Shodan使用與尋找漏洞示範

NASOC 二線工程師 林宜進

E-mail：tjline01@asoc.cc.ntu.edu.tw

日期：2020/07/30

虛擬機下載連結

- Google雲端連結：https://ppt.cc/fN6sex
- 檔案約4GB
- 虛擬機檔案下載時間到2020/12/31
- 虛擬機的帳號密碼：user / Shodan_vm

大綱

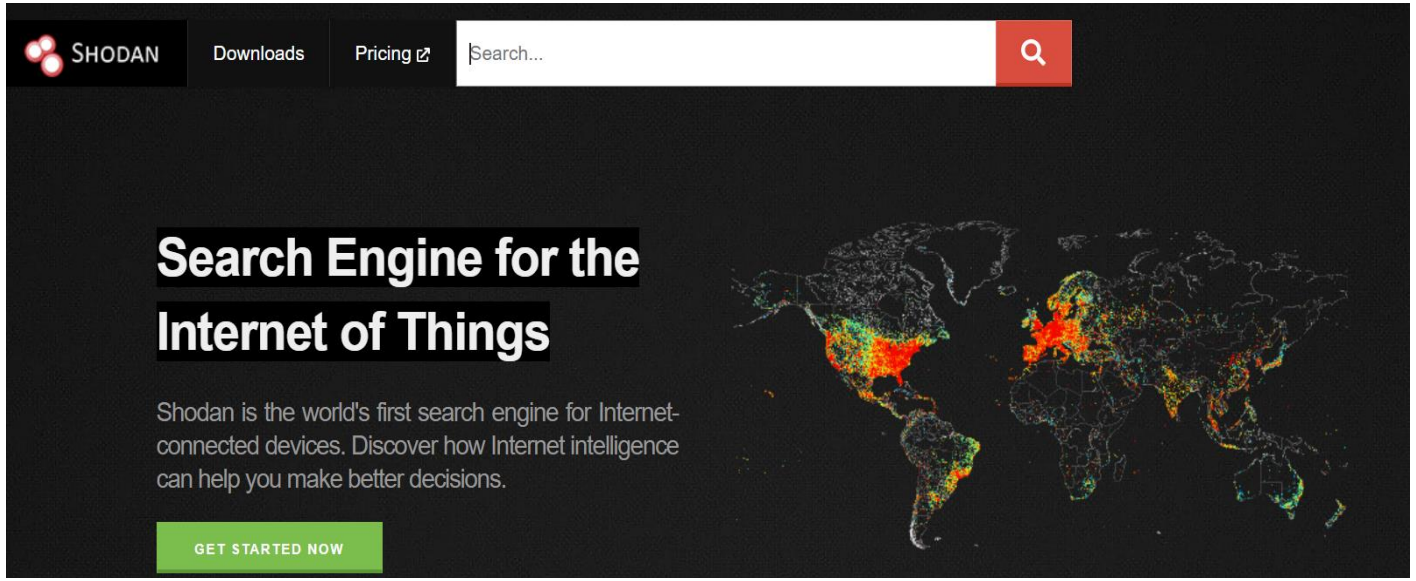
1. 基本介紹
2. 搜尋資料方式介紹與操作
3. 近期研究的漏洞內容
4. 搜尋和驗證示範
5. 資料來源
6. Q&A

基本介紹

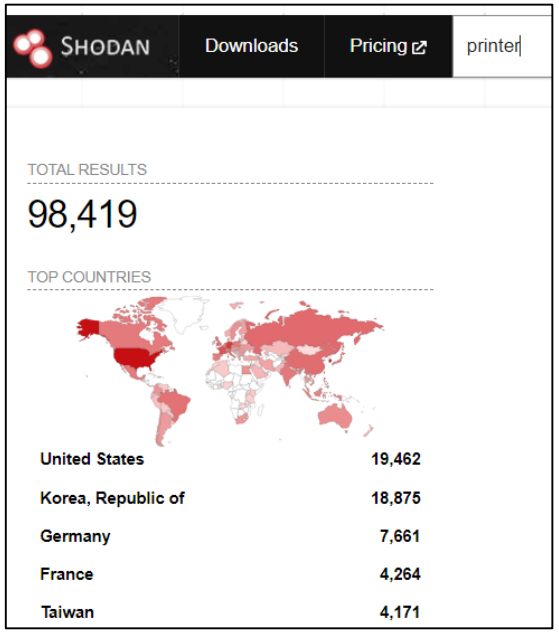
簡易的說明SHODAN與其資料

前言

- Shodan是一個搜尋引擎，主要是尋找網路上的IoT設備
- 利用搜尋語法找出特定的IoT設備(例如：Webcam、Printer、Router、NAS)

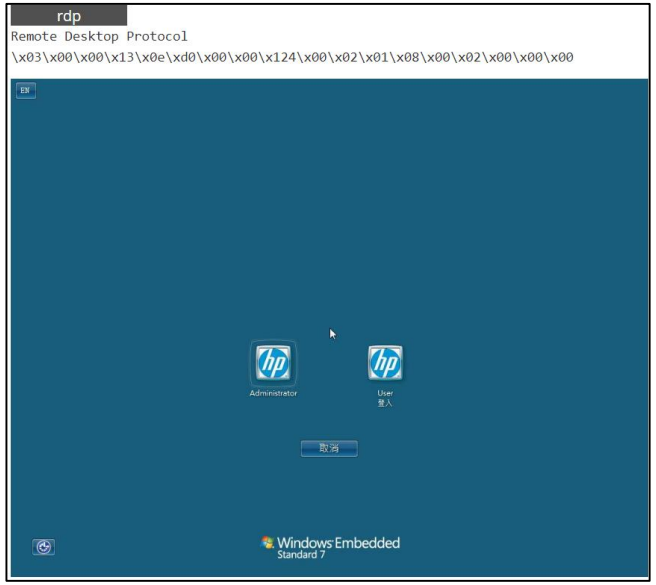


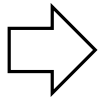
資料來源：https://beta.shodan.io/



資料說明

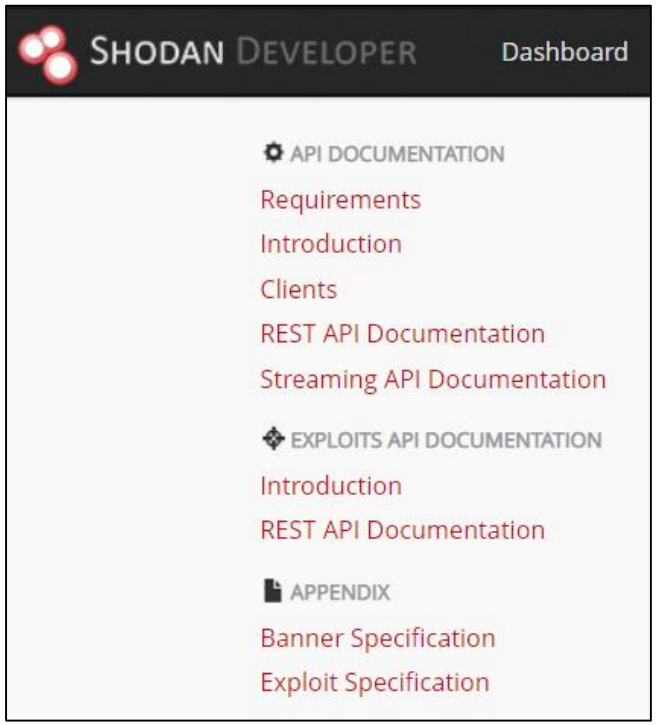
- Shodan每一筆收集到的資料稱為banner，而banner主要是文字記錄該服務的相關內容
- 資料收集的頻率是全年無休；爬蟲伺服器分布全世界各地





banner資料說明

- 在Shodan Developer的Banner Specification頁面，有定義資料的內容



資料來源：https://developer.shodan.io/api/banner-specification

Banner Specification

The banner is the main type of information that Shodan provides through the REST and Streaming API. This document outlines the various properties that are always present and which ones are optional.

Properties

asn	[String] The autonomous system number (ex. "AS4837").
data	[String] Contains the banner information for the service.
ip	[Integer] The IP address of the host as an integer.
ip_str	[String] The IP address of the host as a string.
ipv6	[String] The IPv6 address of the host as a string. If this is present then the "ip" and "ip_str" fields wont be.
port	[Integer] The port number that the service is operating on.
timestamp	[String] The timestamp for when the banner was fetched from the device in the UTC timezone. Example: "2014-01-15T05:49:56.283713"
hostnames	[String[]] An array of strings containing all of the hostnames that have been assigned to the IP address for this device.
domains	[String[]] An array of strings containing the top-level domains for the hostnames of the device. This is a utility property in case you want to filter by TLD instead of subdomain. It is smart enough to handle global TLDs with several dots in the domain (ex. "co.uk")
location	[Object] An object containing all of the location information for the device.
location.area_code	[Integer]The area code for the device's location. Only available for the US.
location.city	[String] The name of the city where the device is located.
location.country_code	[String] The 2-letter country code for the device location.
location.country_code3	[String] The 3-letter country code for the device location.
location.country_name	[String] The name of the country where the device is located.
location.dma_code	[Integer] The designated market area code for the area where the device is located. Only available for the US.
location.latitude	[Double] The latitude for the geolocation of the device.
location.longitude	[Double] The longitude for the geolocation of the device.

banner資料範例

Sample Banner


```
{
   "timestamp": "2014-01-16T08:37:40.081917",
   "hostnames": [
      "99-46-189-78.lightspeed.tukrga.sbcglobal.net"
   ],
   "org": "AT&T U-verse",
   "guid": "1664007502:75a821e2-7e89-11e3-8080-808080808080",
   "data": "NTP\nxxx.xxx.xxx.xxx:7546\n68.94.157.2:123\n68.94.156.17:123",
   "port": 123,
   "isp": "AT&T U-verse",
   "asn": "AS7018",
   "location": {
      "country_code3": "USA",
      "city": "Atlanta",
      "postal_code": "30328",
      "longitude": -84.3972,
      "country_code": "US",
      "latitude": 33.93350000000001,
      "country_name": "United States",
      "area_code": 404,
      "dma_code": 524,
      "region_code": null
   },
   "ip": 1664007502,
   "domains": [
      "sbcglobal.net"
   ],
   "ip_str": "99.46.189.78",
   "os": null,
   "opts": {
      "raw": "\\x97\\x00\\x03*\\x00\\x03\\x00H\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00
\\x00\\x00\\x00\\x00\\x01G\\x06\\xa7\\x8ec.\\xbdN\\x00\\x00\\x00\\x01\\x1dz\\x07\\x02\\x00\\x00\\x00
\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00
\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00q
\\x00\\x00\\x00i\\x00\\x00\\x00\\x00\\x00\\x00\\x00XD^\\x9d\\x02c.\\xbdN\\x00\\x00\\x00\\x01\\x00{\\x0
4\\x04\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00
\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00
\\x00\\x00\\x00\\x00q\\x00\\x00\\x00o\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00YD^\\x9c\\x11c.\\xbdN\\x00\\x0
0\\x00\\x01\\x00{\\x04\\x04\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00
\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00
\\x00\\x00\\x00\\x00\\x00",
      "ntp": {
         "more": false
      }
```


資料來源：https://developer.shodan.io/api/banner-specification

搜尋資料方式介紹與操作

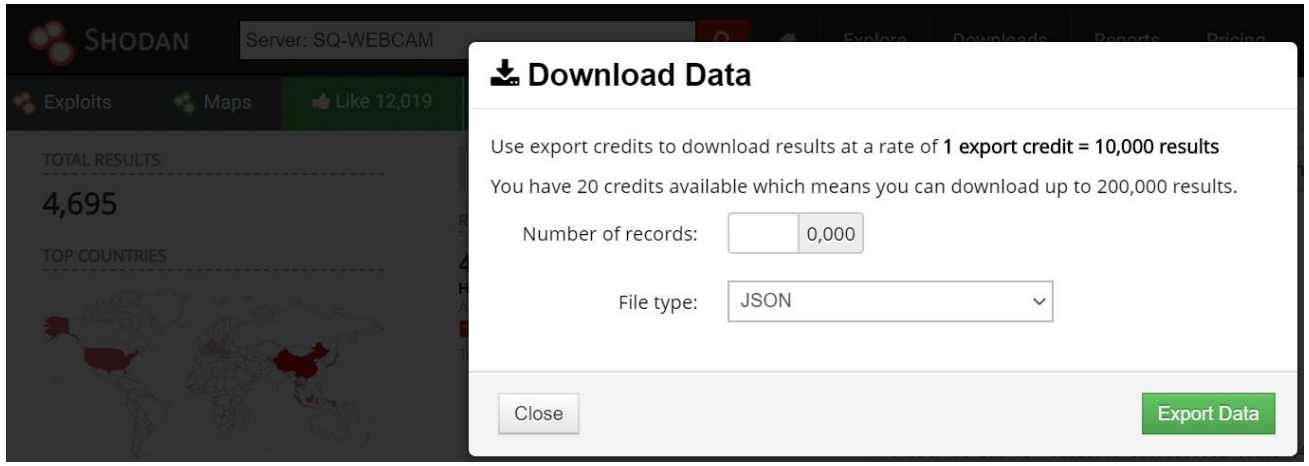
有兩個上機操作的練習

需先安裝開啟虛擬機的軟體，以及下載實驗用的虛擬機

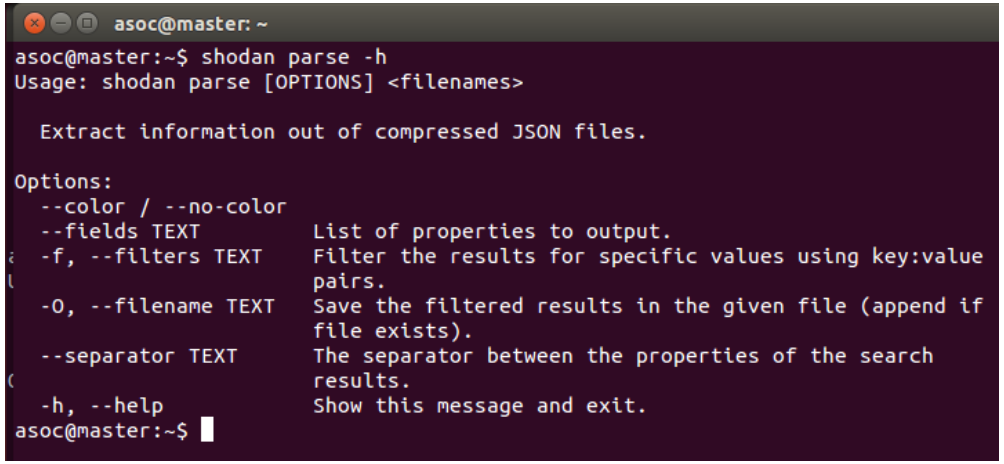
前言

- 使用Shodan相關服務前需要有Shodan帳號
- 使用者可以透過兩種方式從Shodan上取得資料

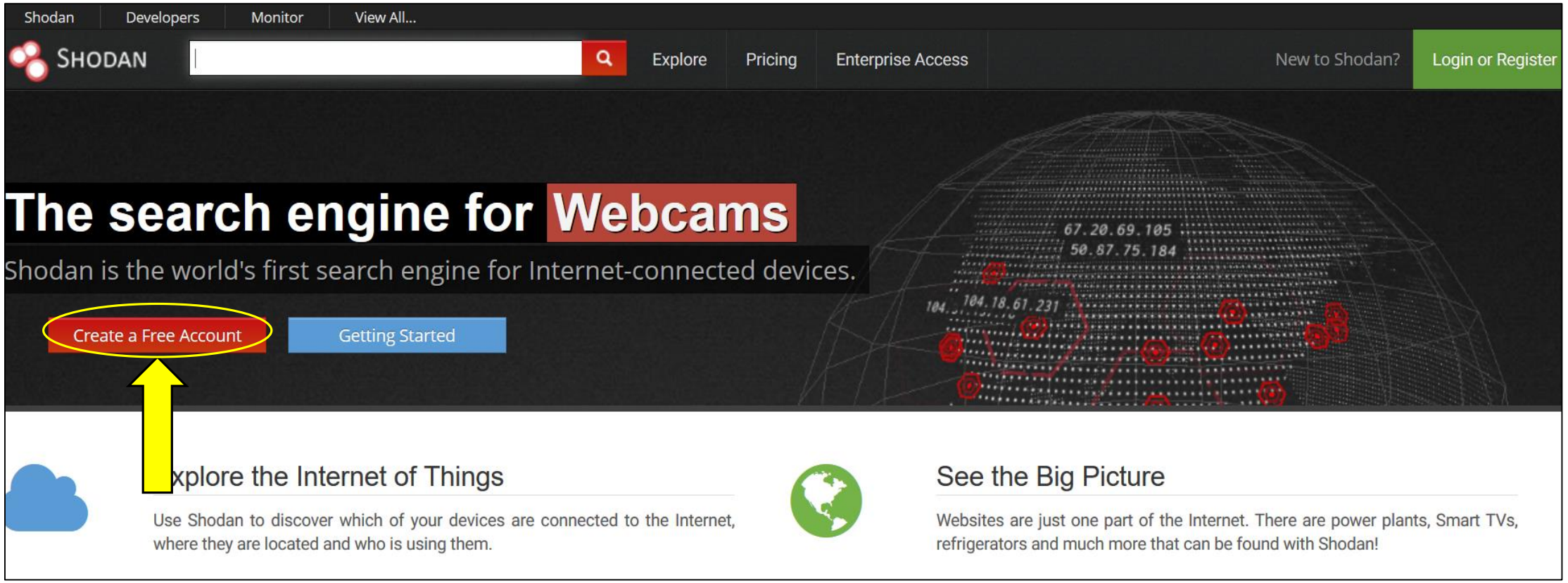
(1)Shodan網頁搜尋



(2)CLI模式下載



建立帳號

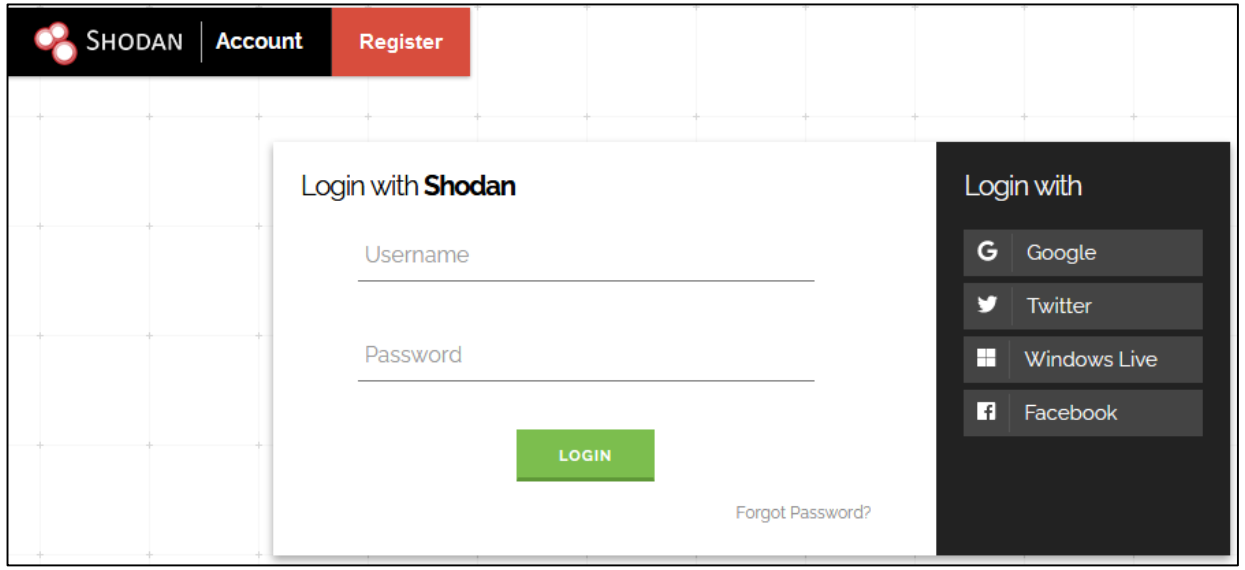

Shodan
Developers
Monitor
View All...
SHODAN
Explore
Pricing
Enterprise Access
New to Shodan?
Login or Register
The search engine for Webcams
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
67.20.69.105
50.87.75.184
104.18.61.231
xplore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

操作方式比較

	Shodan網頁搜尋	CLI模式下載
使用方式	在網頁搜尋列上輸入	安裝套件後輸入指令
使用難易度	簡單	困難
資料呈現方式	直觀，資料有先經過分類、整理	原始資料，需要轉換
原始資料取得	需要花費點數下載	根據帳號權限而有不同的下載數量
可操作的模式	少	多

網頁操作前言

- 在Shodan網頁上操作可快速查詢被掃描到的IoT的設備
- 當近期有公布新的漏洞時，可以先查詢是否有相關設備在網頁上
- 操作前先登入自己的Shodan帳號



	免费版
基础搜索功能 可以通过shodan语法进行搜索，并且可以使用Shodan Maps和Shodan Exploits功能。	✓
热门工具集成 可将shodan集合到Metasploit, Maltego和Nmap等工具中。	✓

圖片來源: http://www.ifuun.com/a20173221436011/

搜尋關鍵字

常用關鍵字	簡易說明	範例
net	搜尋指定的ip 位置或是網段(CIDR)	net:210.xxx.xxx.xxx/24
port	搜尋指定的連接埠	port:80
country	搜尋指定的國家	country:tw
city	搜尋指定的城市	city:taipei
進階關鍵字	**簡易說明**	**範例**
org	搜尋指定的組織或公司	org:google
isp	搜尋指定的isp業者	isp:hinet
hostname	搜尋指定的網域名稱	hostname:noip
version	搜尋指定的軟體版本	version:4.2
geo	搜尋指定的地理位置(緯度，經度)	geo:25,121
product	搜尋指定的作業系統/軟體/產品名稱	product:windows

網頁操作練習

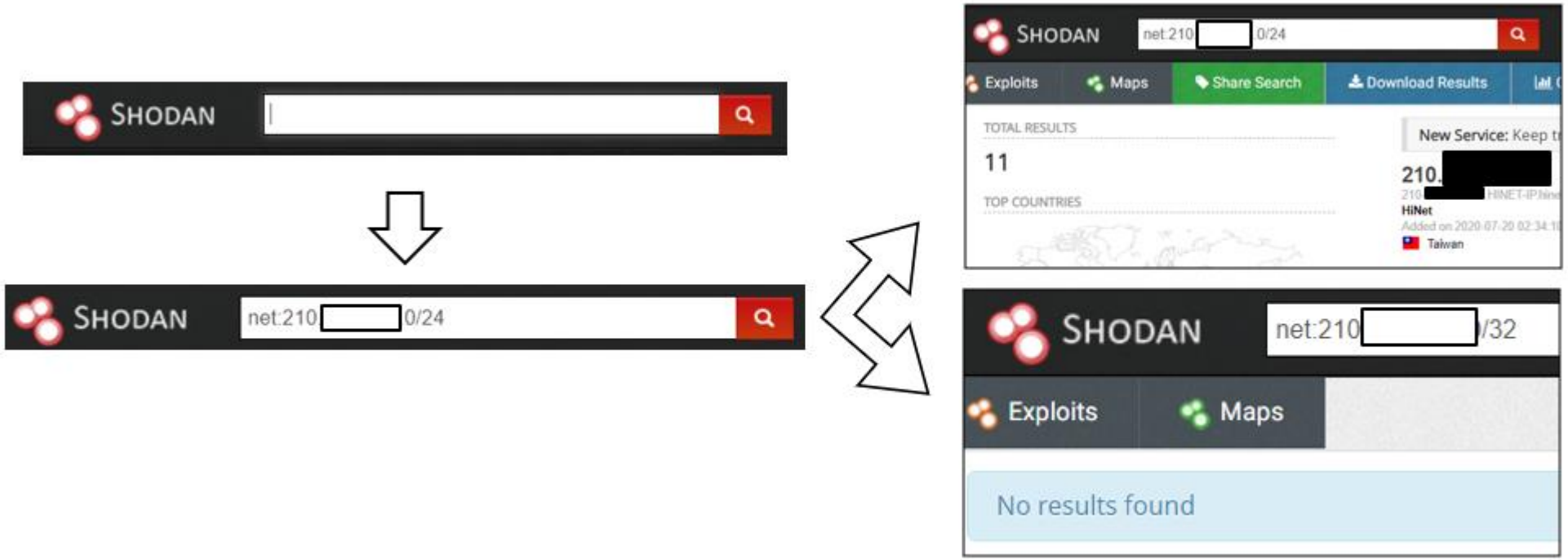
- 本次操作練習分兩個部分：
  1. 在網頁上搜尋任意的IP或網段，是否有資料在上面
  2. 使用兩個或以上的搜尋關鍵字搜尋資料

- 範例：

1. 找IP：Google DNS(net:8.8.8.8)、(自己)學校的網段(net:140.xxx.xxx.xxx/16)…
2. 找port號：遠端桌面(port:3389)、ONIVF協議(port:3702)、印表機服務(port:9100)…
3. 找product：架網站工具(Tomcat)、網路儲存伺服器(NAS)、網路攝影機(webcam)…

網頁操作練習說明-1

- 請參考搜尋關鍵字，搜尋任意的IP或網段



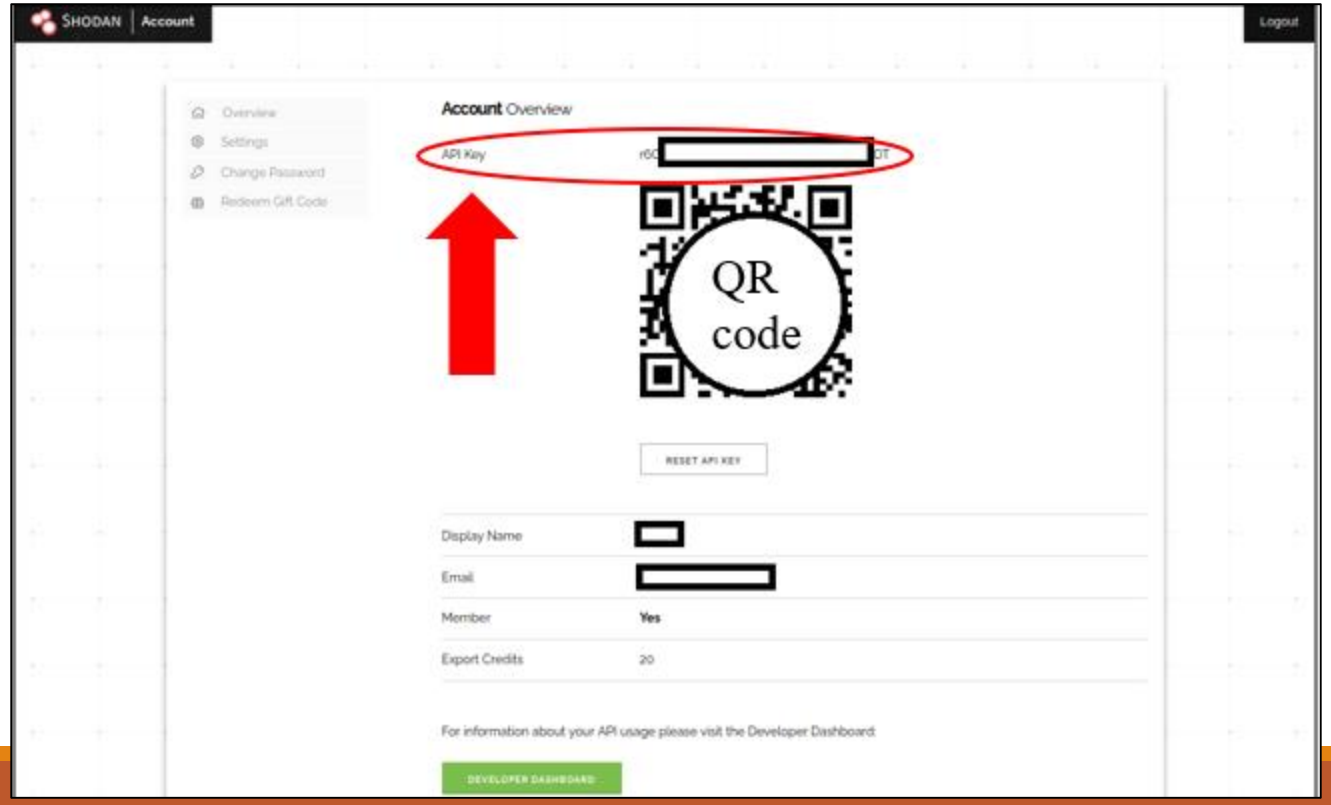
網頁操作練習說明-2

- 搜尋關鍵字可互相搭配使用
- 搜尋關鍵字先後輸入次序不影響結果

➢ 範例：

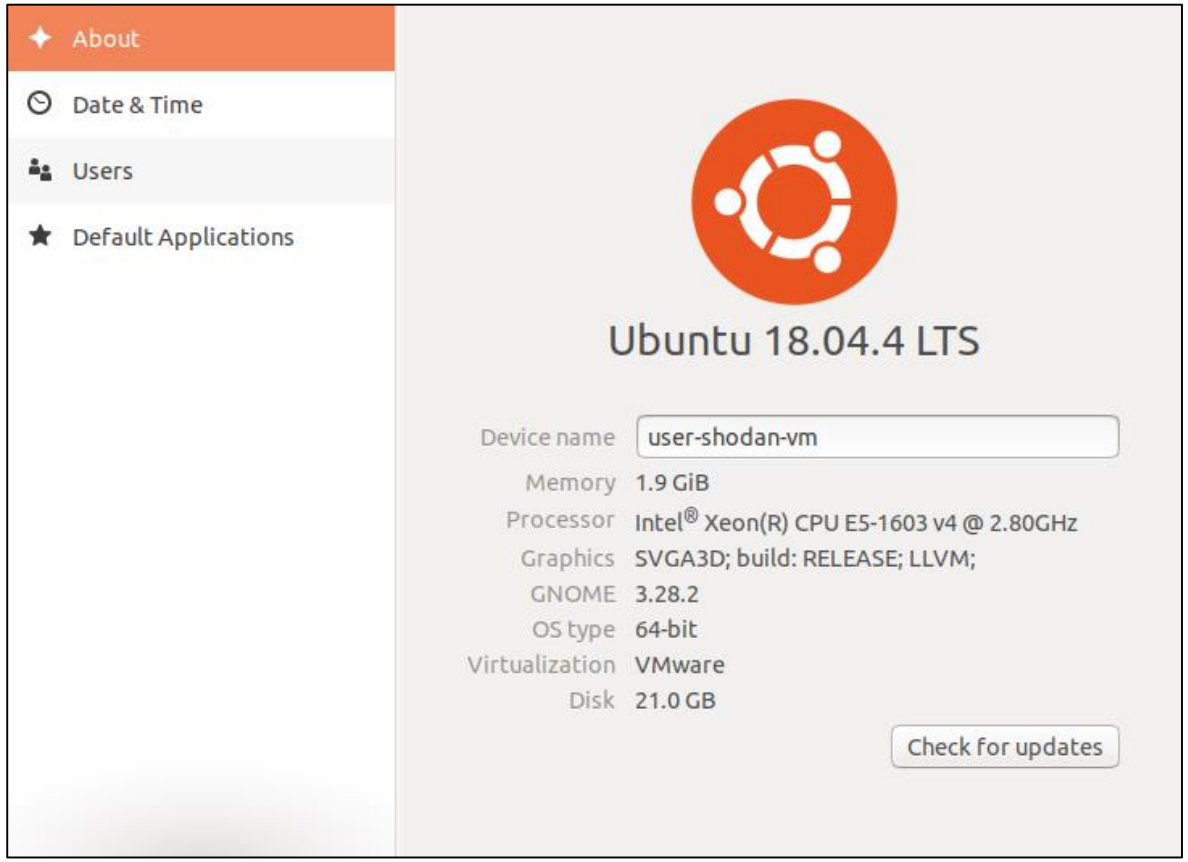
CLI操作前言

- Shodan官方有提供api套件，方便使用者去串接資料
- 操作前先登入自己的Shodan帳號(要用到api key)



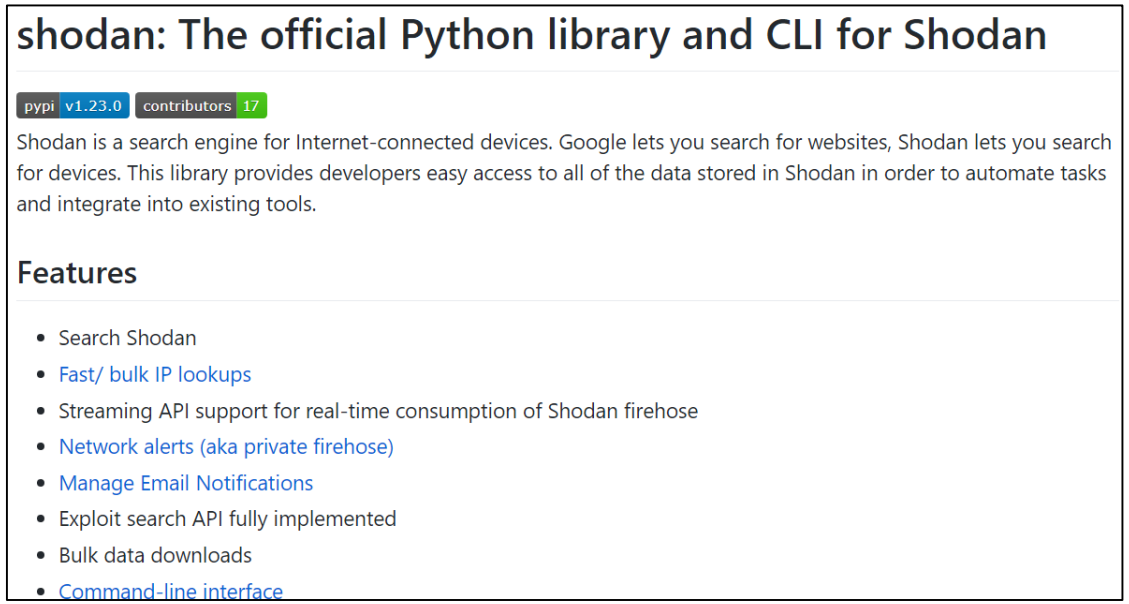
虛擬機環境

- OS:Ubuntu 18.04 LTS
- CPU: 1 core
- Memory: 2GB
- HD: 20GB
- Python版本: 3.6.9



安裝Shodan 套件

- 先安裝python pip管理套件，之後用pip安裝Shodan
  - sudo apt install python3-pip
  - sudo pip3 install shodan



shodan: The official Python library and CLI for Shodan

pypi v1.23.0 contributors 17

Shodan is a search engine for Internet-connected devices. Google lets you search for websites, Shodan lets you search for devices. This library provides developers easy access to all of the data stored in Shodan in order to automate tasks and integrate into existing tools.

Features

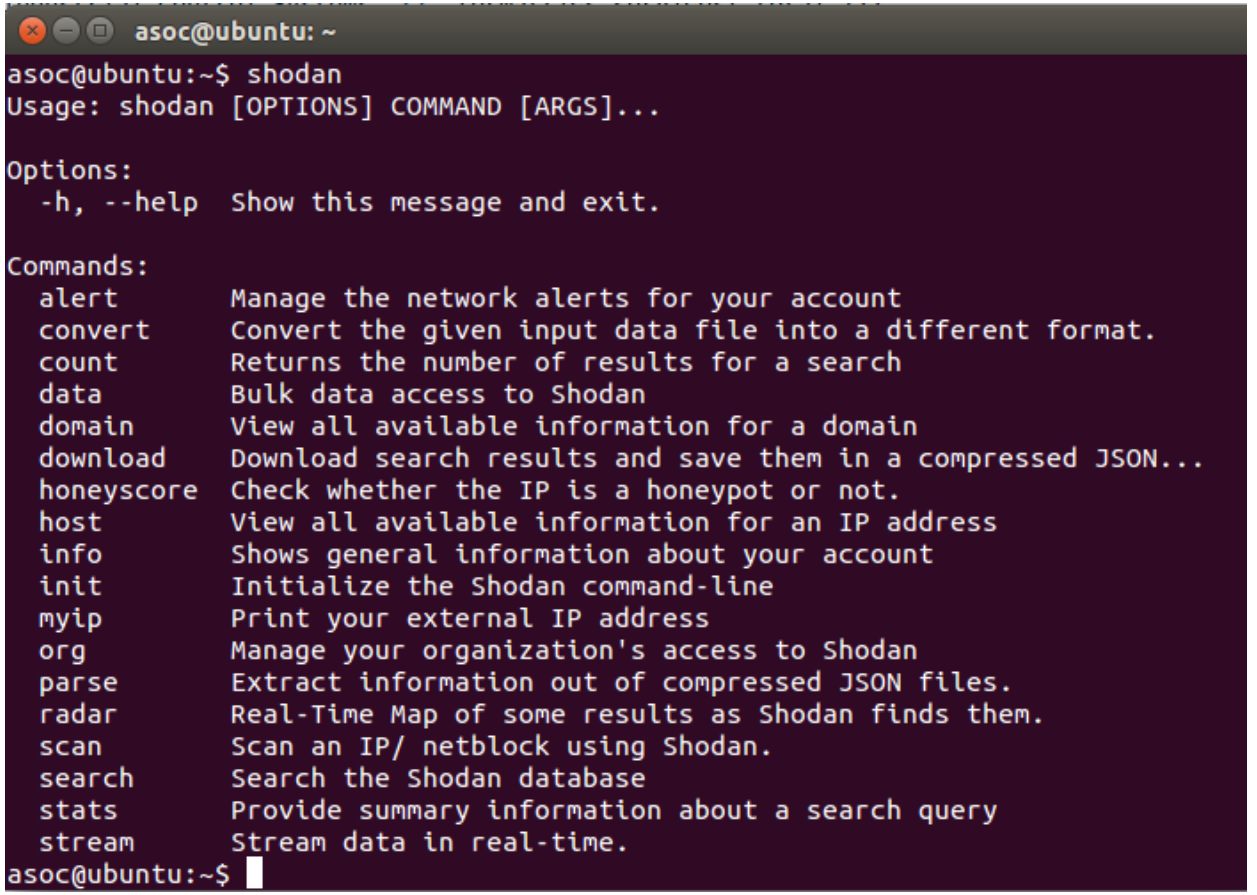
- Search Shodan
- Fast/ bulk IP lookups
- Streaming API support for real-time consumption of Shodan firehose
- Network alerts (aka private firehose)
- Manage Email Notifications
- Exploit search API fully implemented
- Bulk data downloads
- Command-line interface

資料來源：https://github.com/achillean/shodan-python

基本CLI指令

- 列出所有指令
  - shodan

- 查詢某個CLI指令用法
  - shodan <指令> -h



CLI指令說明(1/2)

CLI指令 (常用)	
指令	功能
init	初始化狀態(api key登入)
info	顯示目前帳號的下載點數與掃描點數資訊
myip	顯示目前使用的IP
host	輸入要查詢的IP，並顯示該IP的資料(nmap的掃描後的結果)
count	輸入查詢目標，回傳查詢結果的數量
download	輸入查詢目標，把查詢後的資料下載到檔案(有限制)
convert	輸入要轉換的檔案，轉換成其他格式

CLI指令說明(2/2)

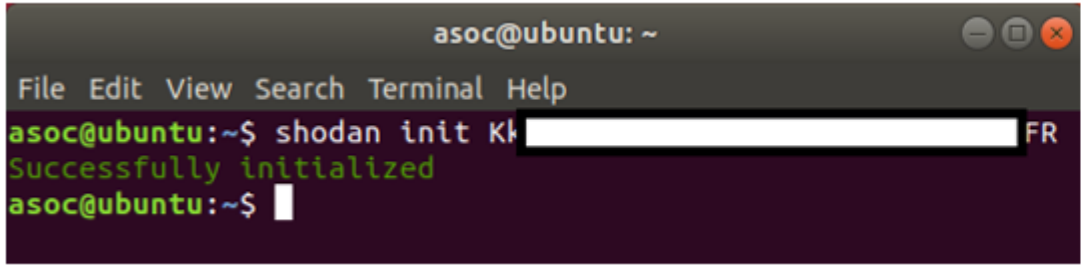
CLI指令 (進階)	
指令	功能
alert (需具備付費會員權限)	管理目前帳戶的網絡告警事件
honeyscore	輸入要查詢的IP，回傳該IP的honeypot(蜜罐)判斷分數
stream (需具備計畫會員權限)	即時顯示Shodan掃描到的資料(文字表示)
scan (需具備付費會員權限)	耗費掃描點數，讓Shodan去掃描輸入的IP或網段
parse	解析提取壓縮的JSON資訊(可指定要顯示的資料Key值)
search	輸入查詢的目標，回傳查詢後的詳細結果
stats	提供搜索結果的總結資訊
org (需具備企業會員權限)	管理組織內部的shodan帳號
domain (需具備付費會員權限)	查詢輸入的Domain，列出所有此Domain中的IP資訊(需要花費下載點數)
radar (需具備企業會員權限)	即時呈現Shodan掃描狀態(動態的文字圖片畫面)
data (需具備企業會員權限)	大量存取Shodan資料

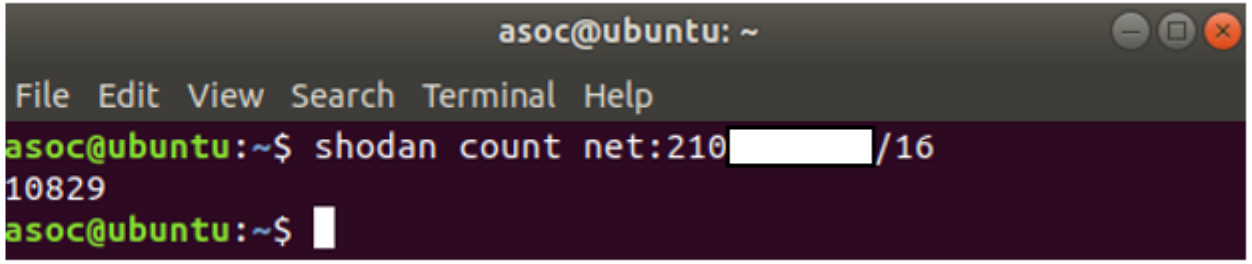
CLI操作練習

- 本次操作練習分四個部分：
  1. 查詢資料
  2. 下載資料
  3. 轉換資料格式
  4. 分析資料

CLI操作練習說明-1

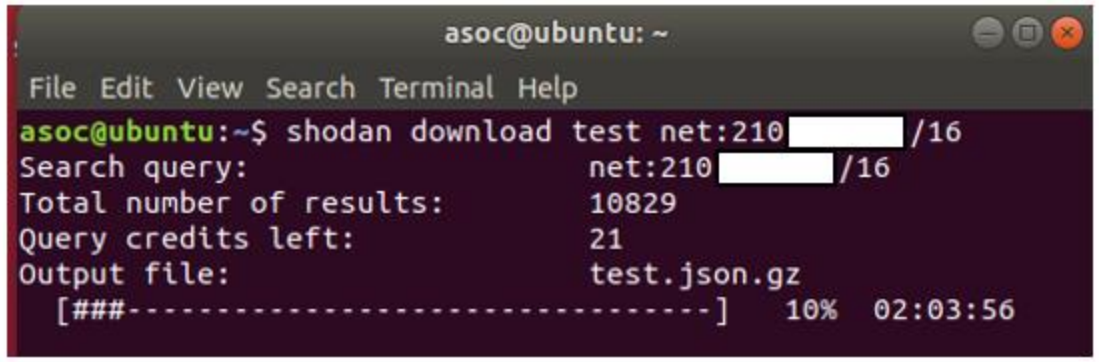
- 查詢資料
  - 登入自己的Shodan帳號
    - 輸入：shodan init <自己的api key>
  - 查詢目標的資料數量
    - 輸入：shodan count <搜尋關鍵字>

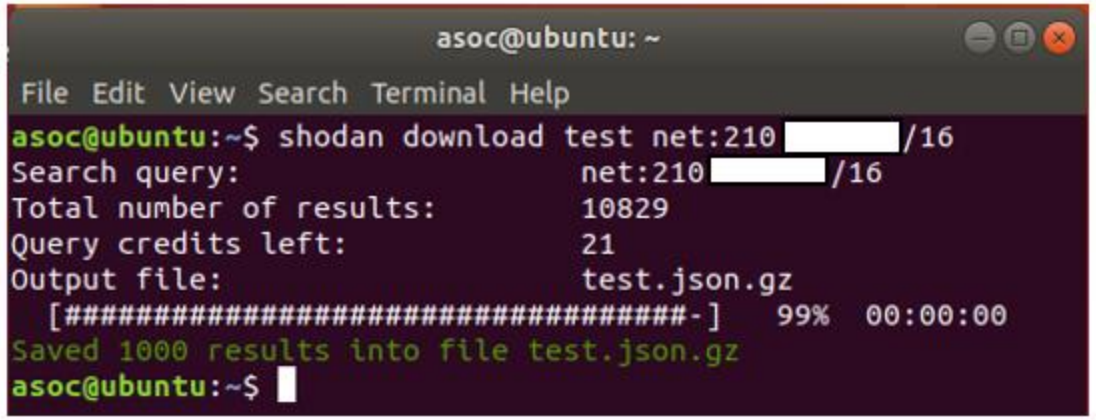




CLI操作練習說明-2

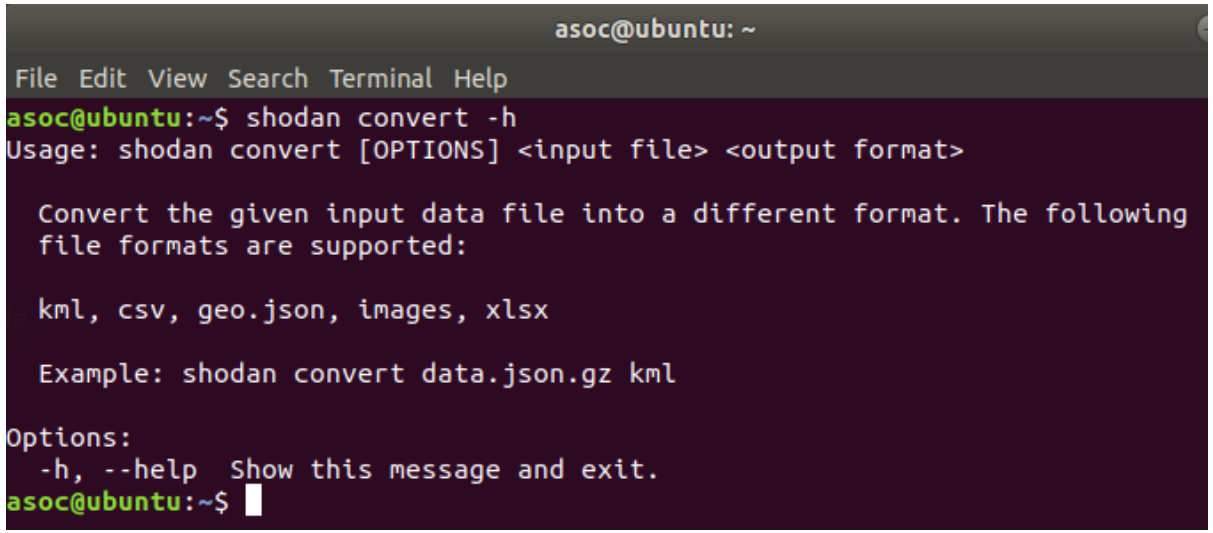
- 下載資料
  - 輸入：shodan download [檔案名稱] <搜尋關鍵字>

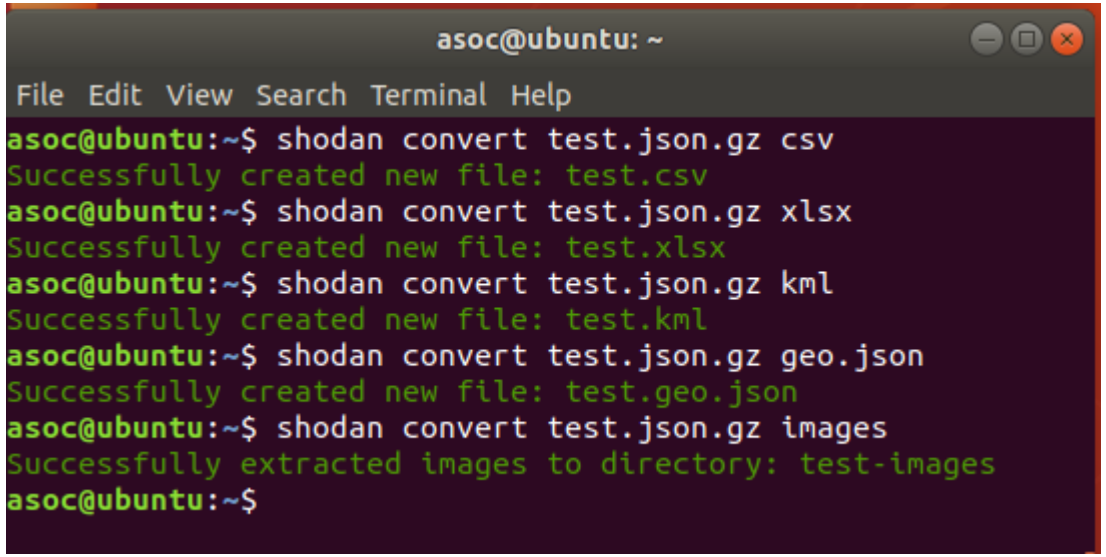




CLI操作練習說明-3

- 轉換資料格式
  - 輸入：shodan convert [檔案名稱] <要被轉換的格式>
  - 建議轉換成csv或是xlsx格式





CLI操作練習說明-4

- 分析資料：找出能被使用的的資訊

xlsx格式欄位			
1	IP	10	City
2	Port	11	OS
3	Timestamp	12	ASN
4	Data	13	Transport
5	Hostnames	14	Product
6	Organization	15	Version
7	ISP	16	Web Server
8	Country	17	Website Title
9	Country ISO Code		

CSV格式欄位			
1	data	17	timestamp
2	hostnames	18	transport
3	ip	19	product
4	ip_str	20	version
5	ipv6	21	vulns
6	org	22	ssl.cipher.version
7	isp	23	ssl.cipher.bits
8	location.country_code	24	ssl.cipher.name
9	location.city	25	ssl.alpn
10	location.country_name	26	ssl.versions
11	location.latitude	27	ssl.cert.serial
12	location.longitude	28	ssl.cert.fingerprint.sha1
13	os	29	ssl.cert.fingerprint.sha256
14	asn	30	html
15	port	31	title
16	tags		

近期研究的漏洞內容

QNAP漏洞有CVE-2019-7192~CVE-2019-7195

本次分析內容是CVE-2019-7192

研究前言

- CVE-2019-7192到CVE-2019-7195是由國內資安廠商在去年六月發現並通報QNAP廠商，QNAP於去年11月發布更新檔修補這些漏洞
- 在今年六月底，HITCON ZeroDay通報平台有出現許多單位的QNAP NAS有此漏洞；其中也包含學術單位被通報

資料來源：https://zeroday.hitcon.org/vulnerability/patching/page/11

漏洞說明

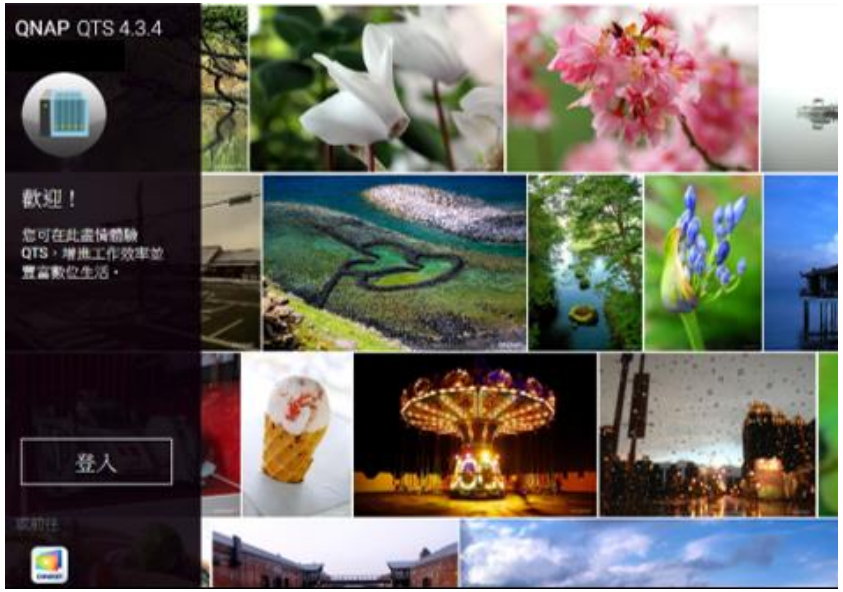
- 漏洞出現在QNAP的線上相簿程式(Photo Station)和QTS上執行的CGI程式
- CVE-2019-7192到CVE-2019-7195，這四個CVSS風險評分皆為重大(9.8)
- 這些漏洞執行難度低，容易被串起來利用進而實現Pre-Auth Root RCE攻擊

漏洞產品	CVE編號	簡易漏洞說明
QTS	CVE-2019-7193	任意程式碼注入：允許攻擊者冒充合法使用者注入任意PHP程式碼，修改連線(session)
Photo Station	CVE-2019-7192	任意文件讀取：此漏洞使攻擊者無需身份驗證即可讀取Photo Station上的任意文件
	CVE-2019-7194	任意命令執行：讓攻擊者將連線(session)內容寫入到伺服器任意位置
	CVE-2019-7195	

受影響的版本

- 如果版本號碼比下面列出的版本舊，就存在此漏洞：

1. QTS版本
   - 4.4.1之前(build 20190918)
   - 4.3.6之前(build 20190919)
2. Photo Station版本
   - 5.2.11 之前
   - 5.4.9 之前
   - 5.7.10 之前
   - 6.0.3 之前



資料來源：QNAP官方網站

建議處理措施

- 目前QNAP官方已針對此漏洞釋出更新程式，官方建議將設備更新至以下版本：

1. QTS：
   - QTS 4.4.1：build 20190918(含)以後版本
   - QTS 4.3.6：build 20190919(含)以後版本
2. Photo Station：
   - QTS 4.4.1：Photo Station 6.0.3(含)以後版本
   - QTS 4.3.4 ~ QTS 4.4.0：Photo Station 5.7.10(含)以後版本
   - QTS 4.3.0 ~ QTS 4.3.3：Photo Station 5.4.9(含)以後版本
   - QTS 4.2.6：Photo Station 5.2.11(含)以後版本

搜尋和驗證示範

上機DEMO示範

示範說明

- 利用Shodan搜尋QNAP設備
- 用PoC程式去檢查是否有漏洞

```
def is_vulnerable_version_date(version_date):
    try:
        version, date = version_date
        if version.startswith('6.'):
            return is_version_smaller(version, '6.0.3')
        if version.startswith('5.7'):
            return is_version_smaller(version, '5.7.10')
        if version.startswith('5.4'):
            return is_version_smaller(version, '5.4.9')
        if version.startswith('5.2'):
            return is_version_smaller(version, '5.2.11')
        return is_date_earlier_than(date, '20190918')
    except Exception:
        pass
    return False
```

資料來源

免費圖庫資料來源

1. Flaticon：https://www.flaticon.com/
2. Freepik：http://www.freepik.com

Shodan資料來源

1. John Matherly (2017), Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work for You, Leanpub. (Shodan官方電子書)
2. Shodan官方網站：https://cli.shodan.io/
3. banner資料說明與範例：https://developer.shodan.io/api/banner-specification
4. Shodan會員資料說明：http://www.ifuun.com/a20173221436011/
5. Shodan安裝(Github)：https://github.com/achillean/shodan-python

QNAP漏洞資料來源

1. iThome報導：https://www.ithome.com.tw/news/137748
2. HITCON通報：https://zeroday.hitcon.org/vulnerability/ZD-2020-00480
3. 原始漏洞分析資訊(大部分內容遭修改)：https://medium.com/bugbountywriteup/qnap-pre-auth-root-rce-affecting-450k-devices-on-the-internet-d55488d28a05
4. CVE-2019-7192說明： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7192
5. CVE-2019-7193說明： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7193
6. CVE-2019-7194說明： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7194
7. CVE-2019-7195說明： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7195
8. QNAP修補漏洞說明：https://www.qnap.com/zh-tw/security-advisory/nas-201911-25

Q & A