Лабораторна робота № 9(3.1.21)

Пошуки через Shodan

Хід роботи:

Частина 1: Створення облікового запису Shodan та реєстрація API ключа

Крок 1: Реєстрація облікового запису Shodan

https://www.shodan.io/ &

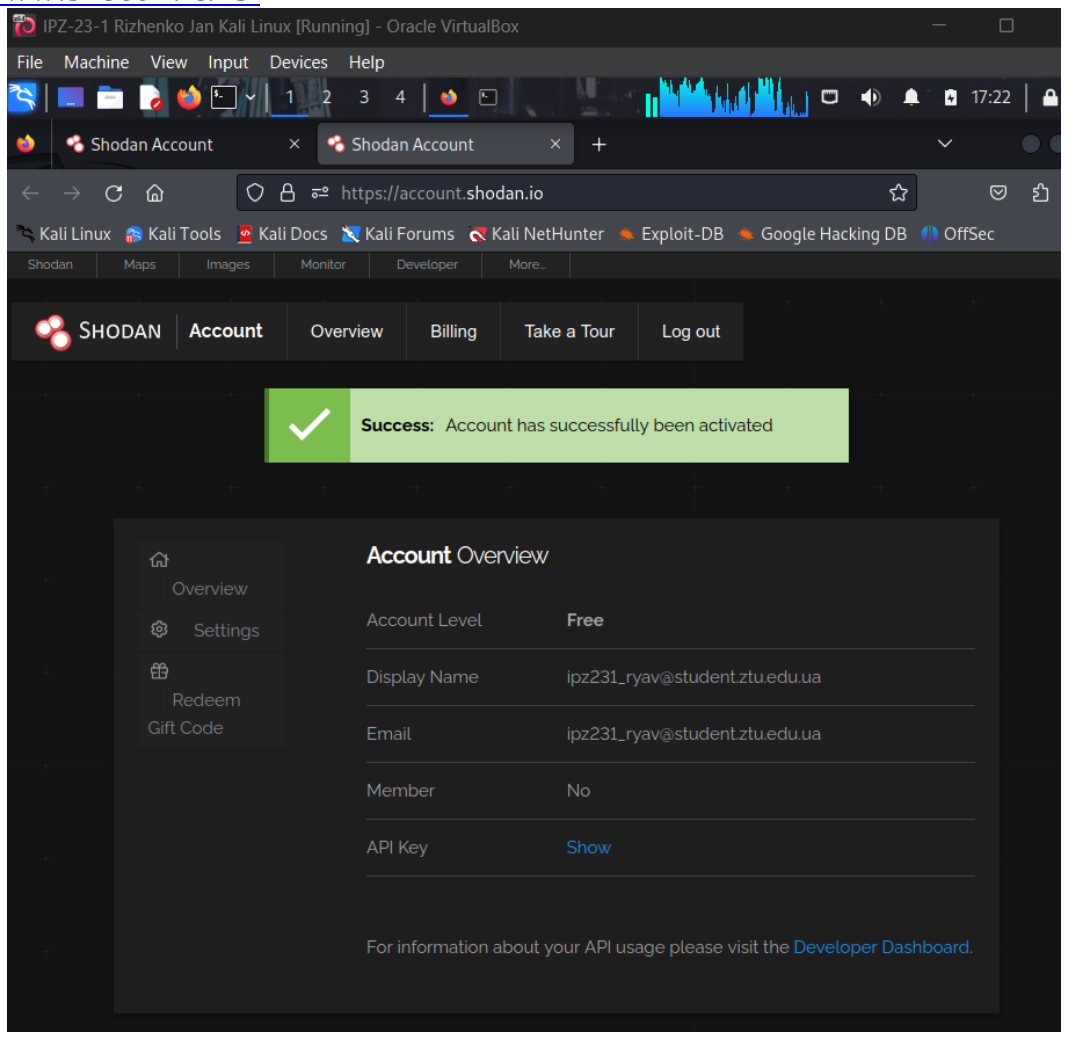

Рис. 1. Успішна реєстрація на сайті shodan.io.

Обмеження безкоштовного облікового запису:

Безкоштовний акаунт:

- До 50 результатів пошуку
- Базові фільтри
- Обмежені API запити (1 запит/секунду)
- Експорт даних обмежений

Платна підписка (від $69/місяць):

- Необмежені результати
- Розширені фільтри
- Більше API запитів

- Повний експорт даних
- Історичні дані
- Інформація про вразливості

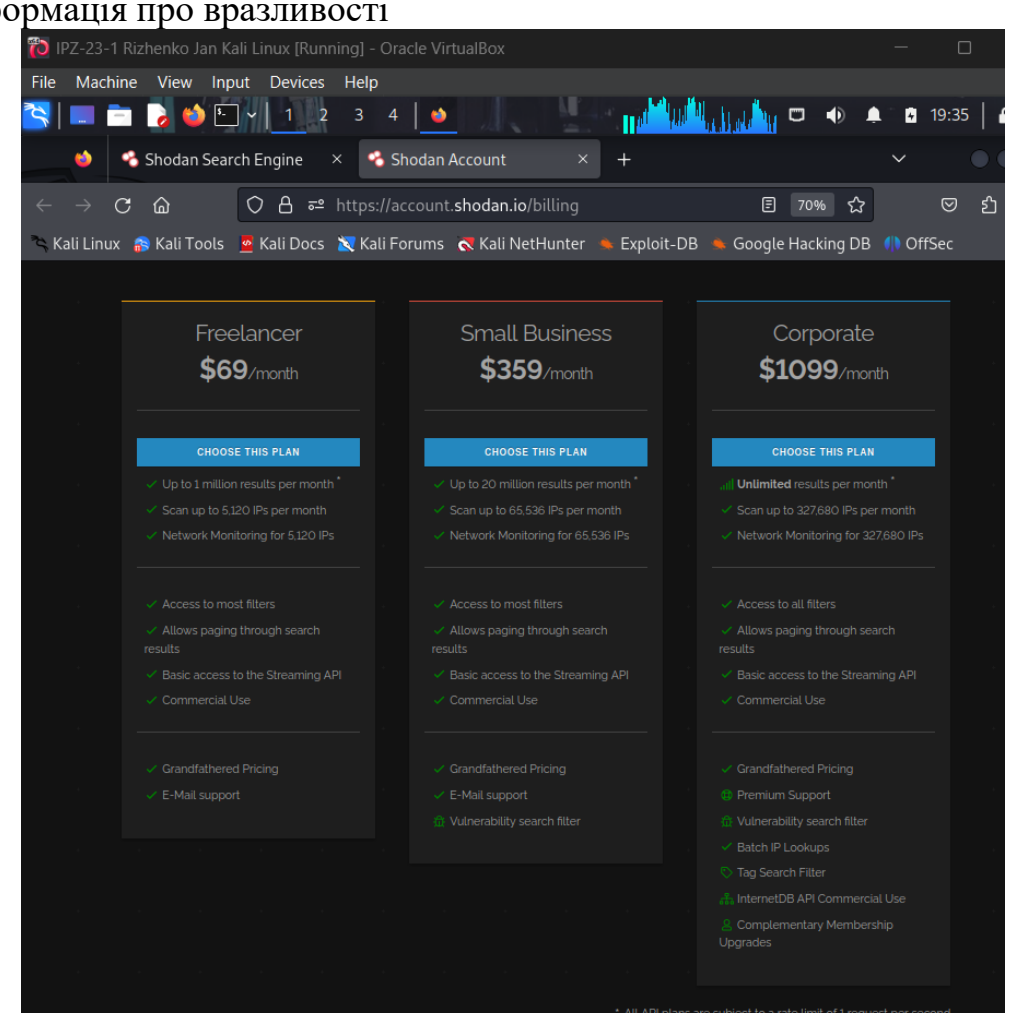

Рис. 2. Порівняння можливостей безкоштовного та платного акаунтів.

Питання: Згідно з Shodan, яка фундаментальна одиниця даних, яку він збирає?

Відповідь:

Banner - це фундаментальна одиниця даних, яку збирає Shodan.

Banner (банер) - це інформація, яку сервіс або пристрій відправляє при підключенні. Він містить:

1. Ідентифікацію сервісу:
   - Назва ПЗ (Apache, nginx, OpenSSH)
   - Версія програми (Apache/2.4.41)
   - Операційна система
2. Інформація про пристрій:
   - Тип пристрою (router, webcam, server)
   - Виробник (Cisco, Hikvision, Dahua)
   - Модель
3. Деталі конфігурації:
   - Відкриті порти
   - Підтримувані протоколи

- SSL/TLS сертифікати

Приклад banner:

HTTP/1.1 200 OK
Server: Apache/2.4.41 (Ubuntu)
Date: Wed, 18 Dec 2024 10:30:00 GMT
Content-Type: text/html
X-Powered-By: PHP/7.4.3

Shodan сканує інтернет, підключається до пристроїв на різних портах, збирає ці banners, та індексує їх у своїй базі даних.

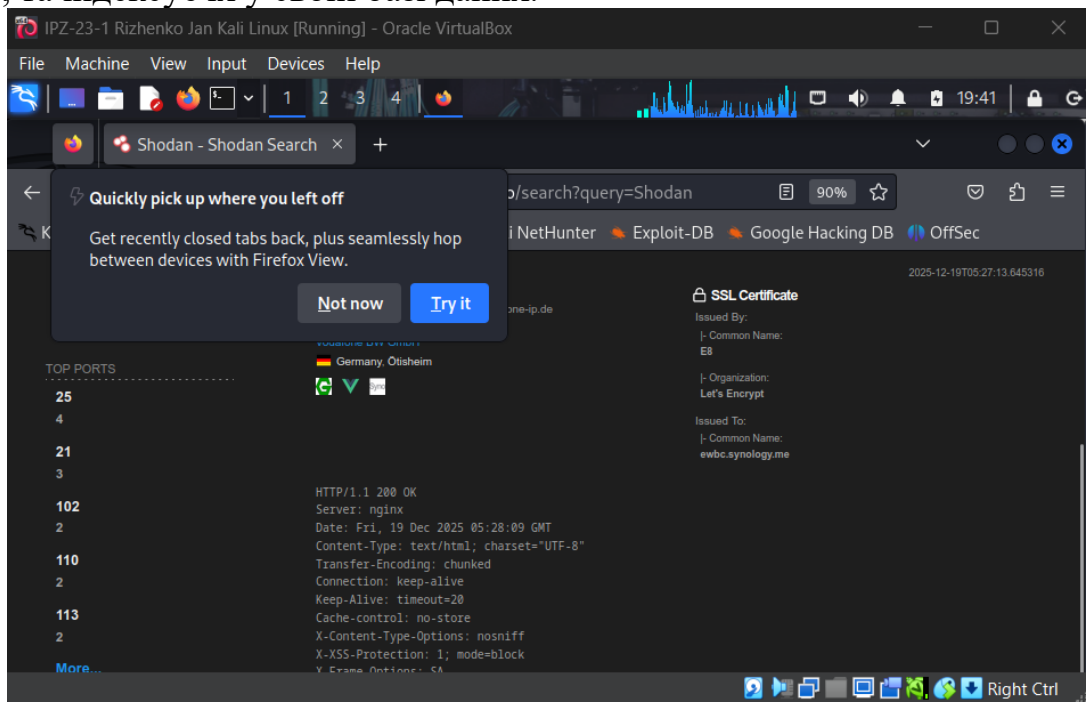

Рис. 3. Приклад banner інформації з результату Shodan.

Частина 2: Використання веб-сайту Shodan для пошуку вразливих IoT пристроїв

Крок 1: Використання пошукового рядка Shodan

Базові пошукові запити:

- Webcam
- Camera
- Router
- Printer
- Scada
- Ics
- plc

Конкретні продукти:

- "default password"
- "admin admin"
- Apache
- Nginx
- Mikrotik
- ubiquiti

Сервіси:

- ftp
- ssh
- telnet
- rdp
- vnc

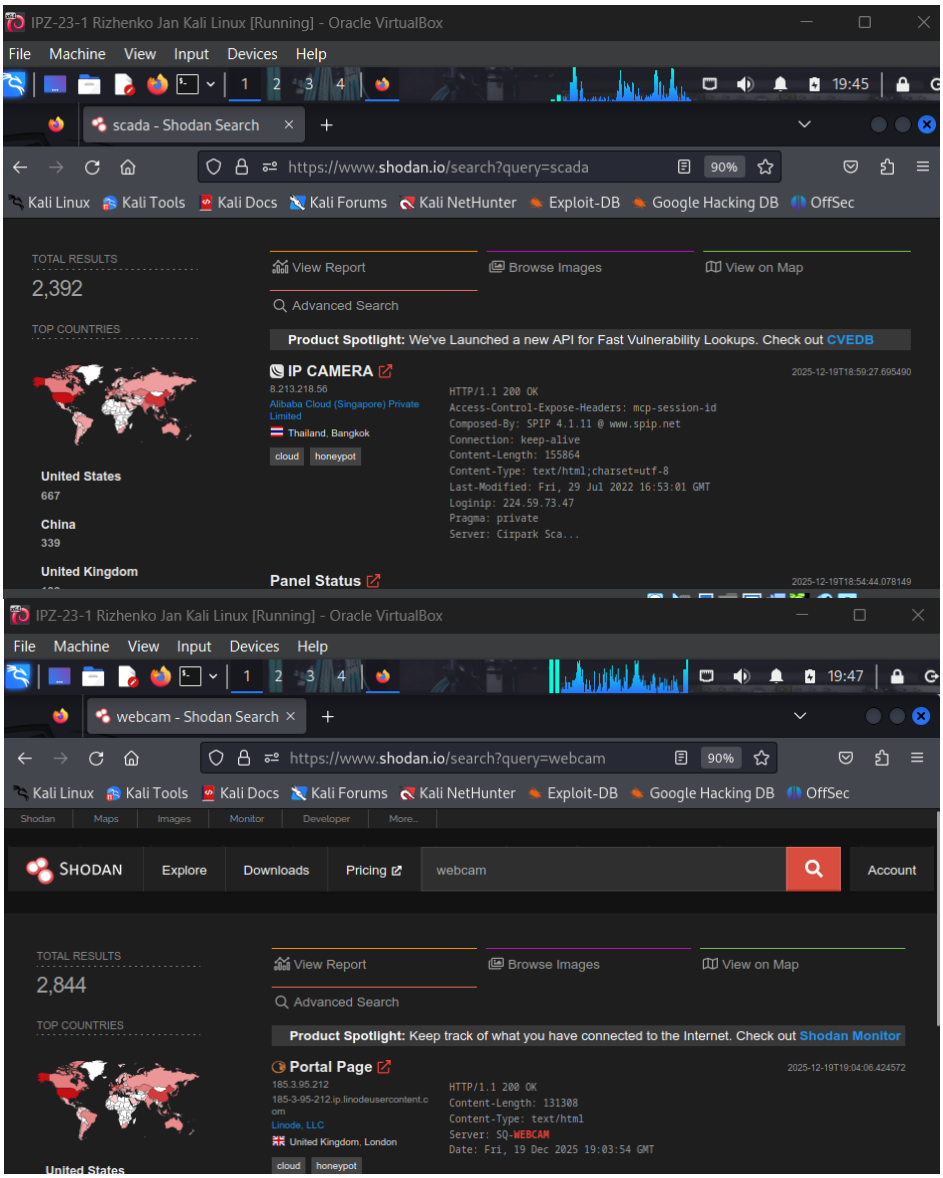

Рис. 4-5. Інтерфейс пошуку Shodan з прикладами запитів.

Питання: Яка країна є топ-країною зі знайденими веб-камерами згідно Shodan?

Відповідь:

Топ-країною є:

1. United States (США)

- Найбільша кількість підключених пристроїв
- Широке впровадження IoT
- Багато commercial та residential deployments

Інші топ-країни:

- China (Китай) - величезна кількість виробництва та споживання

- Germany (Німеччина) - високий рівень технологізації
- South Korea (Південна Корея) - розвинена інфраструктура
- Japan (Японія) - технологічно прогресивна

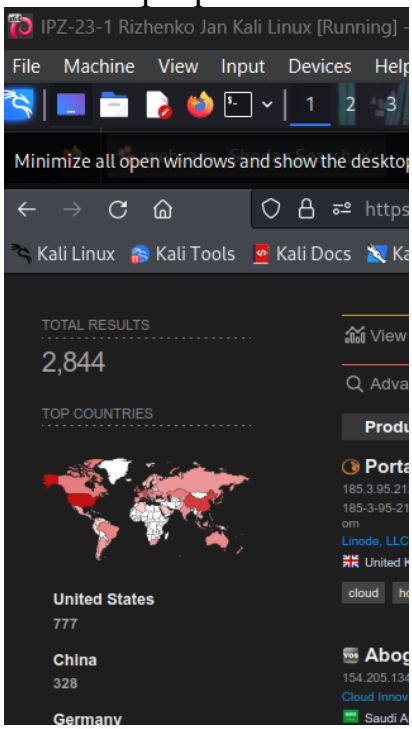

Рис. 6. Карта світу з розподілом знайдених пристроїв за країнами.

Питання: Яка інформація міститься в розділі General Information?

Відповідь:

Розділ General Information містить:

1. Базову інформацію:
   - IP Address - публічна IP адреса
   - Hostname - доменне ім'я
   - ISP - інтернет-провайдер
   - Organization - організація-власник IP
   - ASN - номер автономної системи
2. Географічну інформацію:
   - Country, City, Region
   - Postal Code
   - Coordinates (широта/довгота)
   - Time Zone
3. Технічну інформацію:
   - Ports - відкриті порти
   - Services - запущені сервіси
   - Operating System
   - Last Update - дата останнього сканування
4. Додаткову інформацію:
   - Vulnerabilities (CVE)
   - Tags (webcam, database, industrial)
   - Cloud Provider (AWS, Azure, GCP)

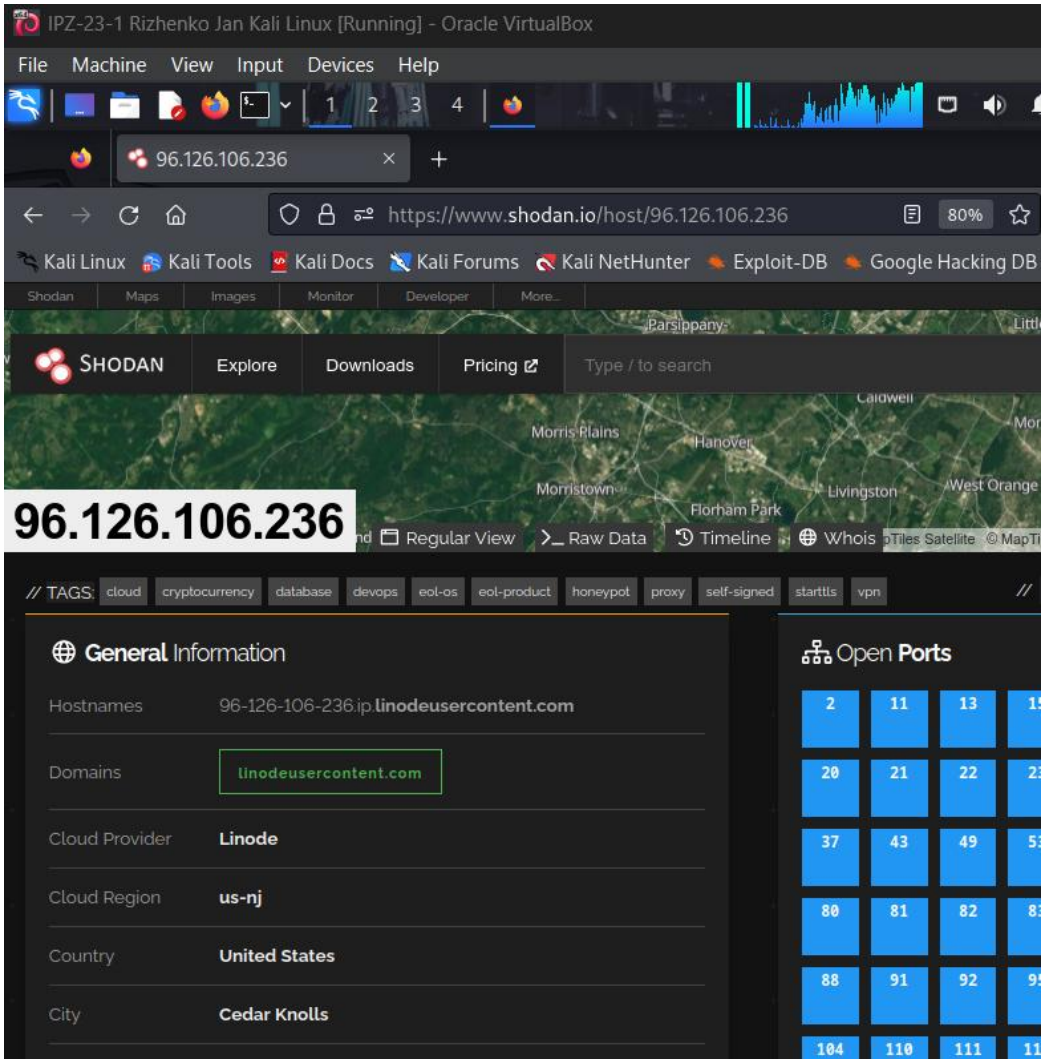

Рис. 7. Розділ General Information для обраного пристрою.

Питання: Які порти відкриті на обраній IP адресі?

Відповідь:

Типові відкриті порти для різних пристроїв:

1. Веб-камера:
   - Port 80 (HTTP) - веб-інтерфейс
   - Port 443 (HTTPS) - захищений веб-інтерфейс
   - Port 554 (RTSP) - потокове відео
   - Port 8080 (HTTP-alt) - альтернативний веб-порт
   - Port 37777 - Dahua DVR порт
2. FTP Server:
   - Port 21 (FTP)
   - Port 20 (FTP Data)
3. SSH Server:
   - Port 22 (SSH)
4. Database:
   - Port 3306 (MySQL)
   - Port 5432 (PostgreSQL)
   - Port 27017 (MongoDB)

5. Remote Access:
   - Port 23 (Telnet)
   - Port 3389 (RDP)
   - Port 5900 (VNC)

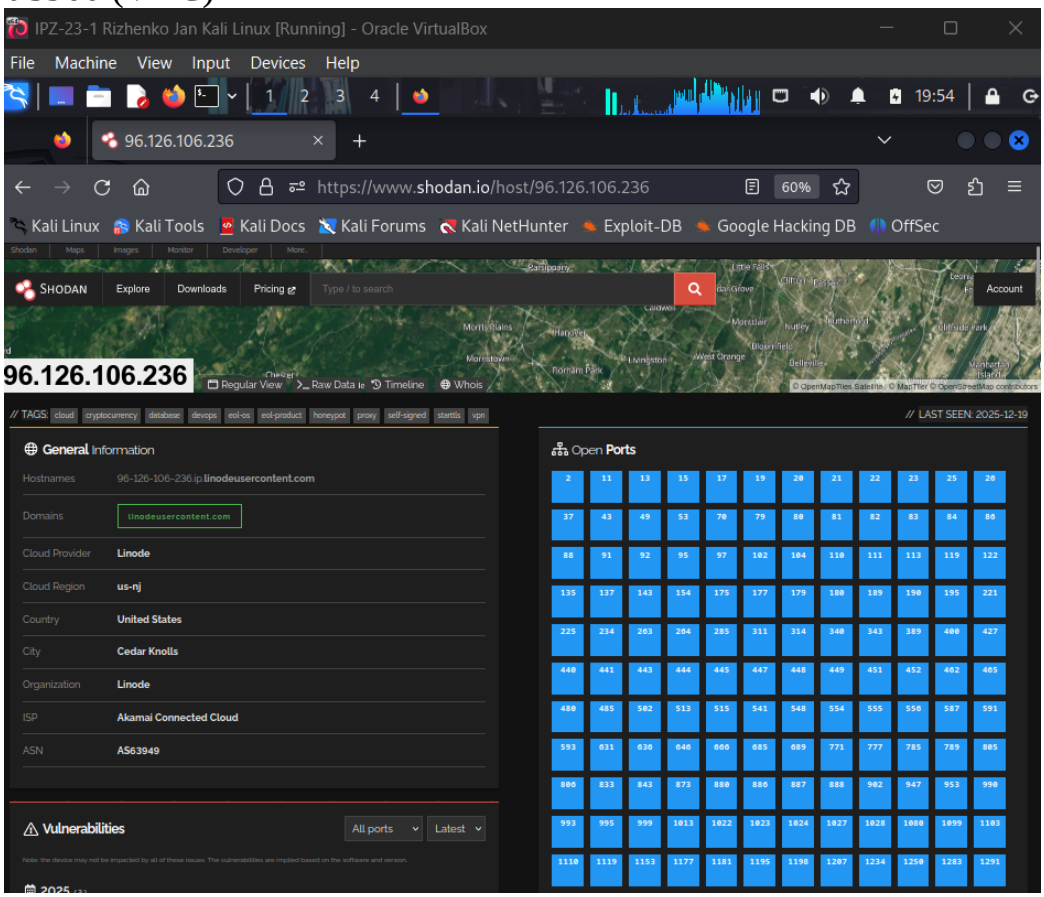

Рис. 8. Список відкритих портів та сервісів для обраного хоста(праворуч).

Питання: Яка інформація доступна для відкритих портів?
Відповідь:
Для кожного відкритого порту Shodan надає:
1. Service Banner:
   HTTP/1.1 200 OK
   Server: nginx/1.18.0
   Date: Wed, 18 Dec 2024 10:30:00 GMT
2. Protocol Information:
   - Тип протоколу (HTTP, FTP, SSH, Telnet)
   - Версія протоколу (HTTP/1.1, SSH-2.0)
3. Application Details:
   - Назва програми (Apache, nginx, OpenSSH)
   - Версія програми (Apache/2.4.41)
   - Модулі або плагіни
4. SSL/TLS Certificate (для HTTPS):
   - Issuer (видавець сертифіката)
   - Subject (кому виданий)
   - Validity period (термін дії)

- Cipher suites
- Certificate chain

5. Authentication Information:
   - Тип автентифікації (Basic, Digest, None)
   - Realm (область автентифікації)
6. Vulnerability Data (якщо є):
   - CVE numbers
   - Severity score
   - Description
7. Additional Metadata:
   - Response time
   - Data size
   - HTTP headers
   - Cookies
   - Redirects

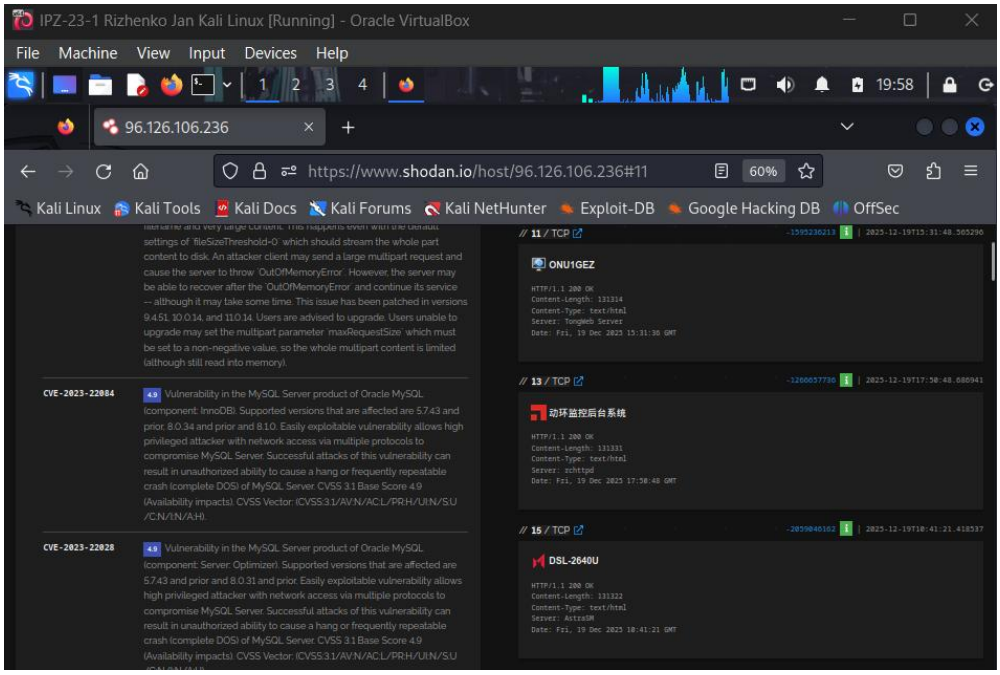

Рис. 9. Детальна інформація про відкритий порт з banner даними.

Крок 2: Використання фільтрів Shodan для уточнення результатів

Таблиця популярних фільтрів Shodan:

ФІЛЬТР	**ОПИС**	**ПРИКЛАД**
country:	Пошук за 2-літерним кодом країни	country:US
city:	Пошук за назвою міста	city:Toronto
region:	Пошук за регіоном/штатом	region:CA
product:	Пошук за назвою продукту	product:Apache
version:	Пошук за версією продукту	version:2.4
vuln:	Пошук за CVE номером	vuln:CVE-2014-0160
port:	Пошук за номером порту	port:22
os:	Пошук за операційною системою	os:Windows
hostname:	Пошук за hostname	hostname:example.com

net:	Пошук за IP діапазоном	net:192.168.1.0/24
org:	Пошук за організацією	org:"Google"
isp:	Пошук за ISP	isp:"AT&T"
asn:	Пошук за ASN	asn:AS15169
before/after:	Пошук за датою	after:01/01/2024
geo:	Пошук за координатами	geo:34.0522,-118.2437

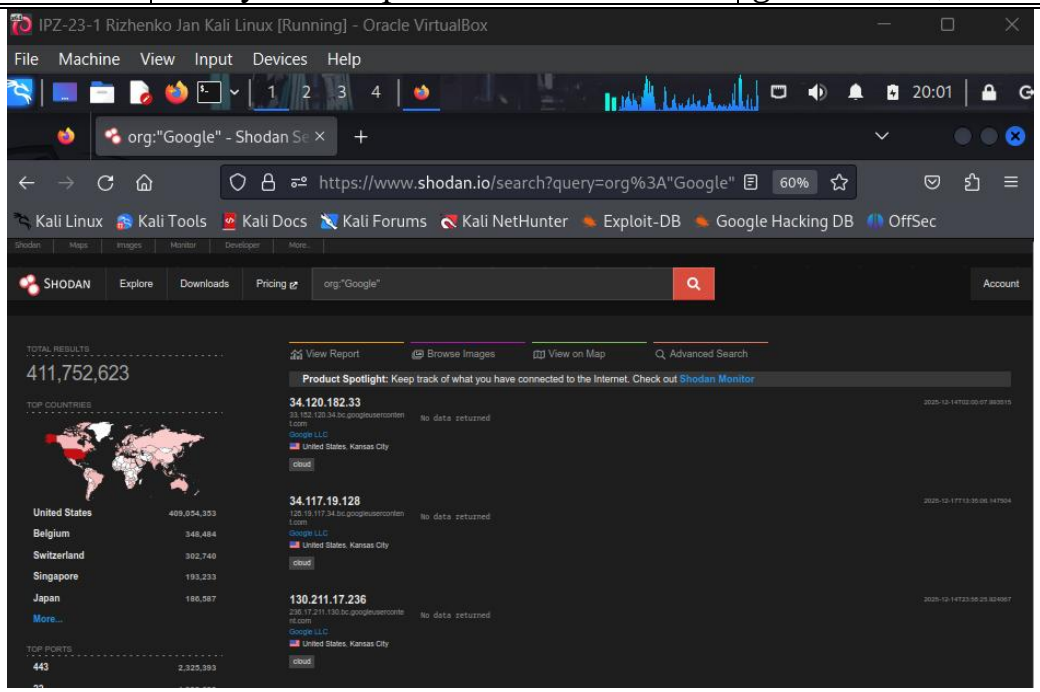

Рис. 10. Панель фільтрів Shodan та приклади використання.

Команди для пошуку:

1. Веб-камери в Toronto:

webcam city:Toronto

2. FTP сервери в San Jose з anonymous login:

port:21 country:US region:CA city:"San Jose" 230

Пояснення: 230 - це FTP response code "User logged in"

3. Apache сервери у вашому місті:

Apache port:80 city:"New York"

4. Вразливі MongoDB databases:

product:MongoDB port:27017 -authentication

5. Відкриті RDP сервери:

port:3389 country:US

6. Промислові системи управління:

tag:ics country:US

7. Сервери з вразливістю Heartbleed:

vuln:CVE-2014-0160

8. Відкриті бази даних:

product:MySQL port:3306

product:PostgreSQL port:5432

product:Redis port:6379

product:Elasticsearch port:9200

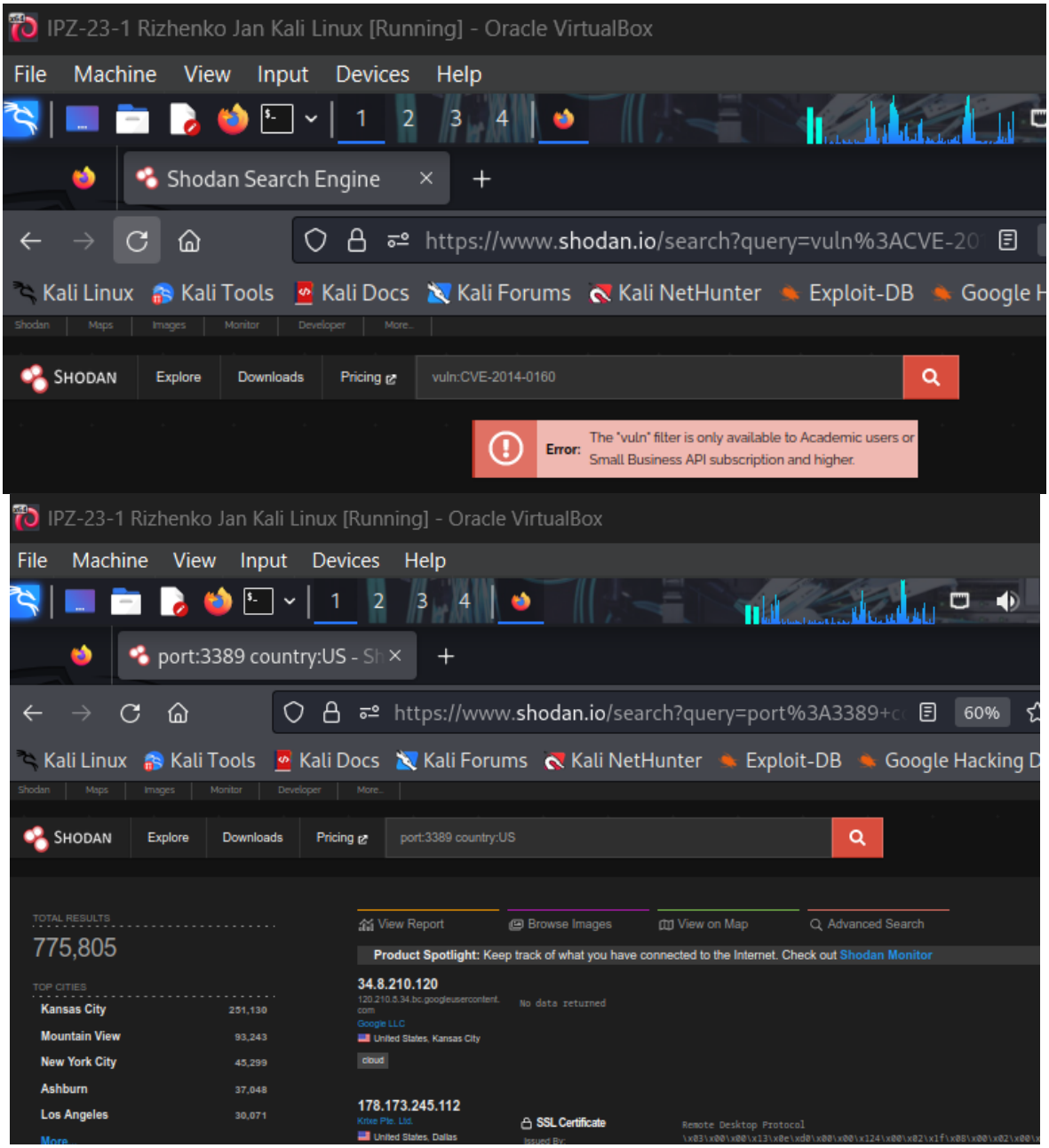

Рис. 11-12. (Результати пошуку з використанням різних фільтрів)

9. Exposed admin panels:

http.title:"Admin" country:US

http.title:"Dashboard" port:80

10. IoT пристрої зі слабкою безпекою:

"default password" port:80

"index of /" intitle:index.of

11. Хмарні інстанси:

cloud:aws

cloud:azure

cloud:gcp

12. Конкретні виробники:

org:"Hikvision"

org:"Dahua"

product:MikroTik

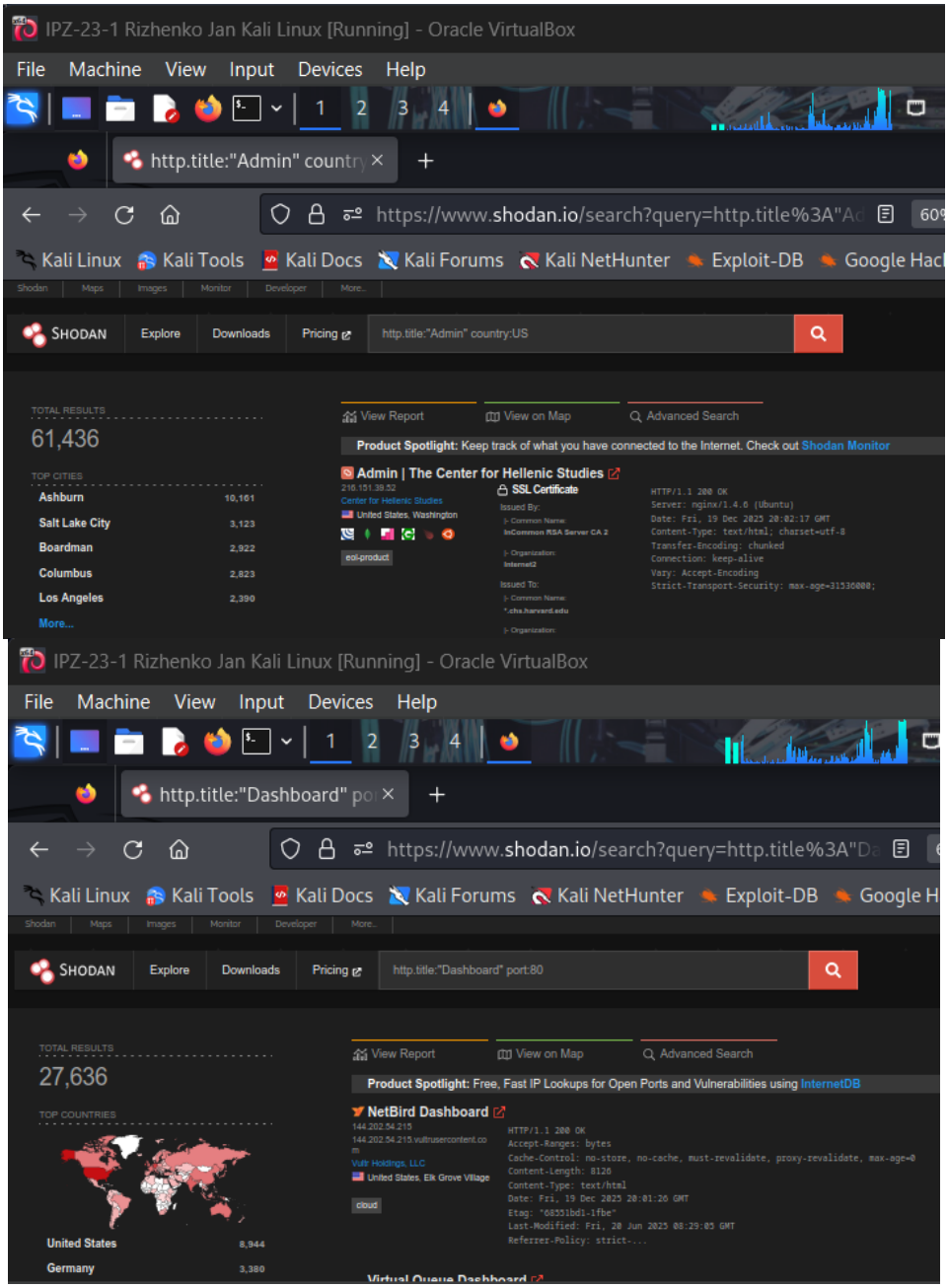

Рис. 13-14. (Приклади знайдених вразливих пристроїв)

Питання: Скільки FTP серверів знайшов Shodan у San Jose, які дозволяють anonymous login?

Відповідь:

Кількість результатів змінюється щодня, але типово: приблизно 10-50 FTP серверів.

Точна кількість залежить від:

Виправлених або вимкнених серверів

Нових вразливих серверів

Оновлень бази даних Shodan

Що означає "230" в пошуку:

FTP Response Codes:

- 220 = Service ready
- 230 = User logged in (без запиту пароля!)

- 331 = User name okay, need password
- 530 = Not logged in

Пошук "230" знаходить FTP сервери, які показали "230 User logged in" без запиту пароля = Anonymous login enabled.

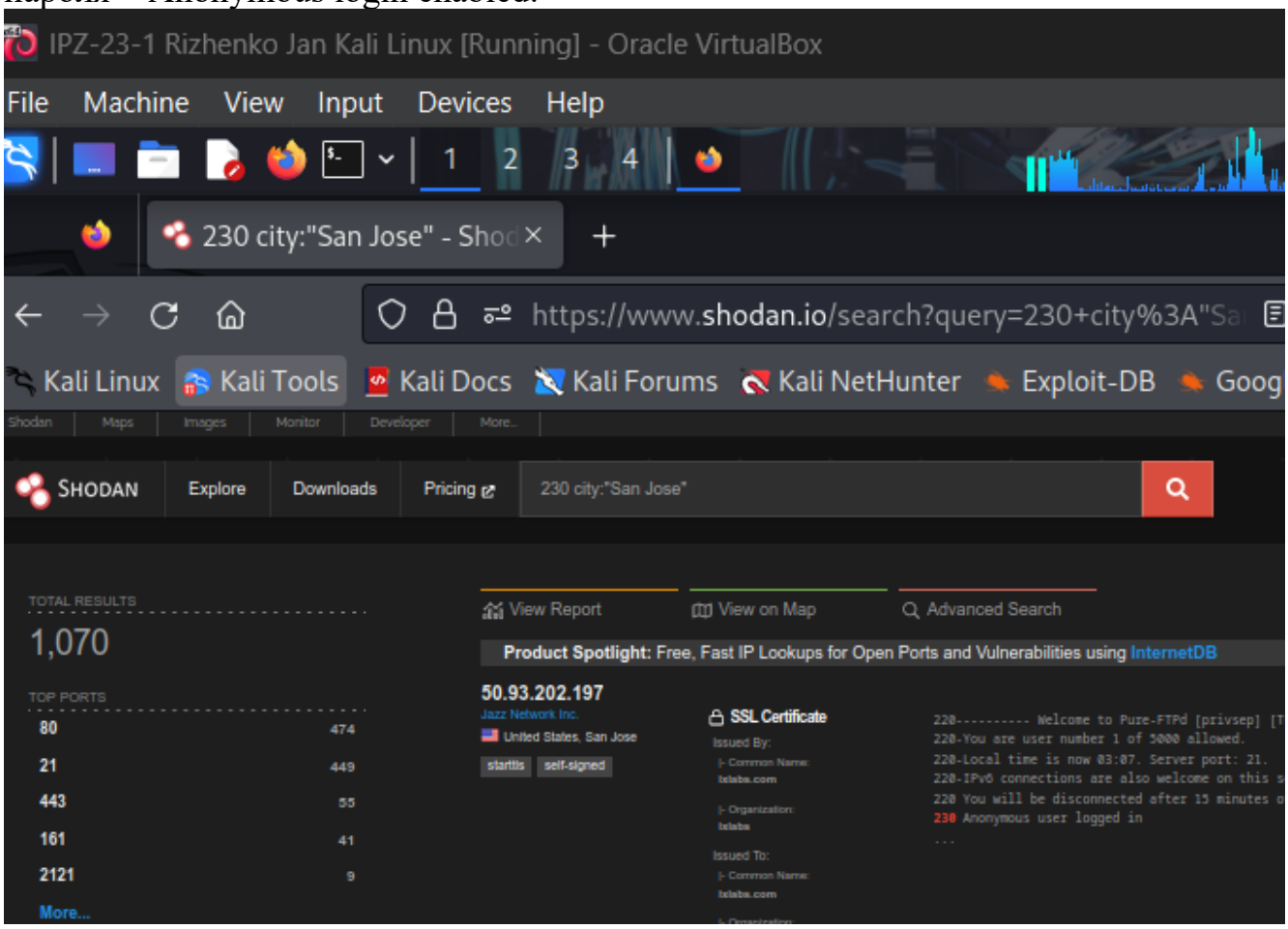

Рис. 15. Результати пошуку FTP серверів з anonymous login.

Питання: Яка додаткова інформація міститься для результатів з міткою "cloud"?

Відповідь:

Для результатів з міткою "cloud" додається:

1. Cloud Provider Information:
   - Cloud Provider (AWS, Azure, GCP, DigitalOcean)
   - Region (us-east-1, eu-west-2)
   - Service (EC2, Lambda, Cloud Functions)
2. Cloud-Specific Tags:
   - cloud:aws, cloud:azure, cloud:gcp
   - Product type (Virtual Machine, Container)
3. Additional Metadata:
   - Instance type
   - Availability Zone
   - VPC information

Крок 3: Використання Shodan для пошуку конкретного продукту або сервісу

Додаткові приклади пошуків:

1. Веб сервери:
   - product:Apache port:80 city:"London"
   - product:nginx version:1.18 country:US
   - product:"Microsoft IIS" version:10.0
2. Датабази:
   - product:MongoDB -authentication city:"New York"
   - product:MySQL port:3306 country:DE
   - product:Redis -protected-mode city:"Tokyo"
3. Інтернет девайси:
   - product:MikroTik city:"Sydney"
   - org:Cisco port:22
   - product:Ubiquiti country:CA
4. IoT девайси:
   - product:Hikvision country:US
   - org:Dahua city:"Los Angeles"
   - product:"IP Camera" port:80
5. Індустріальні системи:
   - tag:ics country:US
   - tag:scada port:502
   - product:Siemens country:DE
6. Вразливі продукти:
   - product:Apache version:2.4.49 vuln:CVE-2021-41773
   - product:OpenSSL vuln:CVE-2014-0160
   - product:WordPress city:"Paris"

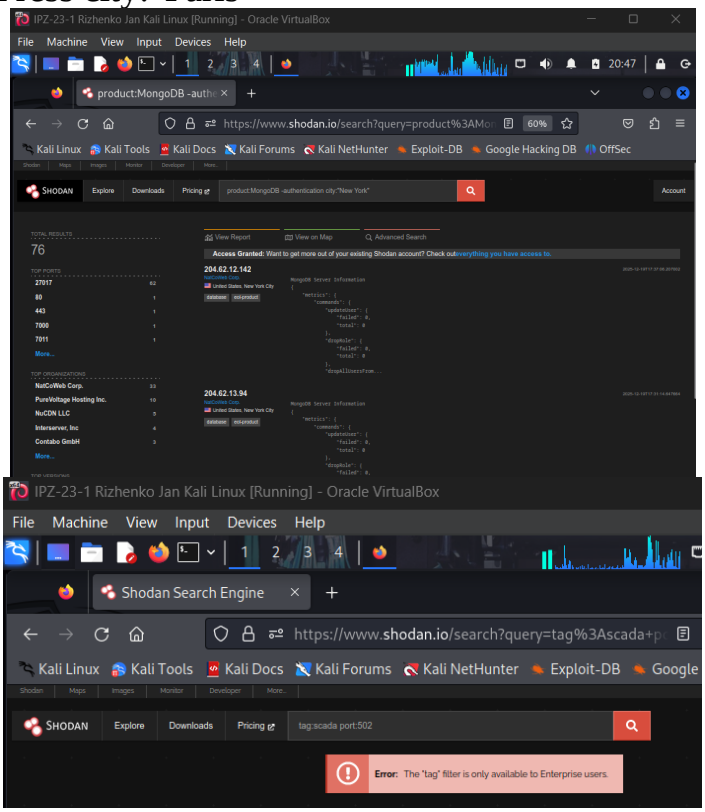

Рис. 16-17. Результати пошуку різних категорій пристроїв та сервісів.

Частина 3: Використання Shodan з командного рядка (CLI)
Крок 1: Ініціалізація Shodan та виконання пошуку
Налаштування Shodan CLI:

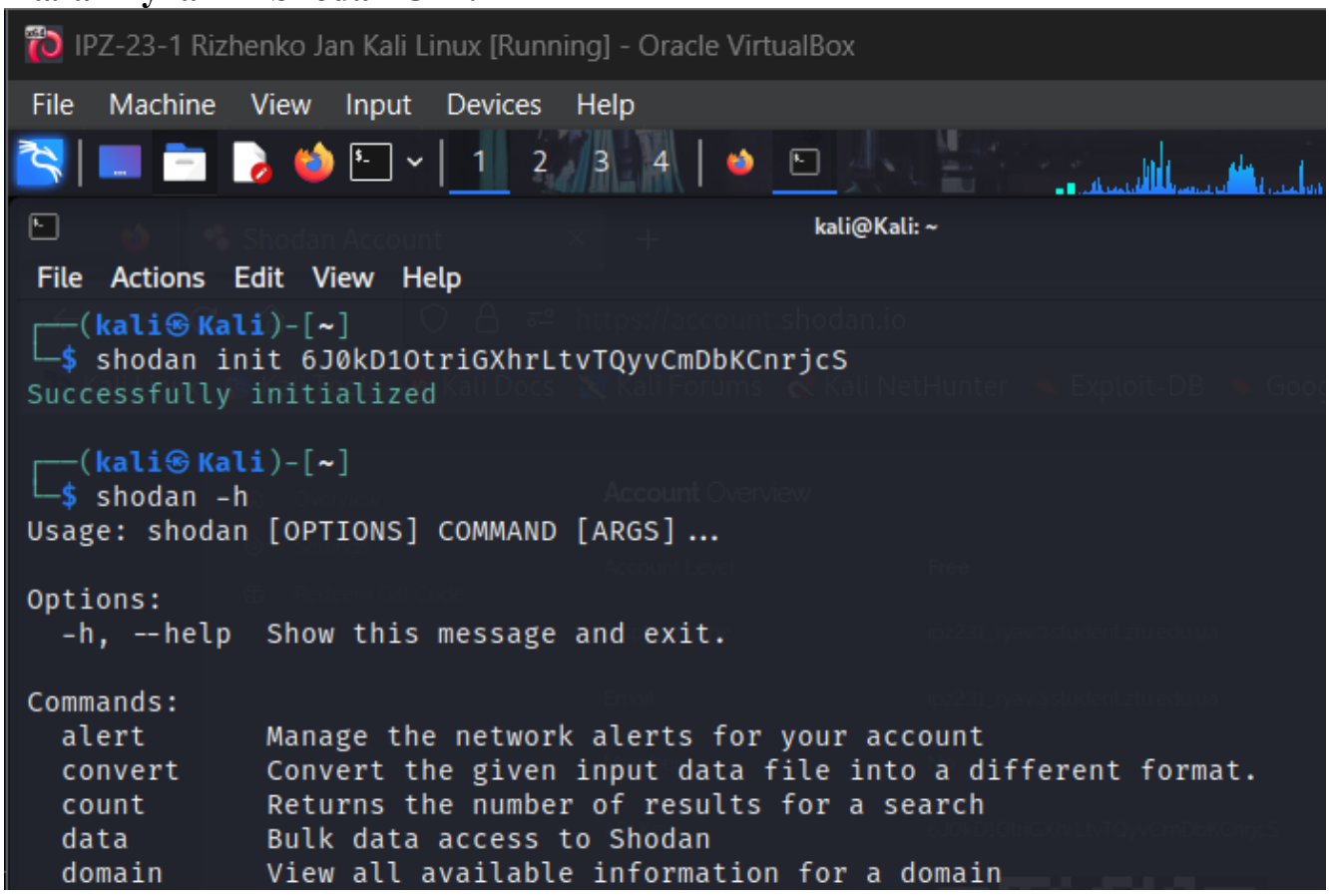

Рис. 18. Ініціалізація за API ключем(з сайту) та перегляд довідки.

Основні команди Shodan CLI:

Commands:
alert - Управління мережевим моніторингом
count - Кількість результатів
download - Завантаження результатів
host - Інформація про хост
info - Інформація про API план
init - Ініціалізація CLI
myip - Ваша зовнішня IP
search - Пошук в базі даних
stats - Статистична інформація
stream - Real-time потік данихБазовий пошук

Базові приклади:

Базовий пошук
shodan search webcam
Пошук з обмеженням
shodan search --limit 10 apache
Пошук з фільтрами
shodan search "port:22 country:US"

Інформація про хост

shodan host 8.8.8.8

Підрахунок результатів

shodan count "apache country:US"

Статистика

shodan stats "webcam"

Ваша IP адреса

shodan myip

Інформація про план

shodan info

Honeypot score

shodan honeyscore 1.2.3.4

Завантаження та парсинг даних:

Завантажити результати

shodan download --limit 100 results.json.gz apache

Парсити результати

shodan parse --fields ip_str,port,org --separator , results.json.gz

Крок 2: Виконання інших команд Shodan CLI

1. Перевірити доступні кредити:
   shodan info
2. Дізнатися свою публічну IP:
   shodan myip
3. Статистика по пошуку:
   shodan stats webcam
4. Інформація про хост:
   shodan host 8.8.8.8
5. Підрахунок результатів:
   shodan count "apache port:80"
6. Honeypot detection:
   shodan honeyscore 1.2.3.4

7. Завантаження результатів:

shodan download --limit 1000 apache_servers.json.gz "product:Apache port:80"

8. Парсинг та експорт у CSV:

shodan parse --fields ip_str,port,org,product apache_servers.json.gz

9. Експорт у CSV

shodan parse --fields ip_str,port,org --separator , apache_servers.json.gz > results.csv

10. Domain lookup:

shodan domain example.com

11. Real-time streaming:

shodan stream

Показує real-time banners по мірі сканування Shodan.

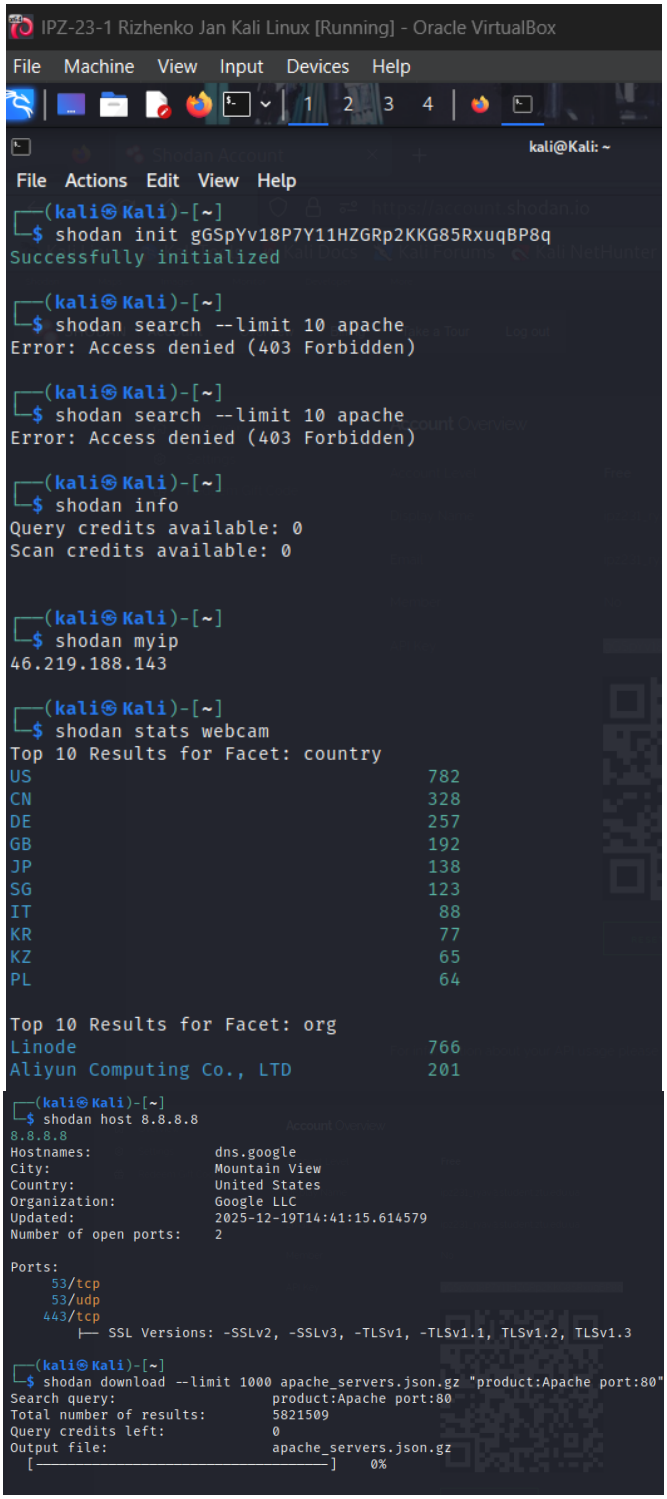

Рис. 19-20. Виконання команд Shodan CLI

Питання для рефлексії

Питання: Shodan може надати багато інформації про системи та пристрої, підключені до інтернету. Які особливості Shodan особливо цінні для IT-адміністраторів?

Відповідь:

Shodan надає надзвичайно цінні можливості для IT-адміністраторів:

1. Виявлення активів та управління інвентаризацією:

- Виявлення тіньових IT: знаходження пристроїв та сервісів, про які IT-відділ може не знати
- Картографування зовнішньої поверхні атаки: повний огляд усіх публічних IP-адрес організації
- Виявлення хмарних активів: знаходження забутих хмарних екземплярів (AWS, Azure, GCP)
- Управління постачальниками: перевірка, які треті сторони мають доступ до мережі

Приклад:
Знайти всі пристрої організації
org:"Назва компанії"
net:203.0.113.0/24

Результат може виявити:

1. Забуті тестові сервери
   - Старі екземпляри для розробки
   - Неавторизовані пристрої інтернету речей
2. Управління вразливостями:
   - Проактивне виявлення вразливостей: знаходження вразливих версій програмного забезпечення перед атакою
   - Перевірка виправлень: перевірка, чи дійсно застосовані виправлення
   - Моніторинг CVE: відстеження конкретних CVE в інфраструктурі
   - Обізнаність щодо вразливостей нульового дня: швидка ідентифікація систем, вразливих до нових загроз
3. Оцінка стану безпеки:
   - Зовнішнє тестування на проникнення: розуміння того, що бачать зловмисники
   - Моніторинг відкритості: які сервіси не потрібно відкривати для інтернету
   - Аудит налаштувань: виявлення неналаштованих сервісів
   - Перевірка відповідності вимогам: перевірка дотримання захисних протоколів
4. Реагування на інциденти та аналіз загроз:
   - Виявлення порушень: знаходження потенційно скомпрометованих систем
   - Індикатори зловмисного програмного забезпечення: пошук ознак компрометації
   - Ідентифікація ботнетів: виявлення систем, що є частиною ботнету
   - Полювання на загрози: активний пошук загроз в інфраструктурі
5. Моніторинг мережі та виявлення змін:
   - Безперервний моніторинг: регулярне сканування для виявлення змін
   - Несанкціоновані зміни: виявлення нових сервісів або портів
   - Моніторинг відповідності вимогам: автоматичне відстеження відхилень від вимог
   - Історичні дані: порівняння поточного стану з архівними даними
6. Управління ризиками третіх сторін:

- Оцінка безпеки постачальників: оцінка стану безпеки постачальників
- Безпека ланцюга постачання: моніторинг третіх сторін
- Відповідність партнерів вимогам: перевірка, що партнери дотримуються стандартів
- Належна перевірка: оцінка безпеки перед придбанням

7. Управління безпекою хмари:
   - Видимість у багатьох хмарах: огляд усіх хмарних розгортань
   - Виявлення неправильних налаштувань: відкриті сховища S3, відкриті бази даних
   - Перевірка відповідності вимогам: перевірка політик безпеки хмари
   - Оптимізація витрат: виявлення невикористовуваних ресурсів
8. Управління безпекою інтернету речей:
   - Виявлення пристроїв інтернету речей: знаходження всіх пристроїв IoT
   - Моніторинг мікропрограм: відстеження застарілих мікропрограм
   - Виявлення стандартних облікових даних: пошук пристроїв зі стандартними паролями
   - Управління життєвим циклом: відстеження пристроїв від розгортання до виведення з експлуатації
9. Відповідність вимогам та регуляторні вимоги:
   - Підготовка до аудиту: автоматизований збір доказів
   - Забезпечення політики: перевірка політик безпеки
   - Регуляторна відповідність: вимоги PCI-DSS, HIPAA, GDPR
   - Документація: автоматизована звітність для аудиторів
10. Конкурентна розвідка (легальне використання):
    - Аналіз технологічного стеку: розуміння інфраструктури конкурентів
    - Доступність сервісів: моніторинг часу роботи конкурентів
    - Стан безпеки: порівняльний аналіз
    - Ринкові тенденції: загальногалузеве впровадження технологій

Практичний приклад робочого процесу (теоретично):

Щотижневе сканування безпеки

```
COMPANY="Назва компанії"
DATE=$(date +%Y%m%d)
OUTPUT_DIR="shodan_reports/$DATE"

mkdir -p $OUTPUT_DIR
        1. Виявлення активів
shodan search "org:\"$COMPANY\"" --fields ip_str,port,product,version \
  > $OUTPUT_DIR/all_assets.txt
# 2. Перевірка вразливостей
shodan search "org:\"$COMPANY\" vuln:*" --fields ip_str,port,vulns \
  > $OUTPUT_DIR/vulnerabilities.txt
# 3. Відкриті сервіси
shodan search "org:\"$COMPANY\" port:23" > $OUTPUT_DIR/telnet.txt
```

```
shodan search "org:\"$COMPANY\" port:21" > $OUTPUT_DIR/ftp.txt
shodan search "org:\"$COMPANY\" port:3389" > $OUTPUT_DIR/rdp.txt
# 4. Відкриті бази даних
shodan search "org:\"$COMPANY\" product:MySQL" > $OUTPUT_DIR/mysql.txt
shodan search "org:\"$COMPANY\" product:MongoDB" >
$OUTPUT_DIR/mongodb.txt
# 5. Веб-додатки
shodan search "org:\"$COMPANY\" port:80" > $OUTPUT_DIR/http.txt
shodan search "org:\"$COMPANY\" port:443" > $OUTPUT_DIR/https.txt
# 6. Пристрої IoT
shodan search "org:\"$COMPANY\" tag:iot" > $OUTPUT_DIR/iot.txt
# 7. Генерування звіту
echo "Звіт з безпеки для $COMPANY - $DATE" > $OUTPUT_DIR/report.txt
echo "================================" >> $OUTPUT_DIR/report.txt
wc -l $OUTPUT_DIR/*.txt >> $OUTPUT_DIR/report.txt
# 8. Надсилання звіту команді безпеки
mail -s "Щотижневий звіт Shodan - $DATE" security@company.com <
$OUTPUT_DIR/report.txt
```

Висновок: У ході виконання лабораторної роботи було досліджено можливості Shodan - найпотужнішої пошукової системи для пристроїв інтернету речей та підключених до інтернету систем. Створено обліковий запис Shodan та отримано ключ API для програмного доступу. Вивчено веб-інтерфейс Shodan для пошуку вразливих веб-камер, відкритих баз даних, неправильно налаштованих сервісів та інших потенційно небезпечних пристроїв. Освоєно використання фільтрів (country, city, product, port, vuln) для уточнення результатів пошуку. Практично застосовано інтерфейс командного рядка Shodan для автоматизації пошуків та інтеграції з іншими інструментами безпеки. Встановлено, що Shodan надає критично важливу інформацію для IT-адміністраторів: виявлення активів, управління вразливостями, оцінку стану безпеки, моніторинг відповідності вимогам та реагування на інциденти. Робота підкреслила важливість регулярних аудитів Shodan для виявлення тіньових IT, забутих активів, неправильних налаштувань та відкритості до інтернету.