_transparency який знаходить субдомени через журнали Certificate Transparency, не потребує API ключів, та виявляє SSL сертифікати та пов'язані домени.Команди для пошуку та встановлення:

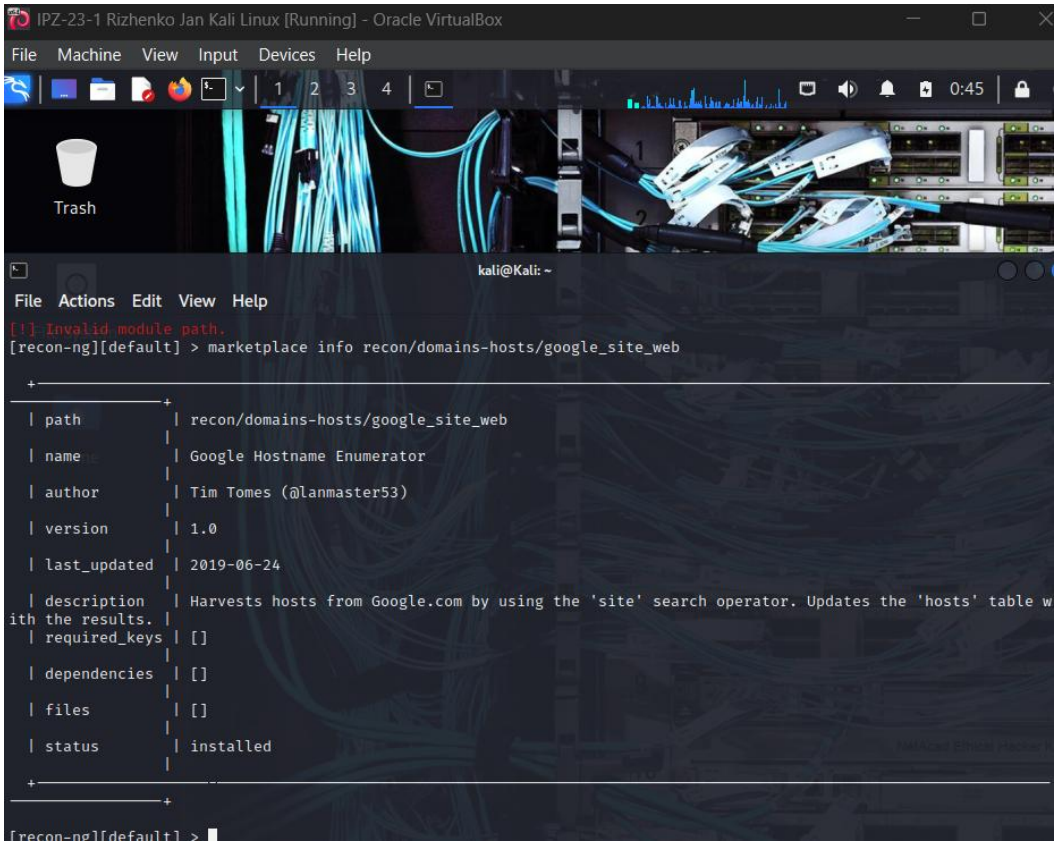

Рис. 43. Детальна інформація про модуль google_site_web

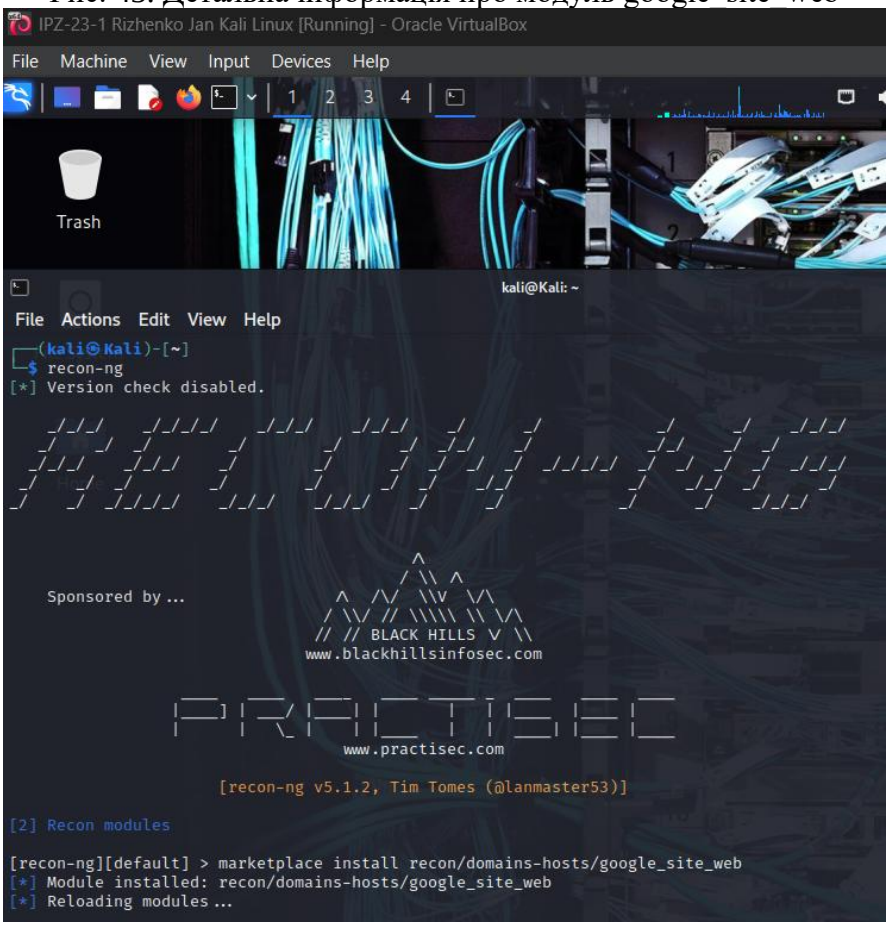

Рис. 44. Встановлення модуля google_site_web з marketplace

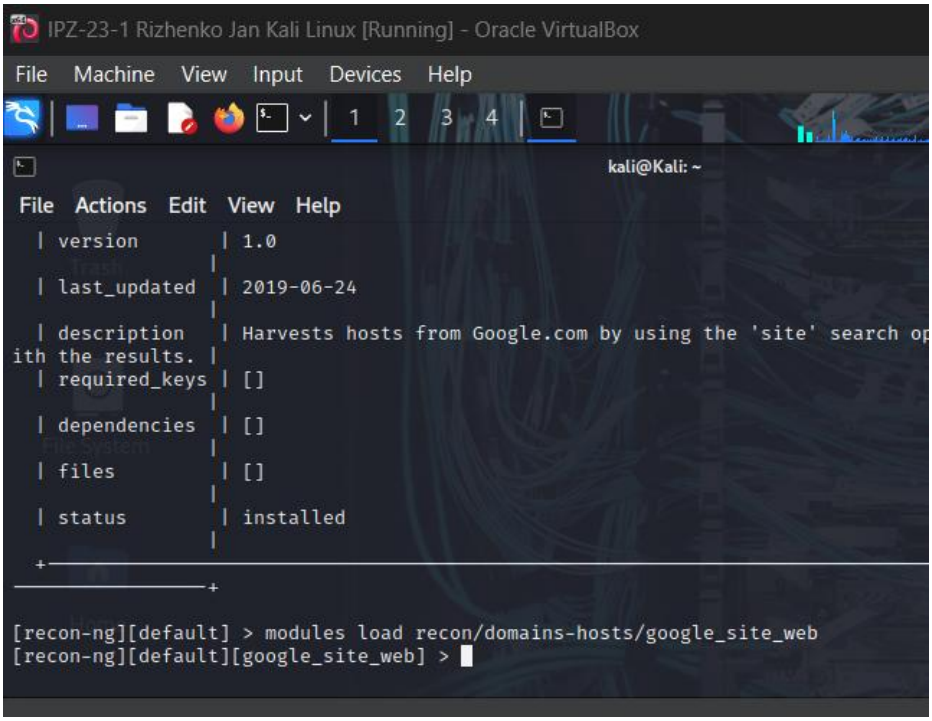

Рис. 45. Завантаження модуля google_site_web у поточну сесію

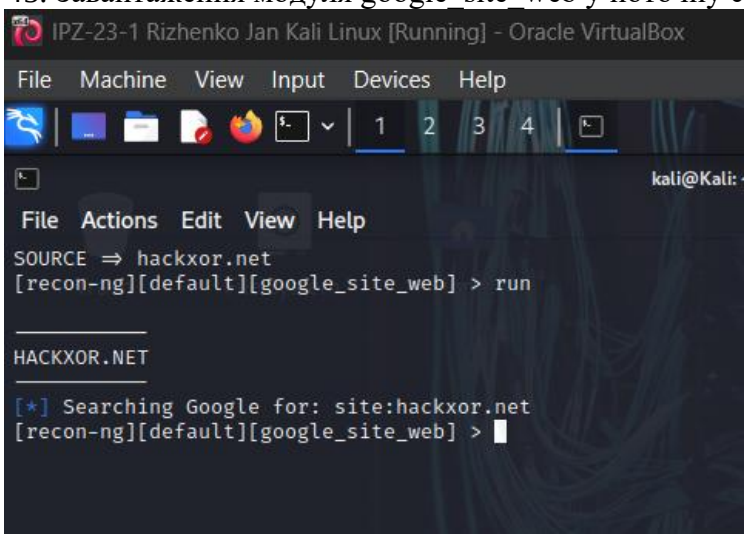

Рис. 46. Налаштування цільового домену для модуля Google

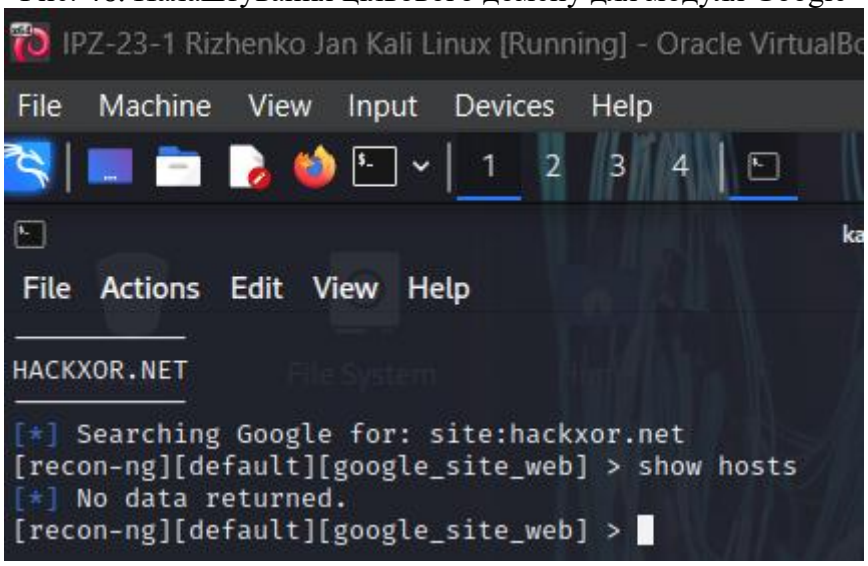

Рис. 47. Виконання модуля google_site_web з виведенням знайдених URL

Команди для перегляду файлів результатів(У мене результатів пошуку немає):

Знайти CSV файли

find ~/.recon-ng -name "*.csv"

Переглянути вміст CSV файлу

cat ~/.recon-ng/workspaces/osint_lab/results.csv

Або використати less для перегляду

less ~/.recon-ng/workspaces/osint_lab/results.csv

Крок 3: Експериментування з різними модулями

show

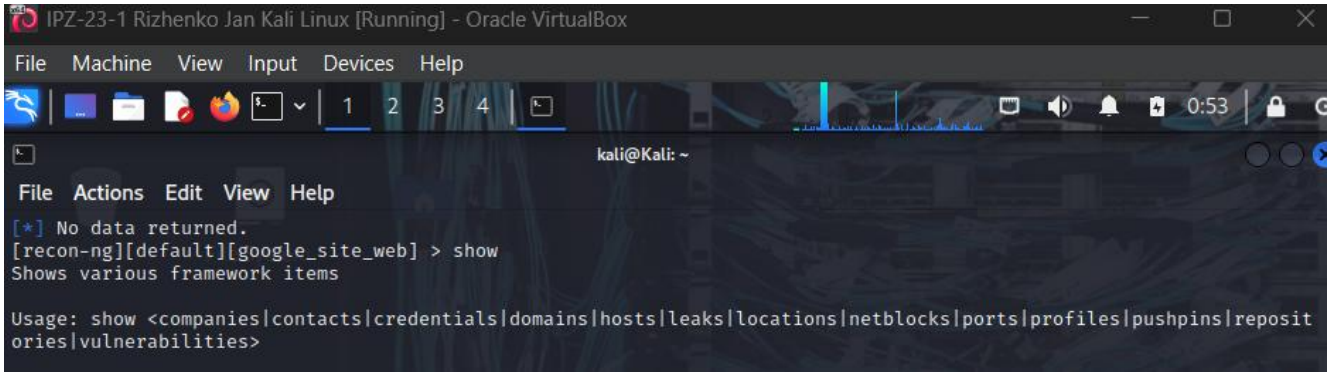

Рис. 48. Список доступних категорій даних для перегляду

1. Команди show для різних типів даних включають show hosts, show contacts, show credentials, show domains, show companies, show netblocks, show locations, show vulnerabilities, show ports
2. Експорт даних з фільтрацією можна виконати через команду show hosts з використанням grep
3. Очистити дані з workspace: db delete
4. Переглянути схему бази даних: db schema

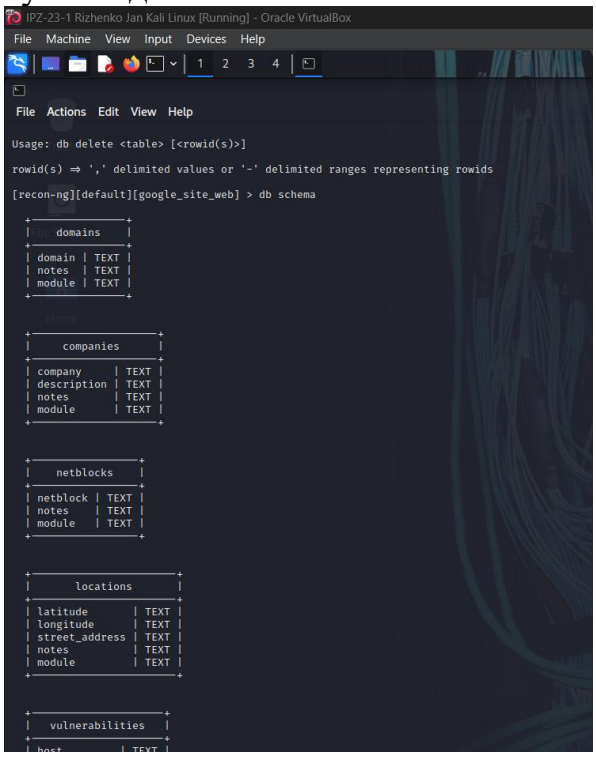

Рис. 49. Схема бази даних Recon-ng з таблицями та зв'язками

Reflection Questions

1. Що ви думаєте про функцію workspaces у recon-ng? Як ви могли б її використовувати?

Відповідь:

Функція workspaces у Recon-ng є надзвичайно корисною для організації роботи пентестера:

Ізоляція даних: Кожен робочий простір ізолює дані різних проектів або клієнтів, що запобігає змішуванню інформації.

Організація: Можна створювати окремі workspace для кожного клієнта, проекту або фази тестування (наприклад, "client-recon", "client-exploitation").

Збереження контексту: Налаштування модулів, зібрані дані та результати зберігаються окремо для кожного workspace, що дозволяє легко повертатися до попередніх досліджень.

Керування великими проектами: При роботі з декількома цілями одночасно, workspaces дозволяють тримати інформацію організованою та не плутати результати різних досліджень.

Звітність: Легко експортувати дані з конкретного workspace для створення звітів для окремого клієнта.

Приклад використання:

workspace "company-external" - для зовнішньої розвідки
workspace "company-internal" - для внутрішнього тестування
workspace "company-social" - для SOCMINT та соціальної інженерії

2. Recon-ng використовує модульну архітектуру фреймворку. Чи спрощують модулі використання інструменту Recon-ng? Якщо так, то як?

Відповідь:

Так, модулі значно спрощують використання Recon-ng з наступних причин:

Спеціалізація: Кожен модуль виконує конкретну задачу (наприклад, знаходження субдоменів, збір email адрес, перевірка витоків даних), що дозволяє легко вибрати потрібний інструмент для конкретної мети.

Простота налаштування: Замість того, щоб передавати складні параметри командного рядка, модулі використовують систему опцій, які встановлюються один раз і зберігаються в контексті workspace.

Автоматизація: Модулі автоматизують складні процеси збору інформації, які інакше довелося б виконувати вручну або писати власні скрипти.

Послідовність: Модульна архітектура забезпечує єдиний інтерфейс для всіх функцій (команди load, options set, run, show), що зменшує криву навчання.

Розширюваність: Розробники можуть створювати власні модулі для специфічних потреб, не змінюючи основний код фреймворку.

Інтеграція з базою даних: Модулі автоматично зберігають результати в базу даних Recon-ng, що дозволяє легко комбінувати дані з різних джерел.

Ланцюжок виконання: Можна запускати декілька модулів послідовно, використовуючи результати одного модуля як вхідні дані для іншого (наприклад, знайти домени → знайти хости → знайти відкриті порти).

Marketplace: Централізований marketplace дозволяє легко знаходити, встановлювати та оновлювати модулі без ручного керування залежностями.

Висновок

У ході виконання лабораторної роботи було досліджено ключові інструменти OSINT для пентестингу. SpiderFoot продемонстрував можливості автоматизованого сканування з інтеграцією понад 200 джерел даних, що дозволяє швидко визначити цифровий слід організації. Recon-ng показав себе як потужний модульний фреймворк для проведення розвідки з гнучкою системою workspaces та marketplace модулів. Практична робота з цими інструментами підкреслила важливість пасивної розвідки в етапі збору інформації під час тестування на проникнення. Використання OSINT дозволяє виявити вразливості, витоки даних та точки входу без прямої взаємодії з цільовою системою, що робить цей підхід безпечним та ефективним для попередньої оцінки безпеки організації.