Лабораторна робота 1 – Пошук ІоТ вразливостей на Shodan search engine

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Цілі

Part 1: Отримати доступ до можливостей Shodan search engine, які надаються на безоплатній основі.

Part 2: Дослідити активні IoT пристрої

1. Background / Scenario

**Попередження**: Не намагайтеся ввійти на будь-який пристрій, який ви знайдете в пошуковій системі Shodan. Це порушує вашу угоду про етичне хакерство.

У цій лабораторній роботі ви будете використовувати пошукову систему Shodan, щоб зрозуміти, чому безпека повинна бути в центрі уваги будь-якої реалізації IoT.

Shodan має сервери, розташовані по всьому світу, які постійно сканують Інтернет у пошуках підключених пристроїв. Він може знайти конкретні пристрої та типи пристроїв. Потім ці дані можуть отримати клієнти цього сервісу. Деякі з найбільш популярних пошукових запитів містять такі терміни, як "webcam", "default passwords", "routers", "video games" тощо.

Shodan є популярним інструментом, який використовують дослідники, спеціалісти з безпеки, великі підприємства та команди реагування на комп’ютерні надзвичайні ситуації (CERT):

* Дослідники можуть використовувати Shodan для отримання інформації про те, які пристрої підключені, де вони підключені та які служби на них доступні.
* Професіонали з безпеки можуть використовувати Shodan як частину плану тестування на проникнення, щоб виявити пристрої, які потрібно захищати для запобігання потенційним атакам.
* На великих підприємствах працюють професіонали з безпеки, які повинні знати такі інструменти, як Shodan, для визначення поточного профілю ризику підключених пристроїв підприємства.
* CERT можуть використовувати Shodan для швидкого створення звітів про нову атаку на підключені пристрої.

Shodan також є інструментом, який використовують хакери. Shodan може прискорити атаку розвідку зловмисником пристроїв, підключених до Інтернету. Як і всі інструменти в цьому курсі, ви повинні використовувати його відповідально.

1. Необхідні ресурси
* ПК з доступом до Інтернету
* SANS Penetration Testing стаття, “[Getting the Most Out of Shodan Searches](https://www.sans.org/blog/getting-the-most-out-of-shodan-searches/)”
1. Доступ до можливостей Shodan search engine, які надаються на безоплатній основі
	* + 1. Створіть обліковий запис на сайті Shodan https://www.shodan.io/.
			2. Увійдіть до свого акаунту, натисніть лінк **Shodan** щоб повернутись на головну сторінку.



Опишіть можливості, які надає цей сервіс на безоплатній основі, які контракті плани доступні і які вони мають переваги

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Дослідження активних ІоТ пристроїв
	* 1. Використання можливостей Shodan search engine.

З головної сторінки Ви можете використовувати ключові слова в полі пошуку.

* + - 1. Зробіть пошук для слова **cisco**. Прокоментуйте результати, наведіть скріншоти.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + - 1. З правої сторони головна секція результатів Вашого пошуку показує пристрої, які відповідають критеріям пошуку. Знайдіть елемент, який виглядає для Вас цікавим і заповніть наступну інформацію про нього:

IP address:

Hostname:

ISP:

Date the entry was added:

Country:

Додайте скріншот:



* + - 1. Ваш елемент також може відображати деяку інформацію про банер. Ви можете побачити початок банера SSH або банера HTTP. Натисніть **Details**, щоб дізнатися більше про цей елемент. Ви повинні побачити кілька відкритих портів. Якщо ні, спробуйте інший елемент. Запишіть нижче інформацію, яку ви знайшли:

City and Country:

Ports open:

Services running:

Key types:

* + - 1. Поверніться на головну сторінку сервісу та натисніть **Explore**. Яку інформацію можна отримати на цій сторінці?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. Знайдіть і прокоментуйте інформацію про стан ІоТ в Україні та порівняйте з іншою країною на Ваш вибір. Додайте скріншоти.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_





* + - 1. У полі пошуку введіть ключове слово “**default password**” у лапках і натисніть Enter. Який ваш результат? Додайте скріншот.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + - 1. У полі пошуку введіть ключове слово “webcam” у лапках і натисніть Enter. Який ваш результат? Додайте скріншот.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + - 1. У полі пошуку введіть ключове слово “refrigerator” у лапках і натисніть Enter. Який ваш результат? Додайте скріншот.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + 1. Використовуйте ключові слова разом із пошуковими операторами, щоб відфільтрувати пошук.

Можливо, ви помітили, що з безкоштовним доступом до облікового запису ви можете отримати лише дві сторінки результатів. Однак навіть з платним обліковим записом ви не захочете переглядати сторінки, які містять тисячі чи мільйони результатів. Натомість ви можете комбінувати ключові слова та оператори пошуку, щоб фільтрувати результати.

Shodan шукає служби, запущені на пристрої. Потім він збирає інформацію про банери для кожної служби. Наприклад, ось інформація про банер для служби SNMP, що працює на пристрої Cisco, знайдена за допомогою пошуку Shodan:

Cisco Internetwork Operating System Software

IOS (tm) 7200 Software (UBR7200-IK9SU2-M), Version 12.3(23)BC10, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2011 by cisco Systems, Inc.

Пошук лише за словом «cisco», швидше за все, покаже вам від одного до двох мільйонів результатів. Ця інформація може бути вам корисною. Однак, якщо вас цікавить більш конкретна інформація, ви захочете відфільтрувати свій пошук, використовуючи назви фільтрів і значення з інформації про банер.

Наприклад, якщо вам цікаво дізнатися, скільки маршрутизаторів Cisco 7200 у Сполучених Штатах використовують службу SNMP, ви повинні ввести таку пошукову фразу.

country:US product:"Cisco 7200 Router" port:161

**Note**: Shodan searches use the two letter (alpha-2) country code based on the International Standards Organization’s 3166 publication (ISO 3166-1993).

**Створіть власні запити, щоб знайти наступне:**

* + - 1. Minecraft — це популярна відеогра, де гравці можуть налаштувати власні сервери, щоб інші мали доступ до них онлайн. Використовуйте пошук в Інтернеті, щоб знайти наступну інформацію.

Який загальний номер порту використовують сервери Minecraft? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Який ISO 3166 alpha-2 code для Південної Африки? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Яку пошукову фразу Shodan можна використати, щоб дізнатися, скільки серверів Minecraft зараз онлайн у Південній Африці?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Скільки серверів Minecraft зараз онлайн у Південній Африці? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + - 1. Moxa є постачальником пристроїв для підключення промислового обладнання до Інтернету. Скільки пристроїв Moxa використовують службу Telnet у Бразилії?

Пошукова фраза: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Отримані результати: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + - 1. Існує багато домашніх пристроїв, підключених і керованих за допомогою IoT. Застосуйте методи, які раніше використовували для пошуку “garage door” в штаті Мічиган у Сполучених Штатах. Який рядок пошуку ви використовували? Наведіть скріншоти результатів

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Скільки результатів було отримано?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Яке місто має найбільше підключених гаражних воріт?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Які потенційні ризики того, що хтось має доступ до цієї інформації?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



* + - 1. Запропонуйте своє завдання для пошуку та надайте опис його виконання

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

