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

Команди та кроки:

firefox https://www.shodan.io/ &

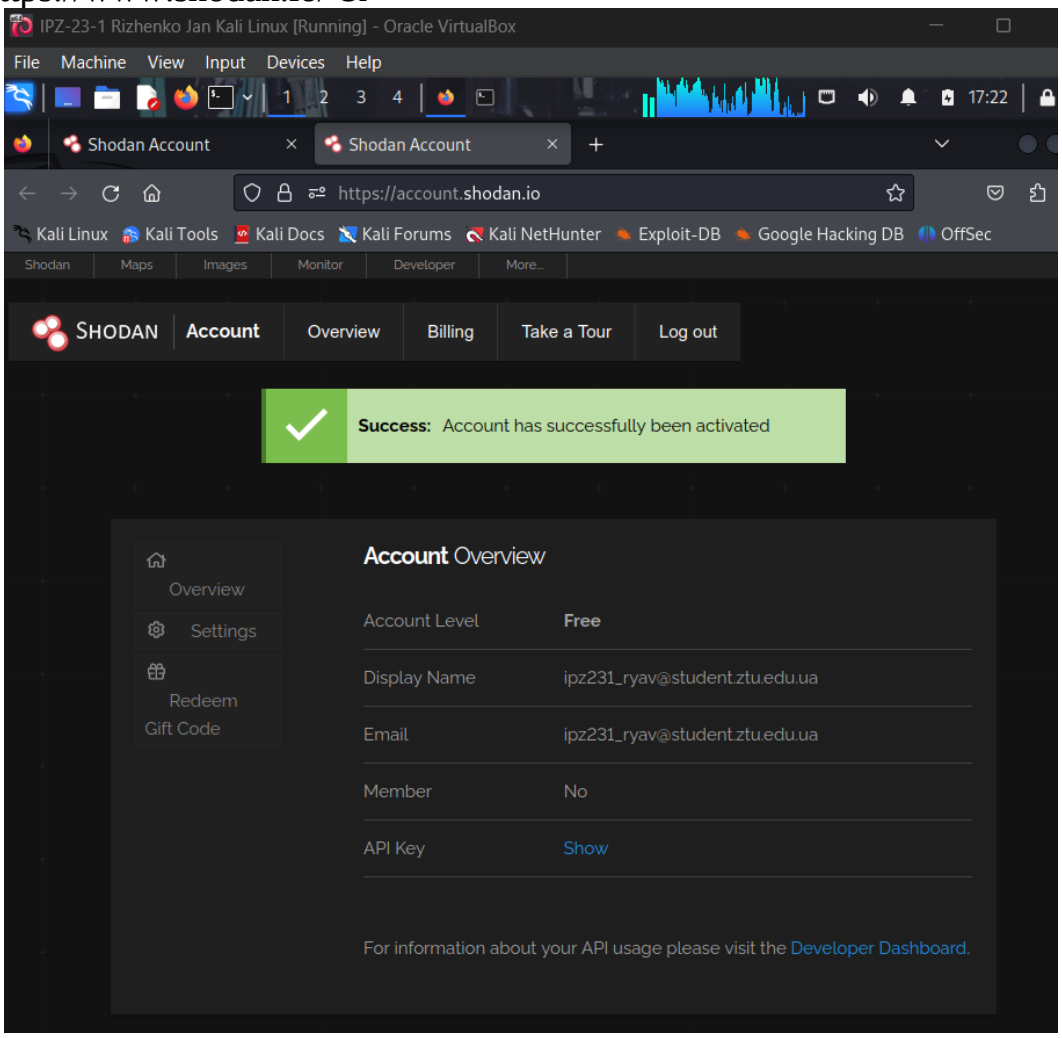

Рис. 1. Успішна реєстрація на сайті shodan.io.

Обмеження безкоштовного облікового запису:

Безкоштовний акаунт:

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

Платна підписка (від $59/місяць):
- Необмежені результати
- Розширені фільтри
- Більше API запитів
- Експорт даних
- Historical data
- Vulnerability data

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

Відповідь:

Banner - це фундаментальна одиниця даних, яку збирає Shodan.

Пояснення:

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

1. Service identification:
   - Назва програмного забезпечення (Apache, nginx, OpenSSH)
   - Версія програми (Apache/2.4.41)
   - Операційна система
2. Device information:
   - Тип пристрою (router, webcam, server)
   - Виробник (Cisco, Hikvision, Dahua)
   - Модель
3. Configuration details:
   - Відкриті порти
   - Supported protocols
   - SSL/TLS certificates

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.

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

Крок 1: Використання пошукового рядка Shodan для виявлення IoT пристроїв

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
Питання: Яка країна є топ-країною зі знайденими веб-камерами згідно Shodan?
Відповідь:
Топ-країною зазвичай 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
Примітка: Точні результати можуть варіюватися залежно від часу пошуку та оновлень бази даних Shodan.
Питання: Яка інформація міститься в розділі General Information?
Відповідь:
Розділ General Information містить:
1. Базова інформація:
- IP Address - публічна IP адреса пристрою
- Hostname - доменне ім'я (якщо є)
- ISP - інтернет-провайдер
- Organization - організація-власник IP діапазону
- ASN (Autonomous System Number) - номер автономної системи
2. Географічна інформація:
- Country - країна
- City - місто
- Region - регіон/штат
- Postal Code - поштовий індекс
- Coordinates - географічні координати (широта/довгота)
- Time Zone - часовий пояс

3. Технічна інформація:
- Ports - відкриті порти
- Services - запущені сервіси
- Operating System - операційна система (якщо виявлено)
- Last Update - дата останнього сканування
4. Додаткова інформація (якщо доступна):
- Vulnerabilities - виявлені вразливості (CVE)
- Tags - теги класифікації (webcam, database, industrial)
- Cloud Provider - хмарний провайдер (AWS, Azure, GCP)

Питання: Які порти відкриті на обраній IP адресі?

Відповідь (приклади):

Типові відкриті порти для веб-камери:
Port 80 (HTTP) - веб-інтерфейс
Port 443 (HTTPS) - захищений веб-інтерфейс
Port 554 (RTSP) - Real-Time Streaming Protocol
Port 8080 (HTTP-alt) - альтернативний веб-порт
Port 8000 - додатковий веб-сервіс
Port 37777 - Dahua DVR порт
Port 9000 - специфічний для виробника
Інші типові порти для різних пристроїв:
FTP Server:
- Port 21 (FTP)
- Port 20 (FTP Data)

SSH Server:
- Port 22 (SSH)

Database:
- Port 3306 (MySQL)
- Port 5432 (PostgreSQL)
- Port 27017 (MongoDB)

Web Server:
- Port 80 (HTTP)
- Port 443 (HTTPS)
- Port 8080, 8000, 8888 (alternatives)

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

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

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

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 в вашому місті
Apache port:80 city:"New York"
4. Vulnerable MongoDB databases
product:MongoDB port:27017 -authentication
5. Exposed RDP servers
port:3389 country:US
6. Telnet services (insecure)
port:23 country:DE
7. Webcams з default credentials
webcam "admin:admin"
8. Industrial Control Systems
tag:ics country:US
9. Vulnerable Heartbleed servers
vuln:CVE-2014-0160
10. Exposed databases
product:MySQL port:3306
product:PostgreSQL port:5432
product:Redis port:6379
product:Elasticsearch port:9200
11. Exposed admin panels
http.title:"Admin" country:US
http.title:"Dashboard" port:80
12. IoT devices з weak security
"default password" port:80
"index of /" intitle:index.of
13. Cloud instances
cloud:aws
cloud:azure
cloud:gcp
14. Honeypots
tag:honeypot
15. Specific vendors
org:"Hikvision"
org:"Dahua"
product:MikroTik

Питання: Скільки FTP серверів знайшов Shodan у San Jose, які дозволяють anonymous login?
Відповідь:
Кількість результатів буде залежати від поточного стану інтернету, але типово:
Приблизно 10-50 FTP серверів з anonymous login у San Jose.
Примітка: Точна кількість змінюється щодня, оскільки:
- Сервери можуть бути виправлені або вимкнені
- Нові вразливі сервери з'являються
- Shodan постійно оновлює свою базу даних
Що означає "230" в пошуку:
FTP Response Codes:
- 220 = Service ready
- 230 = User logged in, proceed
- 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
Питання: Яка додаткова інформація міститься в розділі General Information для результатів з міткою "cloud" порівняно з результатом, записаним у Кроці 1c?
Відповідь:
Для результатів з міткою "cloud" додається:
1. Cloud Provider Information:
- Cloud Provider - назва провайдера (AWS, Azure, GCP, DigitalOcean)
- Region - хмарний регіон (us-east-1, eu-west-2)
- Service - тип сервісу (EC2, Lambda, Cloud Functions)
2. Cloud-Specific Tags:
- cloud:aws, cloud:azure, cloud:gcp
- Product type (Virtual Machine, Container, Serverless)
3. Organization Details:
- Більш детальна інформація про організацію
- ASN частіше пов'язаний з cloud provider
4. Additional Metadata:
- Instance type (якщо відомо)
- Availability Zone
- VPC information (іноді)
Приклад порівняння:
Regular Device:
- Organization: Comcast Cable
- ASN: AS7922
- Hostname: c-67-123-45-67.hsd1.ca.comcast.net
- Tags: webcam

Cloud Device:
- Organization: Amazon Technologies Inc.
- ASN: AS16509
- Hostname: ec2-54-123-45-67.compute-1.amazonaws.com
- Tags: cloud, aws, webcam
- Cloud: AWS
- Region: us-east-1

Крок 3: Використання Shodan для пошуку конкретного продукту або сервісу

Додаткові приклади пошуків:

Web servers

product:Apache port:80 city:"London"
product:nginx version:1.18 country:US
product:"Microsoft IIS" version:10.0

Databases

product:MongoDB -authentication city:"New York"
product:MySQL port:3306 country:DE
product:Redis -protected-mode city:"Tokyo"

Network devices

product:MikroTik city:"Sydney"
org:Cisco port:22
product:Ubiquiti country:CA

IoT devices

product:Hikvision country:US
org:Dahua city:"Los Angeles"
product:"IP Camera" port:80

Industrial systems

tag:ics country:US
tag:scada port:502
product:Siemens country:DE

Vulnerable products

product:Apache version:2.4.49 vuln:CVE-2021-41773
product:OpenSSL vuln:CVE-2014-0160
product:WordPress city:"Paris"

Частина 3: Використання Shodan з командного рядка (CLI)

Крок 1: Ініціалізація Shodan та виконання пошуку

Команди для налаштування Shodan CLI:

Account → Overview → API Key (скопіювати)

1. Ініціалізувати Shodan з API ключем

shodan init YOUR_API_KEY_HERE

Вивід: Successfully initialized

2. Переглянути довідку

shodan -h

Основні команди Shodan CLI:

Переглянути всі команди

```
shodan -h
Usage: shodan [OPTIONS] COMMAND [ARGS]...
Commands:
  alert       Manage network monitoring alerts
  convert     Convert file between formats
  count       Returns the number of results
  data        Bulk data access
  domain      View domain information
  download    Download search results
  honeyscore  Check honeypot probability
  host        View all available information
  info        Show API plan information
  init        Initialize the CLI
  myip        Print your external IP address
  org         Manage organization
  parse       Extract information from files
  radar       Real-time map of some results
  scan        Scan an IP/netblock
  search      Search the Shodan database
  stats       Provide summary information
  stream      Stream data in real-time
  version     Print version information
```

Базовий пошук

```
shodan search webcam
```

Пошук з обмеженням результатів

```
shodan search --limit 10 apache
```

Пошук з фільтрами (потрібна платна підписка)

```
shodan search "port:22 country:US"
```

Отримати інформацію про конкретний хост

```
shodan host 8.8.8.8
```

Підрахувати результати

```
shodan count "apache country:US"
```

Статистика по пошуку

```
shodan stats "webcam"
```

Дізнатися свою IP адресу

```
shodan myip
```

Переглянути інформацію про API план

```
shodan info
```

Honeypot score

```
shodan honeyscore 1.2.3.4
```

Завантажити результати у файл

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

Парсити завантажені результати

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

Крок 2: Виконання інших команд Shodan CLI
Детальні приклади команд:
1. Перевірити доступні кредити
shodan info
Query credits available: 0
Scan credits available: 0
Unlocked: false
Plan: Free
HTTPS API: true
Telnet: false
DNS: false
2. Дізнатися свою публічну IP
shodan myip
203.0.113.45
3. Статистика по пошуку
shodan stats webcam
Top 10 Countries:
United States: 45678
China: 23456
Germany: 12345

Top 10 Organizations:
Comcast Cable: 8765
AT&T: 5432

Top 10 Operating Systems:
Linux: 34567
Windows: 12345

4. Інформація про конкретний хост
shodan host 8.8.8.8

8.8.8.8
City: Mountain View
Country: United States
Organization: Google LLC
Operating System: None
Ports: 53, 443
Hostnames: dns.google

5. Підрахунок результатів
shodan count "apache port:80"
12345678

6. Honeypot detection
shodan honeyscore 1.2.3.4
0.8
Score від 0.0 до 1.0, де 1.0 = ймовірно honeypot
7. Завантаження результатів
shodan download --limit 1000 apache_servers.json.gz "product:Apache port:80"
8. Парсинг завантажених даних
shodan parse --fields ip_str,port,org,product apache_servers.json.gz
Експорт у CSV
shodan parse --fields ip_str,port,org --separator , apache_servers.json.gz > results.csv
9. Domain lookup
shodan domain example.com
10. Streaming (real-time results)
shodan stream
Показує real-time banners по мірі сканування Shodan
Автоматизація з Python:

```
!/usr/bin/env python3
 shodan_search.py
import shodan
 API Key
API_KEY = "YOUR_API_KEY_HERE"
api = shodan.Shodan(API_KEY)
 Базовий пошук
try:
    results = api.search('apache')

    print(f'Results found: {results["total"]}')

    for result in results['matches']:
        print(f'IP: {result["ip_str"]}')
        print(f'Port: {result.get("port", "N/A")}')
        print(f'Organization: {result.get("org", "N/A")}')
        print(f'Location: {result.get("location", {}).get("city", "N/A")}')
        print('---')
except shodan.APIError as e:
    print(f'Error: {e}')
 Host lookup
try:
    host = api.host('8.8.8.8')
    print(f'IP: {host["ip_str"]}')
    print(f'Organization: {host.get("org", "N/A")}')
    print(f'Operating System: {host.get("os", "N/A")}')
    for item in host['data']:
        print(f'Port: {item["port"]}')
```

```
        print(f'Banner: {item["data"]}')
except shodan.APIError as e:
    print(f'Error: {e}')
 Count results
try:
    count = api.count('apache country:US')
    print(f'Total Apache servers in US: {count["total"]}')

except shodan.APIError as e:
    print(f'Error: {e}')

 My IP
try:
    my_ip = api.tools.myip()
    print(f'My IP: {my_ip}')

except shodan.APIError as e:
    print(f'Error: {e}')
```

Запуск Python скрипта:

Зробити виконуваним

```
chmod +x shodan_search.py
```

Запустити

```
python3 shodan_search.py
```

Додаткові корисні техніки

Розширені пошукові запити:

Комбінування множинних фільтрів

```
port:80 product:Apache country:US city:"New York" version:2.4
```

Boolean operators

```
(product:Apache OR product:nginx) port:80
```

Негативний пошук

```
apache -country:US
port:22 -product:OpenSSH
```

Wildcard search

```
hostname:*.example.com
```

IP range

```
net:192.168.1.0/24
```

Specific ASN

```
asn:AS15169
```

SSL certificate search

```
ssl.cert.subject.cn:example.com
ssl.cert.issuer.cn:"Let's Encrypt"
```

HTTP-specific

```
http.title:"Dashboard"
http.html:admin
```

http.status:200
Vulnerable versions
product:Apache version:2.4.49
product:OpenSSL version:1.0.1
Tags
tag:compromised
tag:malware
tag:tor
tag:vpn
tag:proxy

Інтеграція з іншими інструментами:

Комбінування з nmap

```
shodan search "port:22" --fields ip_str --limit 100 > ips.txt
nmap -iL ips.txt -p 22 -sV
```

Експорт у формат для Metasploit

```
shodan parse --fields ip_str,port results.json.gz | awk '{print $1":"$2}' > msf_targets.txt
```

Використання з curl

```
curl -s "https://api.shodan.io/shodan/host/8.8.8.8?key=YOUR_API_KEY" | jq .
```

Використання з nuclei для vulnerability scanning

```
shodan download results.json.gz "product:WordPress"
shodan parse --fields ip_str results.json.gz > wordpress_ips.txt
nuclei -l wordpress_ips.txt -t wordpress/ -o vulnerabilities.txt
```

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:

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

Приклад:

Знайти системи, вразливі до Log4Shell

org:"Назва компанії" product:Java vuln:CVE-2021-44228

Знайти незахищені бази даних

org:"Назва компанії" product:MongoDB -authentication

Знайти старі версії

org:"Назва компанії" product:Apache version:2.4.49

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

Приклад:

Знайти відкриті адміністративні панелі

org:"Назва компанії" intitle:admin

org:"Назва компанії" http.title:"Dashboard"

Знайти незахищені протоколи

org:"Назва компанії" port:23 # Telnet

org:"Назва компанії" port:21 # FTP

Знайти стандартні облікові дані

org:"Назва компанії" "default password"

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

Приклад:

Знайти потенційно скомпрометовані системи

org:"Назва компанії" tag:malware

org:"Назва компанії" tag:compromised

Знайти сервери командування та управління

org:"Назва компанії" "command and control"

Виявлення медових горщиків
shodan honeyscore <IP_АДРЕСА>
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

Приклад:
Налаштування системних попереджень (Shodan Monitor)
Сповіщення електронною поштою при:
- Нових відкритих портах
- Змінах в SSL-сертифікатах
- Виявленні вразливостей
- Появі нових пристроїв

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

Приклад:
Оцініть безпеку постачальника
org:"Назва постачальника"
org:"Компанія-партнер"
Перевірка на вразливості
org:"Назва постачальника" vuln:*
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

Приклад:
Знайти хмарні ресурси
cloud:aws org:"Назва компанії"
cloud:azure org:"Назва компанії"
Знайти відкриті хмарні сховища
org:"Назва компанії" product:"Amazon S3"
org:"Назва компанії" "azure blob storage"
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

Приклад:
Знайти пристрої IoT
org:"Назва компанії" product:camera
org:"Назва компанії" product:printer
org:"Назва компанії" tag:iot
Знайти пристрої з відомими проблемами
org:"Назва компанії" product:Hikvision
org:"Назва компанії" "default password"

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

Приклад:
Перевірка відповідності PCI-DSS
org:"Назва компанії" port:3389 # Без відкритого RDP
org:"Назва компанії" ssl.version:SSLv3 # Без старого SSL
Відповідність HIPAA
org:"Медична організація" port:3306 # Без відкритих баз даних

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:
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
```

Shodan є незамінним інструментом для сучасних IT-адміністраторів, оскільки він:

- Надає безперервну видимість усієї зовнішньої поверхні атаки
- Дозволяє проактивну безпеку замість реактивної
- Забезпечує автоматизований моніторинг та сповіщення
- Допомагає з відповідністю вимогам та регуляторними вимогами
- Економить час та ресурси через автоматизацію
- Надає аналіз загроз для прийняття обґрунтованих рішень

Shodan перетворює безпеку з "реактивного гасіння пожеж" на "проактивне управління ризиками".

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.