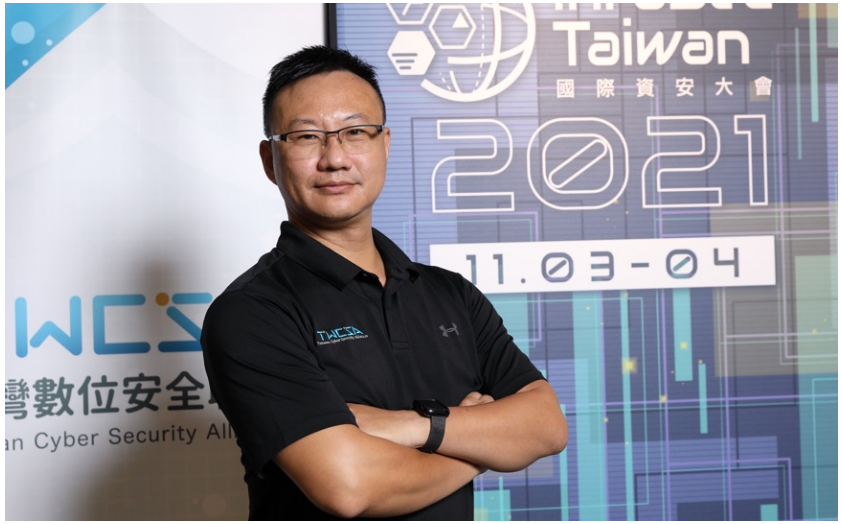
資安工具101

20230309

蔡一郎 / 高偉碩

SHIELDXTREME

Google Me.



蔡一郎 Steven Tsai

現任

- ✓ 微智安聯股份有限公司 創辦人兼執行長
- ✓ 台灣數位安全聯盟 榮譽理事長
- ✓ 台灣網際空間與安全策略發展協會 理事長
- ✓ 台灣數位鑑識發展協會 理事
- ✓ 中華民國資訊安全學會 監事
- ✓ 中華民國數位金融交易暨資料保護協會 理事
- ✓ 台灣資訊及資安服務聯盟 理事
- ✓ 中華民國人壽保險商業同業工會 資安顧問
- ✓ InfoSec Taiwan 國際資安大會 主席
- ✓ OWASP 台灣分會長
- ✓ The Honeynet Project 台灣分會長
- ✓ Cloud Security Alliance 台灣分會長
- ✓ CSCIS 亞太區副總裁
- ✓ 教育部、交通部資安稽核委員
- ✓ 自由作家，資訊圖書著作 35 本，技術專欄文章 90 餘篇
- ✓ 部落格 https://blog.yilang.org
- ✓ 專業證照：
  - ✓ RHCE、CCNA、CCAI、CEH、CHFI、ACIA、ITIL Foundation、ISO 27001 LAC、ISO 20000 LAC、BS10012 LAC、ISO 17065、CSA STAR Auditing、CCSK

曾任

- ✓ 財團法人國家實驗研究院國家高速網路與計算中心 研究員
- ✓ 台灣數位安全聯盟 理事長
- ✓ 總統府、行政院、經濟部資安稽核委員
- ✓ 中華民國資料保護協會 監事
- ✓ 數位經濟暨產業發展協會 理事
- ✓ 中華民國南部科學園區產學協會 理事 監事
- ✓ 台灣資訊安全聯合發展協會 監事

Outline

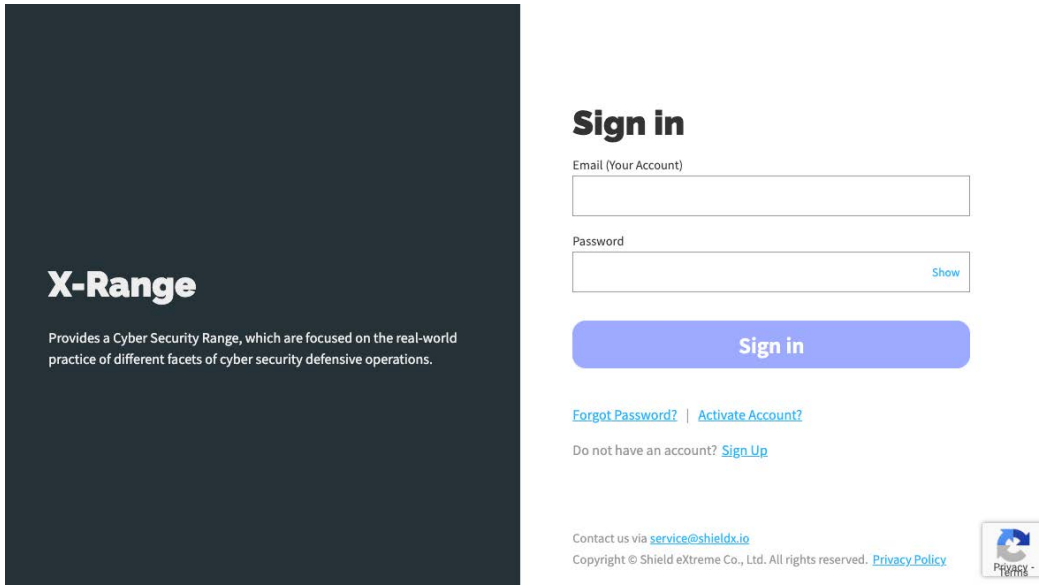
- 資訊安全入門
- 常見的資安工具
- 實務練習

課程資訊

- 協作筆記
  - https://tinyurl.com/20230309X

HackMD

- 實作平台
  - X-Range https://xrange.shieldx.io/



資訊安全入門

SHIELDXTREME

什麼是 101 ？

圖片來源： Klook

資安相關的工具軟體多嗎？

Cyber Security Tools

資安的關鍵痛點

人

- 資安人才供不應求，各產業資安服務需求增加，人力缺乏
- 企業內部現有資訊人員對網路資安知識或能力的不足
- 資安培訓環境與資源不足

事

- 無法掌握最新資安威脅情資
- 情資來源管道眾多，無法驗證情資之有效性
- 無法自動化處理威脅情資，耗費時間人工處理
- 無法與資安設備直接整合

時

- 隨時可能發生資安事件，但卻無法有效因應
- 缺乏經驗無法因應資安事件處理的時效要求
- 與駭客跟時間賽跑，無法掌握有力證據
- 無法在有限制時間內培養防禦能力

地

- 企業隨時隨地可能發生資安事件但卻無法有效因應
- 無法追蹤資安事件發生的地點與發掘根因

物

- 企業數位邊界無法明確定義
- 駭客組織持續找尋企業弱點
- 企業營運的資通訊平台與環境成為遭受攻擊的標的物

認識資安領域相關的搜尋引擎

猜猜這是什麼？

Address	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Format	BASE58 (P2PKH)
Transactions	245
Total Received	19.69028255 BTC
Total Sent	17.77113037 BTC
Final Balance	1.91915218 BTC

Address	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Format	BASE58 (P2PKH)
Transactions	124
Total Received	14.87769994 BTC
Total Sent	14.41067602 BTC
Final Balance	0.46702392 BTC

Fee 0.00002210 BTC
(1.859 sat/B - 0.500 sat/WU - 1189 bytes)
(2.000 sat/vByte - 1105 virtual bytes)

+0.00010810 BTC

https://www.blockchain.com/btc/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Hash 03931ebe702df3da36f887c9fe66aec344f51591d2f9cf25e984721c24...

2022-09-09 09:22

bc1qdvtq5wrelpkcqexff222cumdrraj2uz7q7y6w9	0.00013200 BTC
14Gpu37x74AqQ8eaRfHZKuR5AJAMnXvMuc	0.00039440 BTC
1ET7ZZW4Y1xYCvBccFymEPf5LV9z2yHpXx	0.00017800 BTC
16KhUAxcga98PrQm2kcCanZbzvA3H28tRH	0.00018995 BTC
1FpdJYjDhGBTbEYDQSJJ7E5WjeX79Gt5Q4	0.00080423 BTC

1B1kmLinVJ6NePcaXYZQPayQwrNZfhkWqU	0.00011293 BTC
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	0.00010810 BTC
174sjrmSiwKJSemLiYEhimwQRcv3rRnexK	0.00025607 BTC
bc1q5pz76a8lj64u2vwr70tscl9l758gmnx4g7khg2	0.00000333 BTC
1CdMh1WKos7wkzRYadd6Ljy7s5HCvBhVK6	0.00011931 BTC
1AaCRY1pFTSVnkKAKkP9rawX3Ks2xgfa6n	0.00015600 BTC
1943xu96cHh91JCcYXWUnhc9THx3WAezh3	0.00016975 BTC
1CZdKn77TqNLFQM83ejZbLkNCToPp4ym1x	0.00010807 BTC
1BA5TRKWPxG3bY2Fw5vyjkwEtP3QUvBLud	0.00012871 BTC
154UHT6sBRwq7rw924hzXobY5f7cNbA48E	0.00018973 BTC

SHIELDXTREME

https://www.blockchain.com/btc/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WannaCry Ransomware

常見的資安工具

SHIELDXTREME

Google Hacking

- Google 這個名詞，除了是一個大家熟悉的品牌， 更是資訊人員的好幫手，因為我們常常用它來尋找 我們想要的資料，而Google Hacking 亦是如此， 只是我們利用了一些特殊的語法及關鍵字，找到一 些遺留在網路上的資料。

- 用於資安工作者~~(Hacker)~~卻可以用來蒐集網站相關資訊。

Google Hacking

- 資料量夠大
- 回應速度快
- 最佳化輸出結果
- 頁庫存檔
- 豐富的運算元

Google Search

- 常見Agent
  - Googlebot, Yahoo!Slup, bingbot
  - AhrefsBot, Baiduspider, Ezooms, MJ12bot, YandexBot
- Robots.txt
  - User-agent：可以指定哪一種User-agent
  - Allow/Disallow : 設定檔案或是資料夾，允許不允許被爬取
  - Crawl-delay：設定抓取的延遲時間
  - Sitemap：用來告知搜尋爬蟲網站結構
- 詞彙/關鍵字(term)

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /images/
Disallow: /tmp/
Disallow: /private/
```

Google Hacking相關語法

常用指令

語法	用途
intitle/allintitile	搜尋網頁標題的內容
intext/allintext	搜尋網頁的本文
inurl/allinurl	搜尋網頁的URL內容
filetype	搜尋特定類型的檔案
link	搜尋網站中的鏈結
site	限制搜尋的對象必須來自指定網域
cache	搜尋Google 頁面存檔中最近歸檔的網頁
inanchor/allinanchor	搜尋網站上的鏈結文字，而回傳該鏈結所指向的網頁
related	查詢和指定的網址或URL有關聯的網頁(搜尋類似內容)
info	顯示指定的網域或URL之摘要資訊(網頁相關資訊)
daterange	過濾在特定時間內被google編入索引的網頁(限定時間範圍)
numrange	搜尋有指定範圍內數值的網頁(數字範圍)
define	搜尋名詞的定義
stocks	搜尋某家公司的股票資訊
location/source	縮減新聞資料的搜尋範圍

Google Search 基本搜尋運算子

- +: 用在詞彙的前面，表示此詞彙必須要出現在網頁之中
- -:用在詞彙的前面，表示排除此詞彙
- “” :雙引號刮起來，強制文字之順序
- .: 表示任一字元，如 bl.ck box
- *:表示任一單字，如 Apache/* Server
- ..:搜尋範圍內之數字或是金錢，如 1900..2019、$300..$900
- OR |: 表示其中之一，如 台灣(“科技” | “首府”)
- : Google 會自行判斷輸入文字之語系，做最好之處理。中文會有自行一套斷詞規則，
  - EX:搜尋 國網中心台灣衫

- 那AND呢?

Google Search

Workshop – 找尋密碼

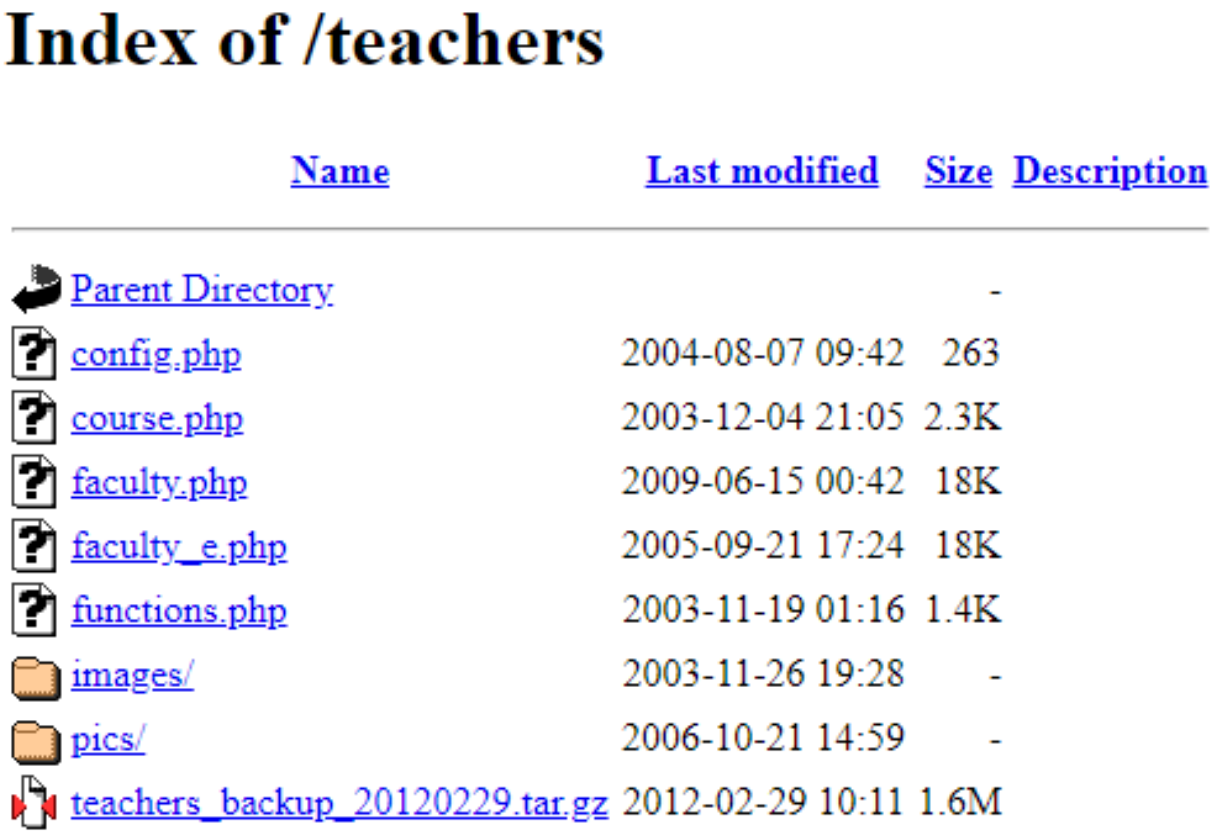
- Password
  - password filetype:xls site:tw
  - "access denied for user" "using password”
  - "AutoCreate=TRUE password=*"
  - "Index of /" +password.txt
  - "Index of /password"

利用Google Hacking尋找資訊洩漏

- 傳統資訊洩漏
- 管理介面的洩漏如同告知歹徒保險箱位置
  - 暴力破解管理帳號
  - 後台防禦較弱
  - 套件管理介面
- 常見路徑
  - /admin, /administrator, /phpmyadmin, /manage
- 管理介面不對外開放存取
- 隱藏管理介面目錄(複雜目錄名稱)
- 加強後台防禦

利用Google Hacking尋找資訊洩漏

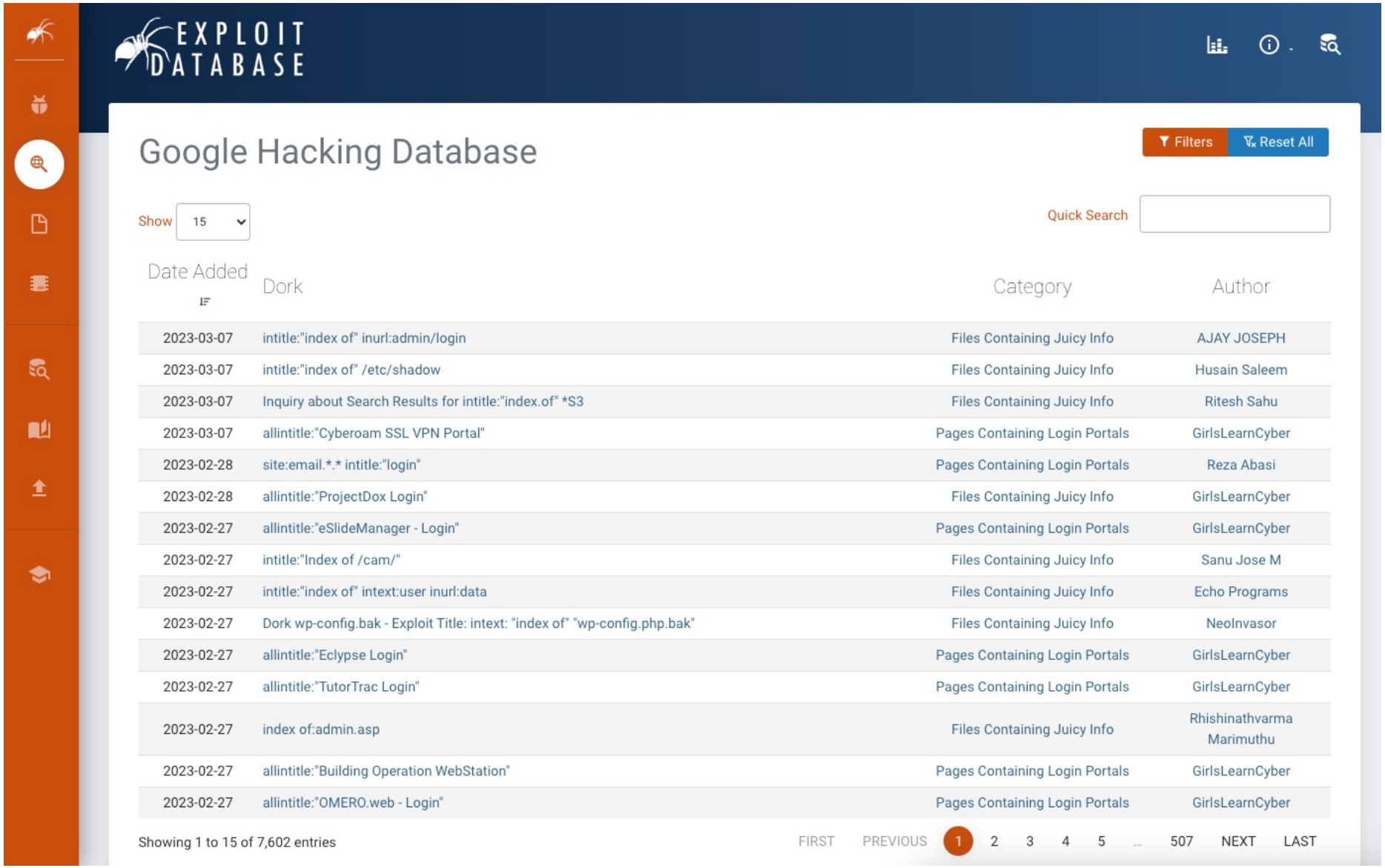
- 目錄瀏覽
  - 洩漏網站目錄結構
  - 有機會存取機敏檔案
  - 有機會存取設定檔



Index of /teachers

Name	Last modified	Size	Description
Parent Directory		-	
config.php	2004-08-07 09:42	263	
course.php	2003-12-04 21:05	2.3K	
faculty.php	2009-06-15 00:42	18K	
faculty_e.php	2005-09-21 17:24	18K	
functions.php	2003-11-19 01:16	1.4K	
images/	2003-11-26 19:28	-	
pics/	2006-10-21 14:59	-	
teachers_backup_20120229.tar.gz	2012-02-29 10:11	1.6M	

Google Hacking Data Base (GHDB)



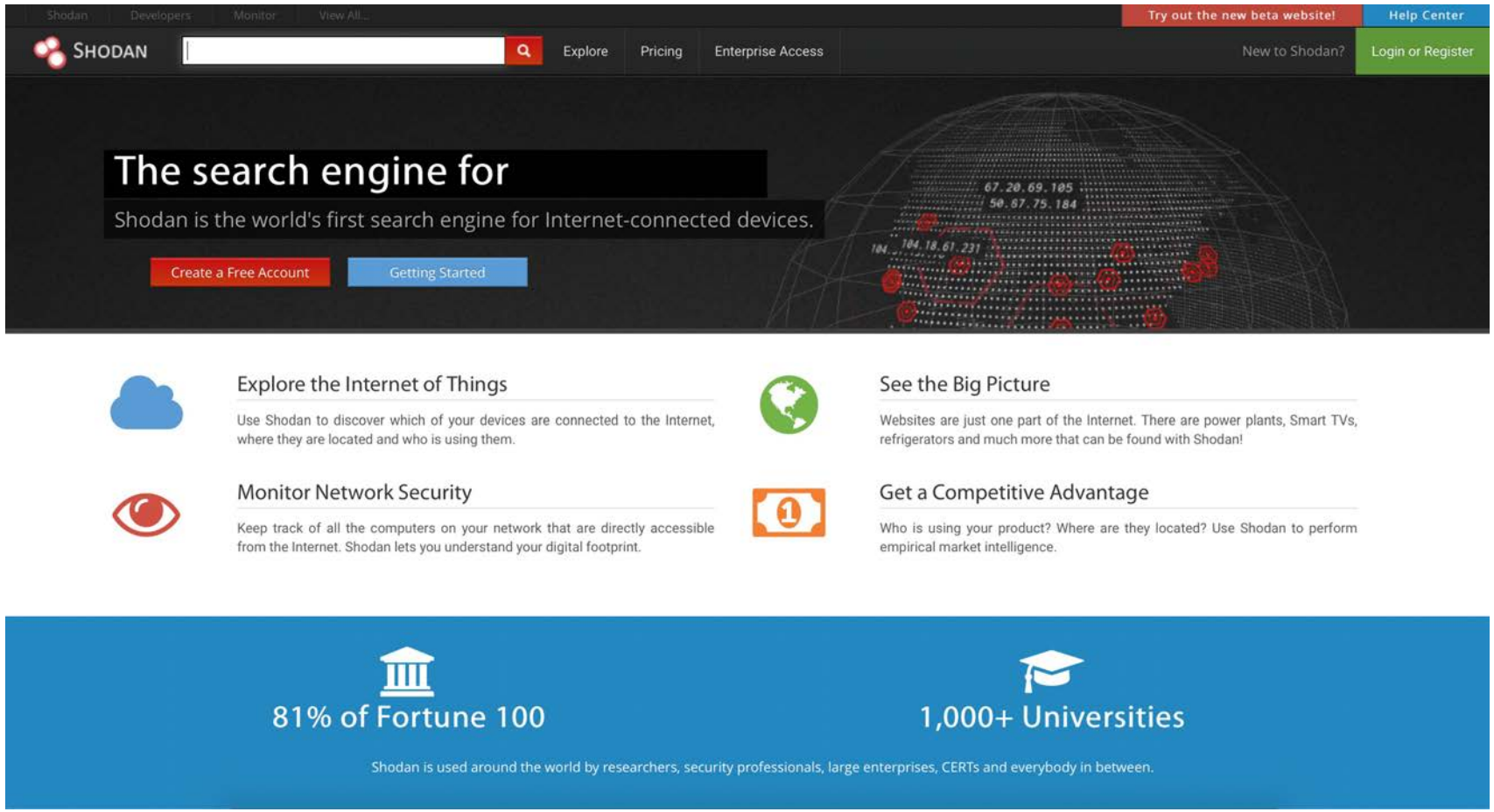
Date Added	Dork	Category	Author
2023-03-07	intitle:"index of" inurl:admin/login	Files Containing Juicy Info	AJAY JOSEPH
2023-03-07	intitle:"index of" /etc/shadow	Files Containing Juicy Info	Husain Saleem
2023-03-07	Inquiry about Search Results for intitle:"index.of" *S3	Files Containing Juicy Info	Ritesh Sahu
2023-03-07	allintitle:"Cyberoam SSL VPN Portal"	Pages Containing Login Portals	GirlsLearnCyber
2023-02-28	site:email.*.* intitle:"login"	Pages Containing Login Portals	Reza Abasi
2023-02-28	allintitle:"ProjectDox Login"	Files Containing Juicy Info	GirlsLearnCyber
2023-02-27	allintitle:"eSlideManager - Login"	Pages Containing Login Portals	GirlsLearnCyber
2023-02-27	intitle:"Index of /cam/"	Files Containing Juicy Info	Sanu Jose M
2023-02-27	intitle:"index of" intext:user inurl:data	Files Containing Juicy Info	Echo Programs
2023-02-27	Dork wp-config.bak - Exploit Title: intext: "index of" "wp-config.php.bak"	Files Containing Juicy Info	NeoInvasor
2023-02-27	allintitle:"Eclypse Login"	Pages Containing Login Portals	GirlsLearnCyber
2023-02-27	allintitle:"TutorTrac Login"	Pages Containing Login Portals	GirlsLearnCyber
2023-02-27	index of:admin.asp	Files Containing Juicy Info	Rhishinathvarma Marimuthu
2023-02-27	allintitle:"Building Operation WebStation"	Pages Containing Login Portals	GirlsLearnCyber
2023-02-27	allintitle:"OMERO.web - Login"	Pages Containing Login Portals	GirlsLearnCyber

Showing 1 to 15 of 7,602 entries

FIRST PREVIOUS 1 2 3 4 5 ... 507 NEXT LAST

類似的 Google Hacking-Shodan

- Shodan
  - 搜索的物件是所有連上網路的物件，它搜索的不是與某個欄位相關聯的內容，而是各式各樣完全不同的 IP 位址



Shodan相關語法

語法	用途	範例語法
hostname	搜尋指定的主機或域名	hostname:shieldx
port	搜尋指定的服務或埠	port:8080
country	搜尋指定的國家	country:TW
city	搜尋指定的城市	IIS city:taipei
org	搜尋指定的組織	org:shieldx
isp	搜尋指定的ISP供應商	isp:hinet
os	搜尋指定的作業系統	os:windows
product	搜尋指定的產品	product:” apche tomcat”
version	搜尋指定的軟體版本	product:apche version:1.3.37
geo	搜尋指定的地理位置(經緯度) geo: 緯度1.經度1,緯度2.經度2	apache geo:42.9693,-74.1224
before/after	搜尋指定收錄的前後時間 格式為dd-mm-yy	before:"11-11-15"
net	搜尋指定的IP地址或是子網域	net:8.8.0.0/16
ASN	搜尋指定的ASN	ASN:AS3462

Workshop – 找尋不安全的印表機

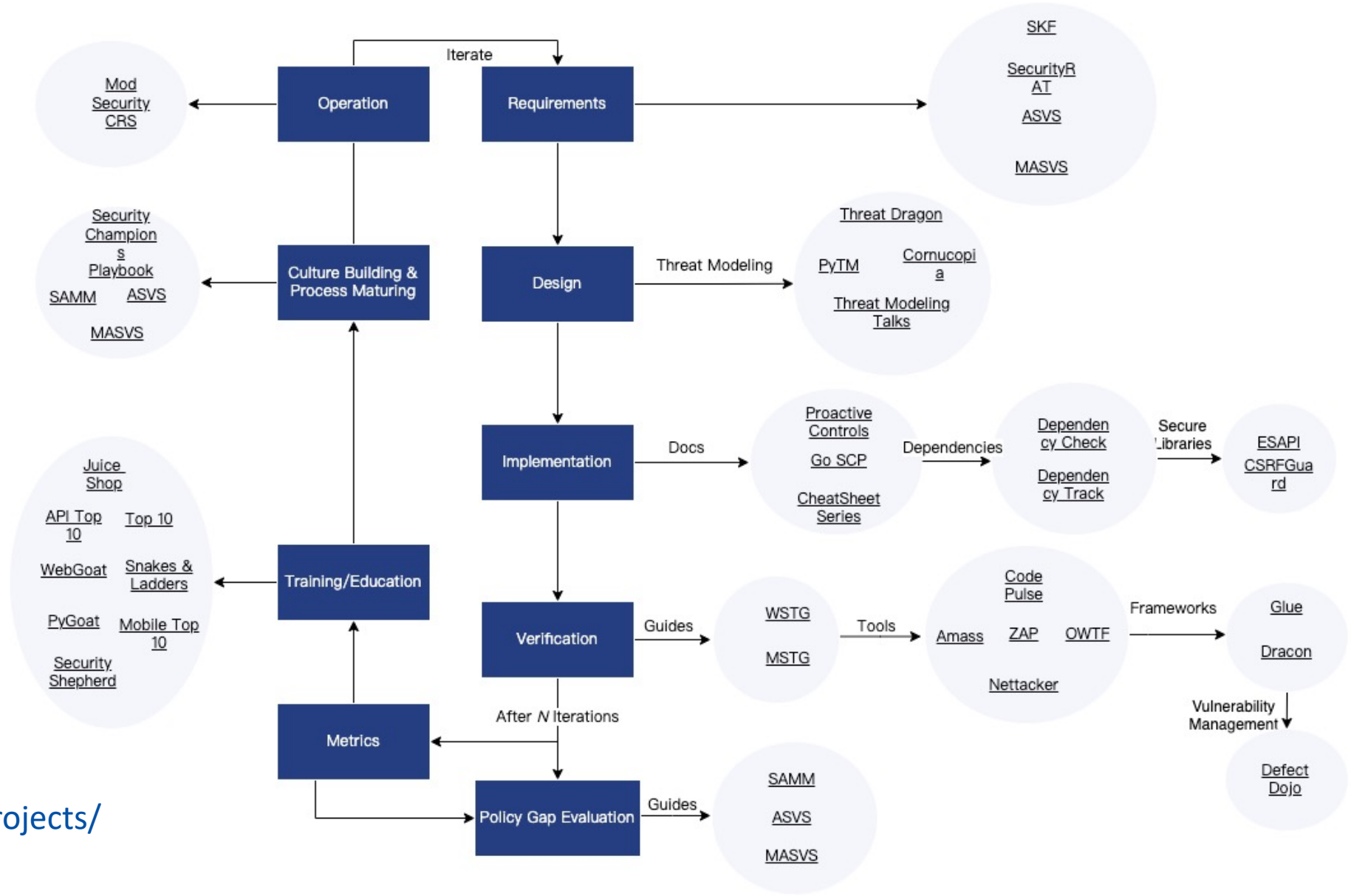
- 試著使用 Shodan 找尋以下品牌且於位台灣的印表機
- 語法：

OWASP:Open Web Application Security Project

OWASP(Open Web Application Security Project)為全球主要針對開放網頁應用程式安全進行研究的非營利組織，目前已有超過45,000名的志願參與者，針對頁應用程式相關的資安問題，進行關鍵的研究並發佈相關的研究成果，對於現今以網頁程式運作為主的資訊環境，更顯得OWASP正扮演著舉足輕重的角色；於2017年OWASP重新啟動台灣分會的運作，希望以更積極主動的方式，將國際間的熱 門 資安議題，以及研究的成果，透過社群活動、大型會議等方式，分享給國內的參與者，OWASP台灣分會依循全球一致的原則，以中立的角色連結產管學研界，希望凝聚國內資安社群的能量，以接軌國際資安社群，能夠同步發佈全球已公開的研究資料，將有助於改善與提昇國內的資安防禦技能與產業環境。

https://www.owasp.org

OWASP 應用程式安全



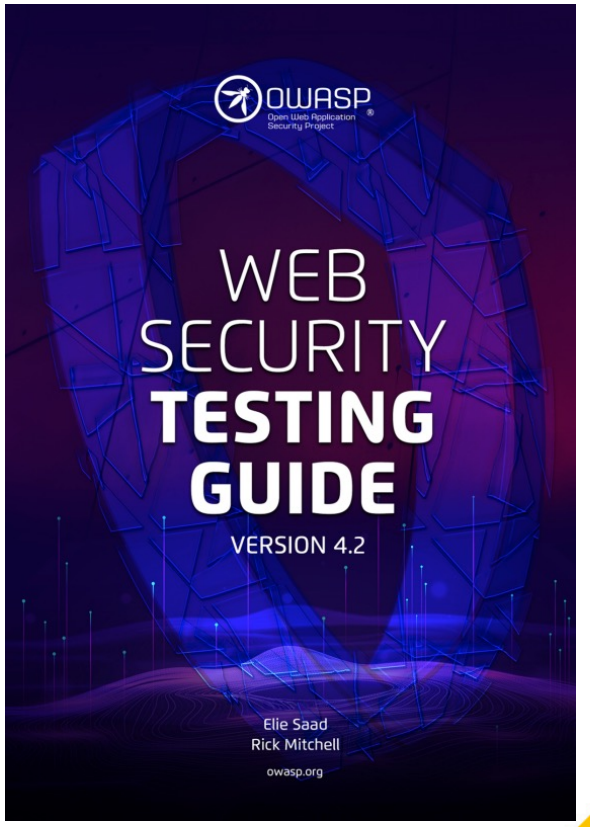
https://owasp.org/projects/

SHIELDXTREME

OWASP Top 10 : 2021

- A01 權限控制失效
- A02 加密機制失效
- A03 注入式攻擊
- A04 不安全設計
- A05 安全設定缺陷
- A06 危險與過舊的元件
- A07 認證與驗證機制失效
- A08 軟體及資料完整性失效
- A09 資安紀錄及監控失效
- A10 伺服器請求偽造

OWASP TOP10



SHIELDXTREME

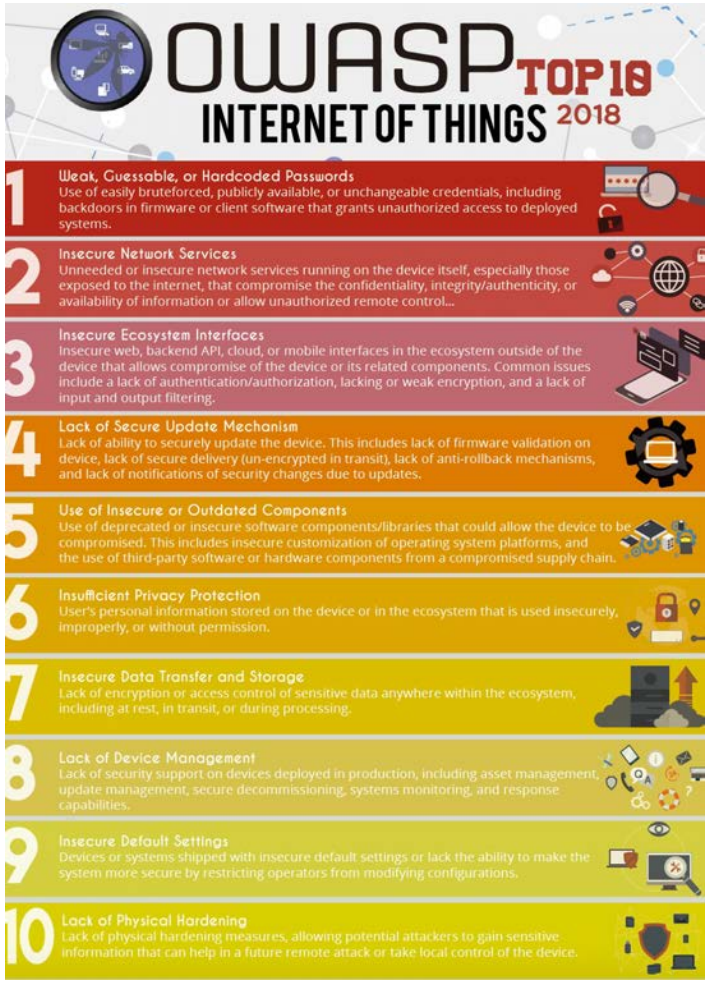
OWASP API Top 10 : 2019

- API 01 破壞物件層級的授權
- API 02 破壞使用者的認證
- API 03 過多的數據曝露
- API 04 缺少資源與速率的限制
- API 05 破壞功能層級的授權
- API 06 大量的分配
- API 07 安全配置錯誤
- API 08 注入攻擊
- API 09 資產管理不當
- API 10 日誌紀錄與監控不足

SHIELDXTREME

OWASP IoT Top 10 : 2018

- I01 脆弱可猜測或硬編碼密碼
- I02 不安全的網路服務
- I03 不安全的生態系介面
- I04 缺乏安全的更新機制
- I05 使用不安全或過時的組件
- I06 隱私保護不足
- I07 不安全的數據傳輸與儲存
- I08 缺乏設備的管理
- I09 不安全的預設配置
- I10 缺乏物理防護的硬體設計



OWASP ZAP

OWASP® Zed Attack Proxy (ZAP)

The world's most widely used web app scanner. Free and open source. Actively maintained by a dedicated international team of volunteers. A GitHub Top 1000 project.

Quick Start Guide | Download Now

Intro to ZAP

If you are new to security testing, then ZAP has you very much in mind. Check out our ZAP in Ten video series to learn more!

Automate with ZAP

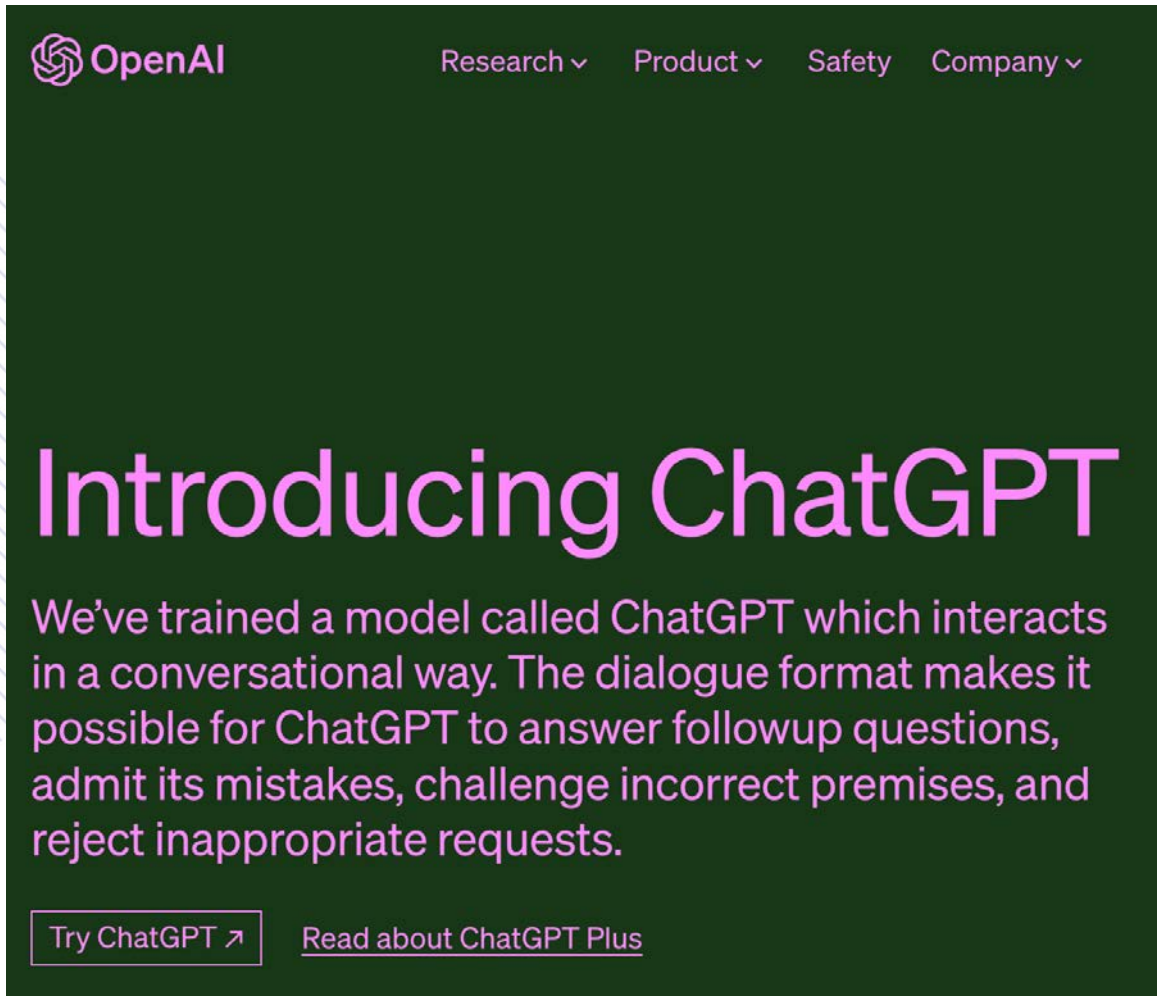
ZAP provides range of options for security automation. Check out the automation docs to start automating!

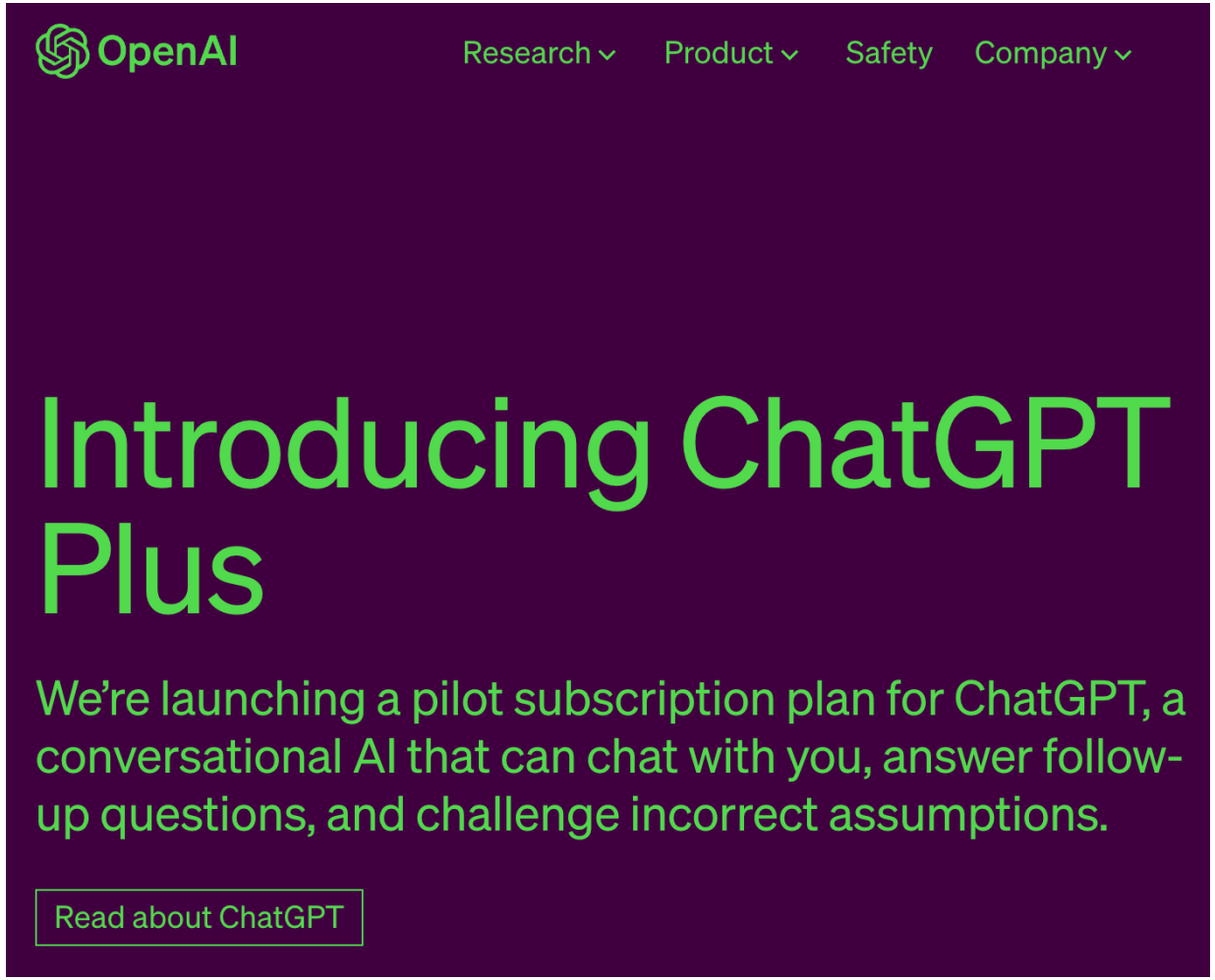
ZAP Marketplace

ZAP marketplace contains add-ons that have been contributed by the community. Check out how you can extend ZAP with the add-ons!

https://www.zaproxy.org/

最近熱門的議題

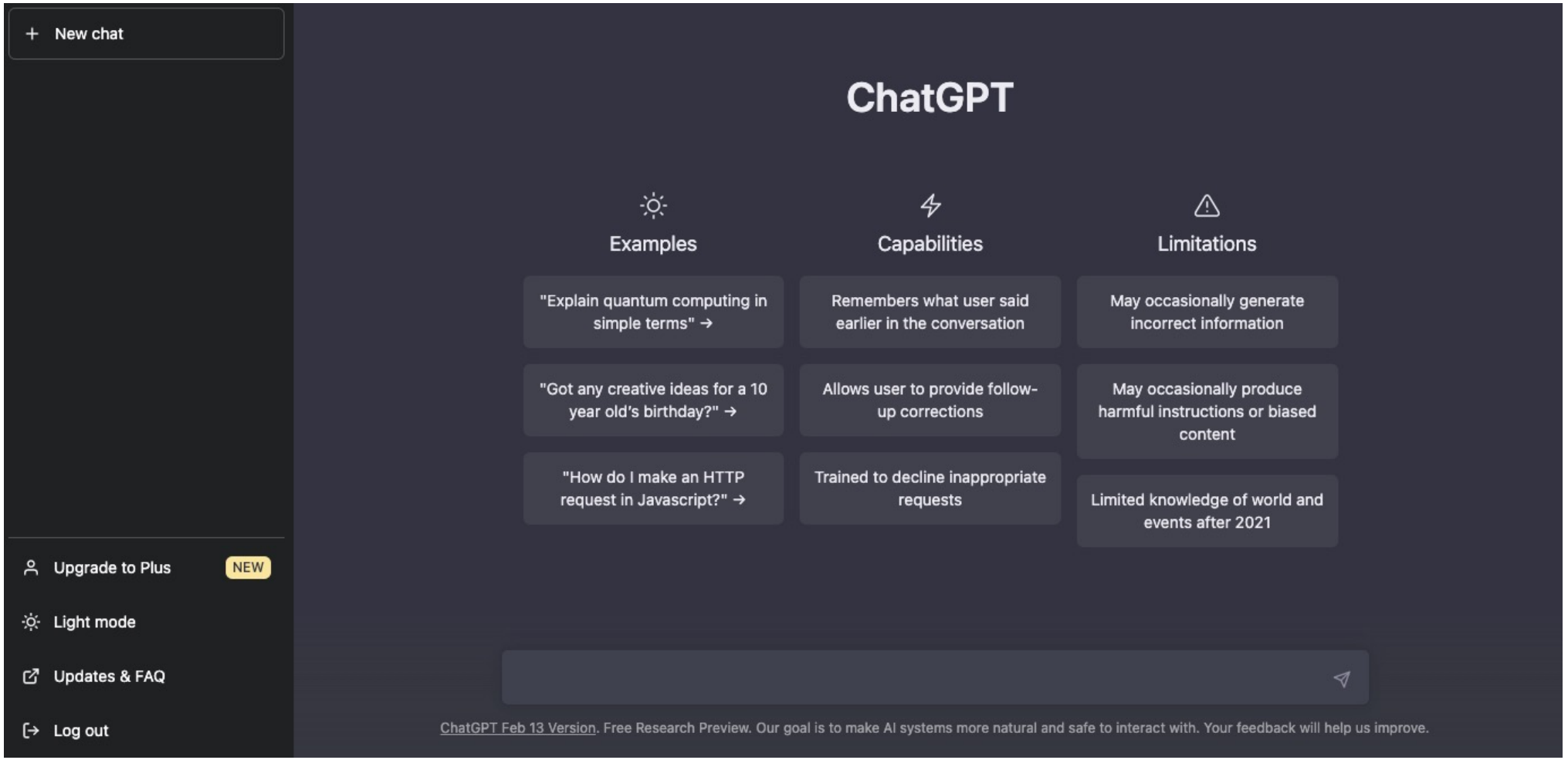




https://openai.com/blog/chatgpt

ChatGPT

聊天生成型預訓練變換模型簡稱ChatGPT，是OpenAI開發的人工智慧聊天機器人程式，於2022年11月推出。該程式使用基於GPT-3.5架構的大型語言模型並以強化學習訓練。



ChatGPT

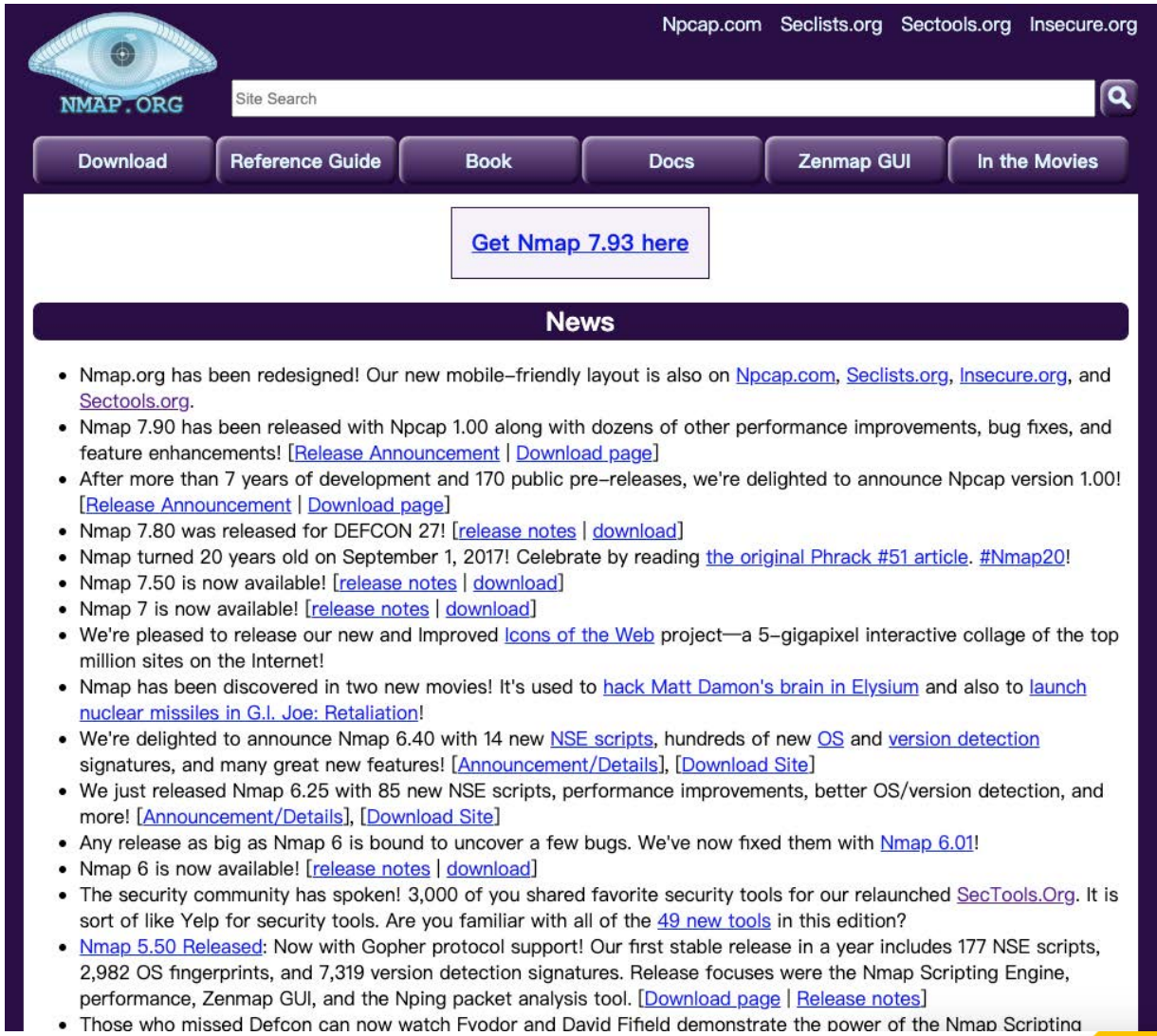
如何學習資訊安全

學習資訊安全需要深入理解各種不同的技術、工具和方法，並且需要經過長時間的實踐和經驗。以下是一些學習資訊安全的建議：

1. 開始瞭解基礎知識：了解資訊安全的基礎知識、安全威脅和漏洞等。這些知識可以從書籍、網上課程、教學視頻和網絡文章等途徑獲得。
2. 探索各種資訊安全領域：資訊安全領域很廣泛，包括網絡安全、數據庫安全、移動安全、應用程序安全等等。試著去了解並探索不同的領域，找到自己最感興趣和最適合的領域。
3. 參與資訊安全社群：加入資訊安全相關的社群和論壇，與其他資訊安全專業人士交流學習經驗，進一步提高自己的技能和知識。
4. 實踐學習：通過參與實際項目、CTF競賽等方式來實踐學習。實踐過程中遇到的問題和挑戰能夠幫助你更好地理解和應用所學知識。
5. 通過認證考試：通過相應的認證考試可以對自己的技能和知識進行評估，並獲得更多的學習和發展機會。

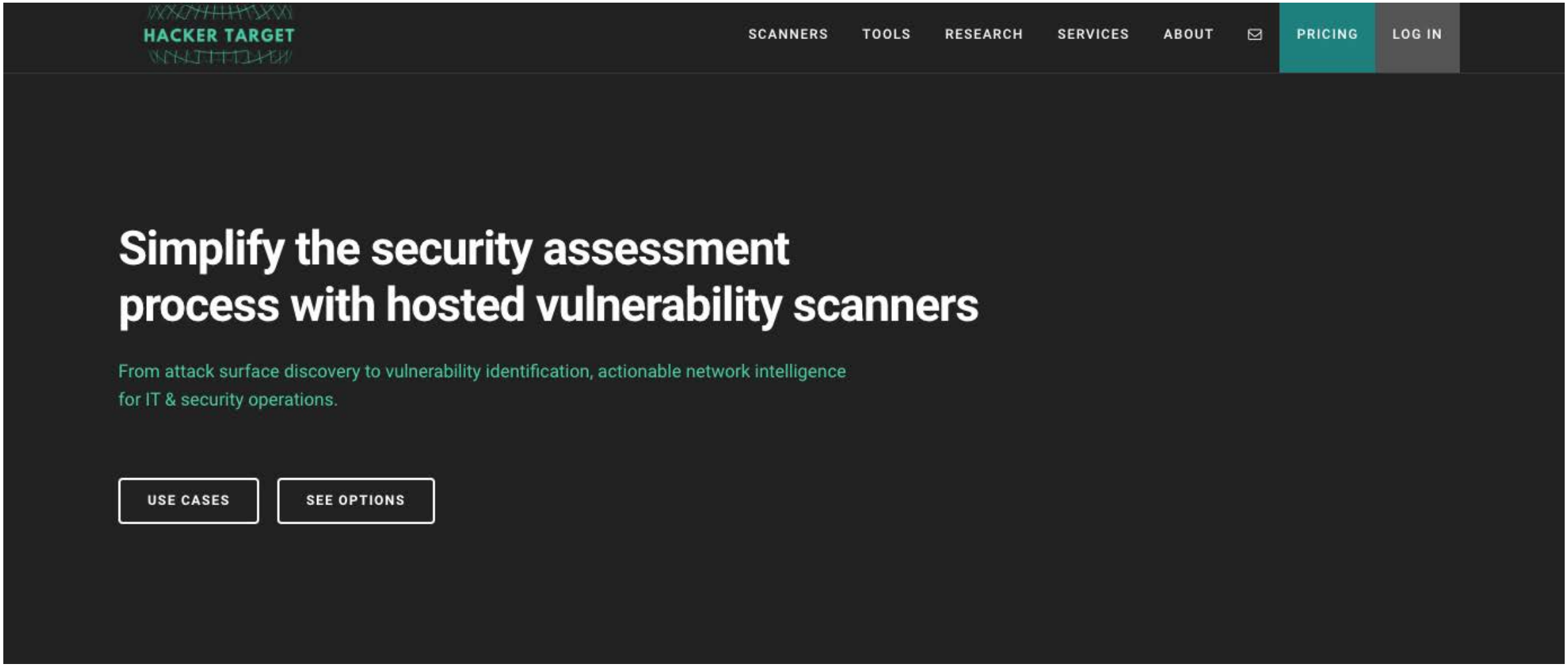
總之，學習資訊安全需要持續的學習和實踐，通過多種途徑不斷提高自己的技能和知識，並且保持對新技術和趨勢的敏銳性。

你不可不知道的網站…



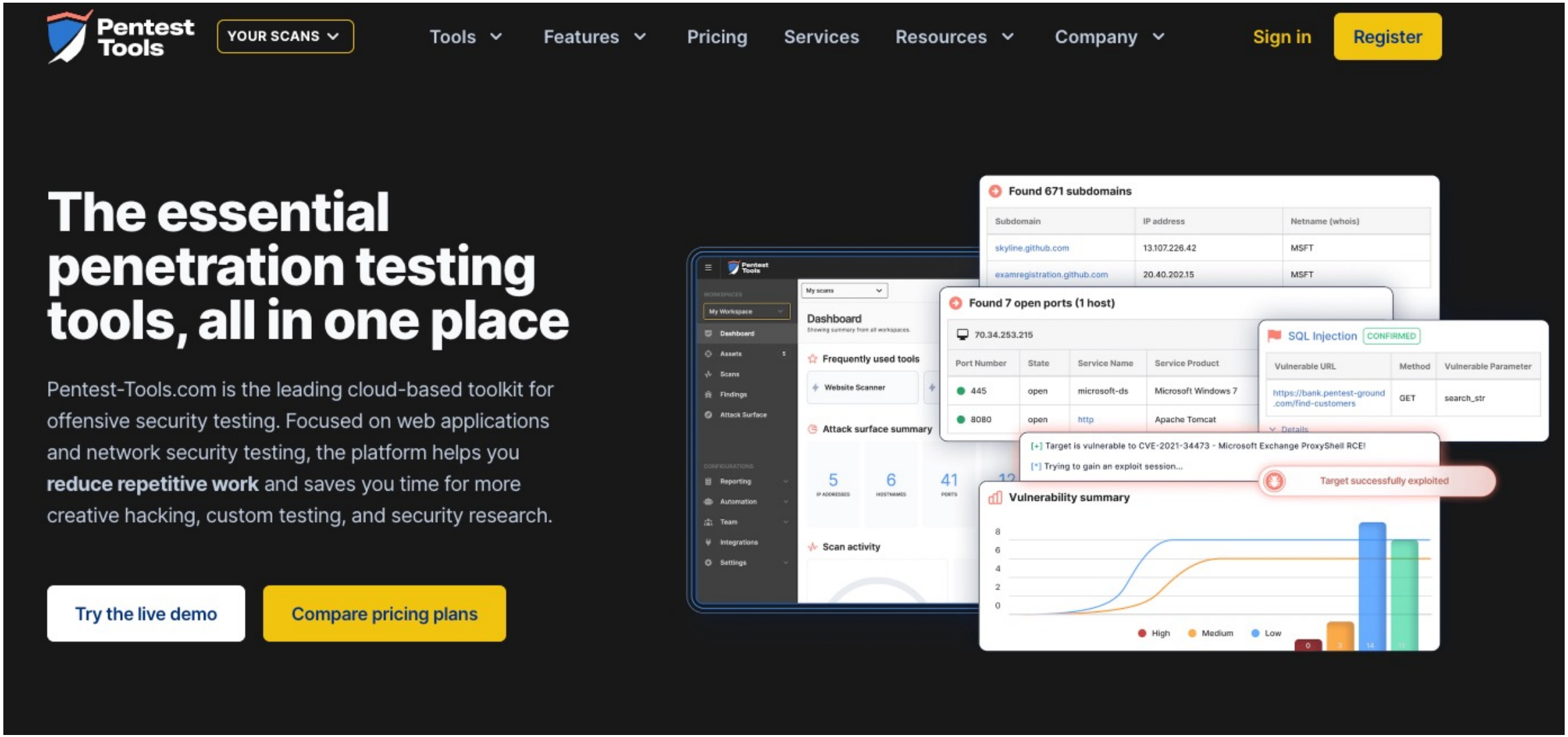
SHIELDXTREME https://sectools.org/ https://nmap.org/

On-Tools

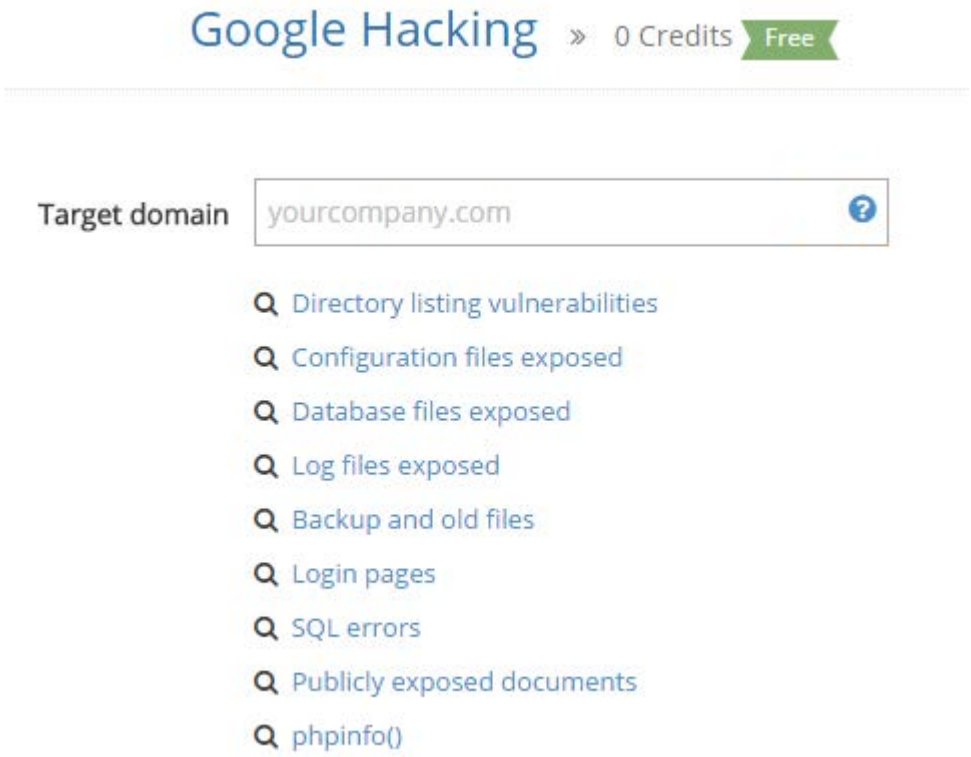


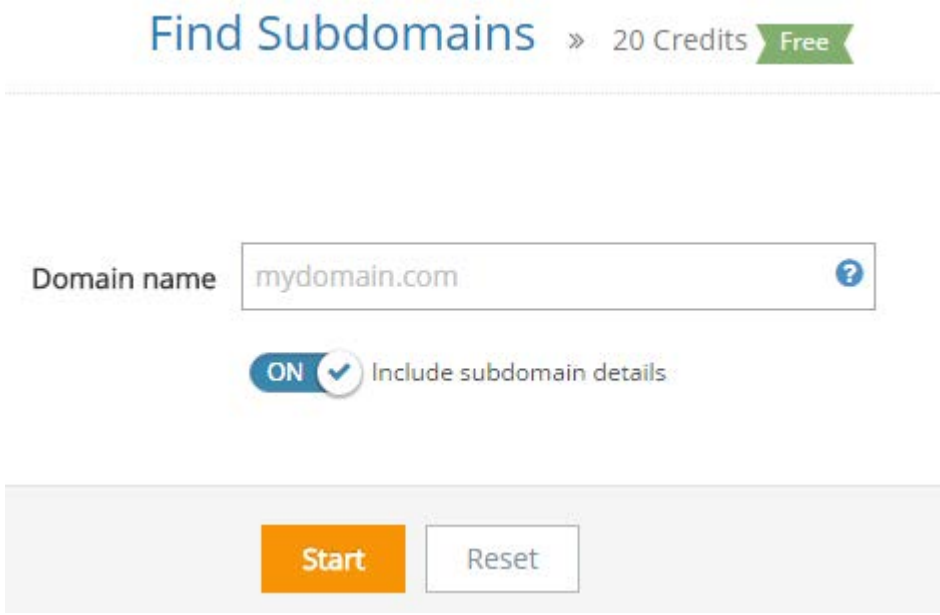
https://hackertarget.com/

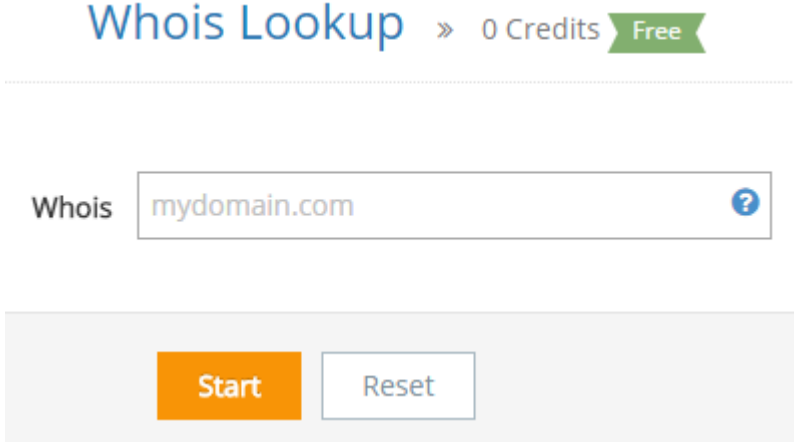
On-Line Tools



pentest-tools.com







網路安全與網路封包

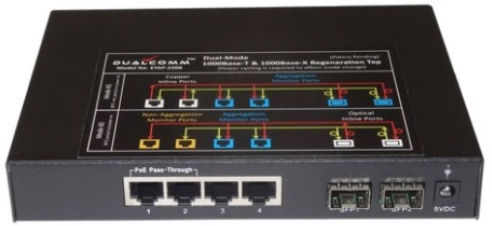
- 要存在一個絕對安全的網路環境是不太可能發生的，因為使用者的需求往往與安全是相衝突的
- 網路封包可以透露使用者的行為
- 配合不同的通訊協定，以進行各種不同的網路服務
- 常見的工具軟體
  - Tcpdump、Sniffer 、NetXRay 、Wireshark (Ethereal)、Netwitness investigator等

網路封包擷取及分析

- 網路封包擷取的需求
  - 瞭解電腦網路目前進行的動作
  - 監聽側錄另一台電腦網路連線
  - 瞭解網路程式如何運行
  - 學習網路通訊協定

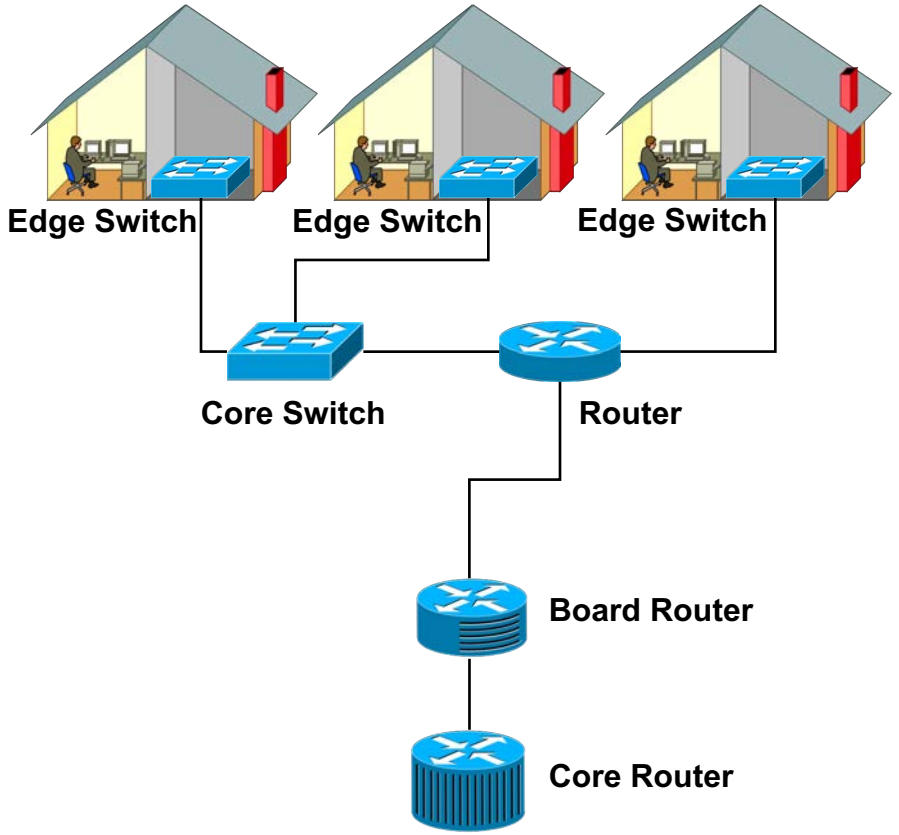
網路封包分析基礎

- 封包截取技術
  - HUB
  - Y-TAP
  - Switch
    - Port Mirror
    - Port Mapping
- 封包截取工具
  - Wireshark(Ethereal)、SnifferPro、TcpDu  ort、MS-NetMonitor、SecuServer…



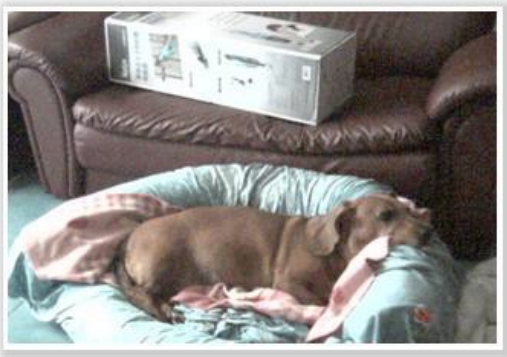
封包截取的關鍵

- 截取位置
  - Host/Server
  - Edge Switch
  - Core Switch
  - Router
  - Board Router
  - Core Router
- 過濾條件
  - 限制 or 忽略
  - 網路架構
- 差異
  - IDS/IPS/IDP —> 已知模式
  - 封包分析 —> 未知模式



另類的開放資料

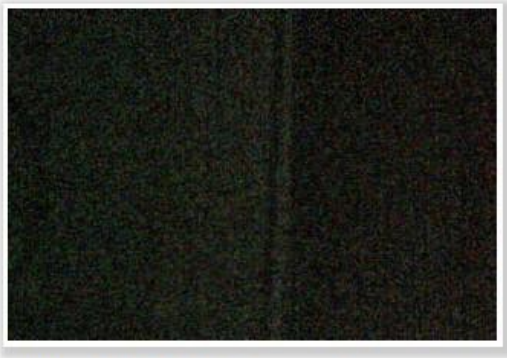
Watch NetCam camera in Taiwan, Province Of Taipei



Watch NetCam camera in Taiwan, Province Of Taipei

Watch NetCam camera in Taiwan, Province Of Taipei

Watch NetCam camera in Taiwan, Province Of Taipei



Watch NetCam camera in Taiwan, Province Of Taipei

Watch NetCam camera in Taiwan, Province Of Taipei

SHIELDXTREME

http://www.insecam.org/

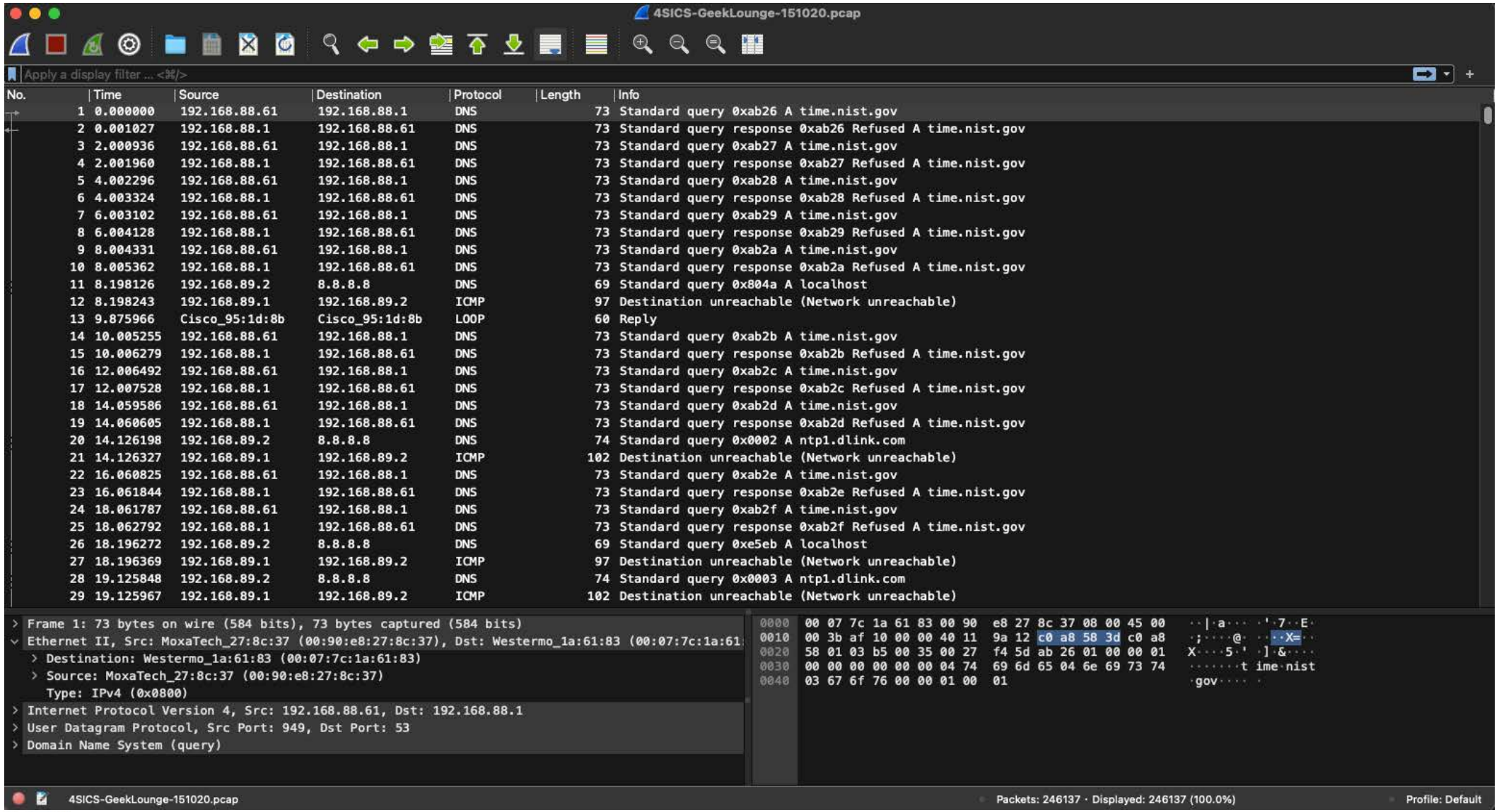
實務練習

SHIELDXTREME

WireShark

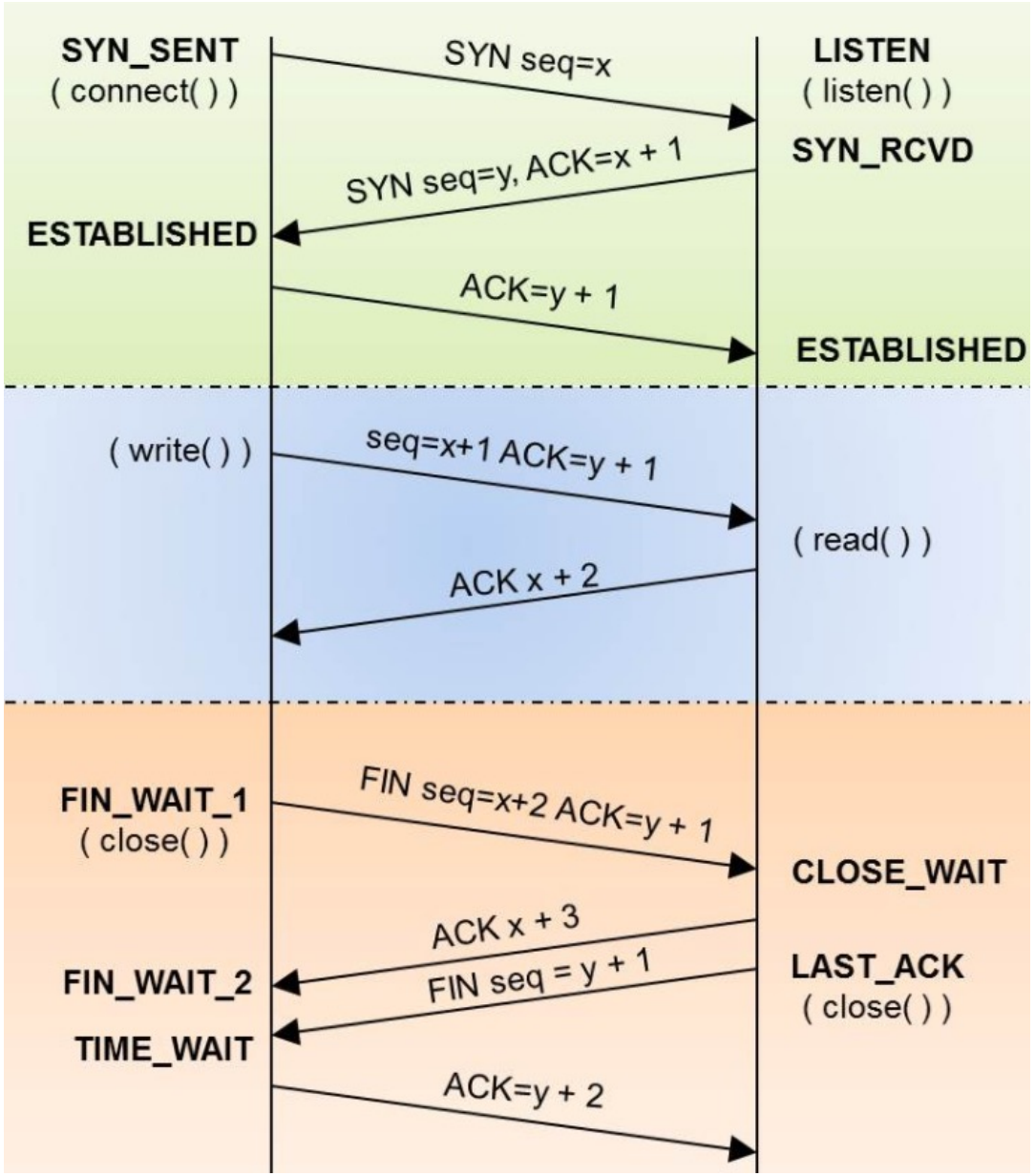
- Wireshark 的前身為Ethereal
- 支援多種作業系統，為免費且功能強大的
- 開放原始碼軟體
- 目前可以解析700+通訊協定
- 圖形化的操作界面，具備排序與過濾的功能
- 亦能夠支援無線網路的環境
- Honeynet Project Extensions
  - WireShnork
  - WireshAV
- https://www.wireshark.org/

WireShark


4SICS-GeekLounge-151020.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab26 A time.nist.gov
2 0.001027 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab26 Refused A time.nist.gov
3 2.000936 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab27 A time.nist.gov
4 2.001960 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab27 Refused A time.nist.gov
5 4.002296 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab28 A time.nist.gov
6 4.003324 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab28 Refused A time.nist.gov
7 6.003102 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab29 A time.nist.gov
8 6.004128 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab29 Refused A time.nist.gov
9 8.004331 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2a A time.nist.gov
10 8.005362 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2a Refused A time.nist.gov
11 8.198126 192.168.89.2 8.8.8.8 DNS 69 Standard query 0x804a A localhost
12 8.198243 192.168.89.1 192.168.89.2 ICMP 97 Destination unreachable (Network unreachable)
13 9.875966 Cisco_95:1d:8b Cisco_95:1d:8b LOOP 60 Reply
14 10.005255 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2b A time.nist.gov
15 10.006279 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2b Refused A time.nist.gov
16 12.006492 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2c A time.nist.gov
17 12.007528 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2c Refused A time.nist.gov
18 14.059586 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2d A time.nist.gov
19 14.060605 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2d Refused A time.nist.gov
20 14.126198 192.168.89.2 8.8.8.8 DNS 74 Standard query 0x0002 A ntp1.dlink.com
21 14.126327 192.168.89.1 192.168.89.2 ICMP 102 Destination unreachable (Network unreachable)
22 16.060825 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2e A time.nist.gov
23 16.061844 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2e Refused A time.nist.gov
24 18.061787 192.168.88.61 192.168.88.1 DNS 73 Standard query 0xab2f A time.nist.gov
25 18.062792 192.168.88.1 192.168.88.61 DNS 73 Standard query response 0xab2f Refused A time.nist.gov
26 18.196272 192.168.89.2 8.8.8.8 DNS 69 Standard query 0xe5eb A localhost
27 18.196369 192.168.89.1 192.168.89.2 ICMP 97 Destination unreachable (Network unreachable)
28 19.125848 192.168.89.2 8.8.8.8 DNS 74 Standard query 0x0003 A ntp1.dlink.com
29 19.125967 192.168.89.1 192.168.89.2 ICMP 102 Destination unreachable (Network unreachable)
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Ethernet II, Src: MoxaTech_27:8c:37 (00:90:e8:27:8c:37), Dst: Westermo_1a:61:83 (00:07:7c:1a:61
Destination: Westermo_1a:61:83 (00:07:7c:1a:61:83)
Source: MoxaTech_27:8c:37 (00:90:e8:27:8c:37)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.88.61, Dst: 192.168.88.1
User Datagram Protocol, Src Port: 949, Dst Port: 53
Domain Name System (query)
0000 00 07 7c 1a 61 83 00 90 e8 27 8c 37 08 00 45 00
0010 00 3b af 10 00 00 40 11 9a 12 c0 a8 58 3d c0 a8
0020 58 01 03 b5 00 35 00 27 f4 5d ab 26 01 00 00 01
0030 00 00 00 00 00 00 04 74 69 6d 65 04 6e 69 73 74
0040 03 67 6f 76 00 00 01 00 01
4SICS-GeekLounge-151020.pcap
Packets: 246137 · Displayed: 246137 (100.0%)
Profile: Default

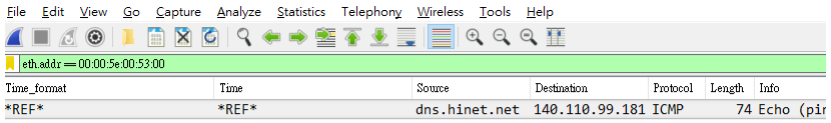
封包過濾

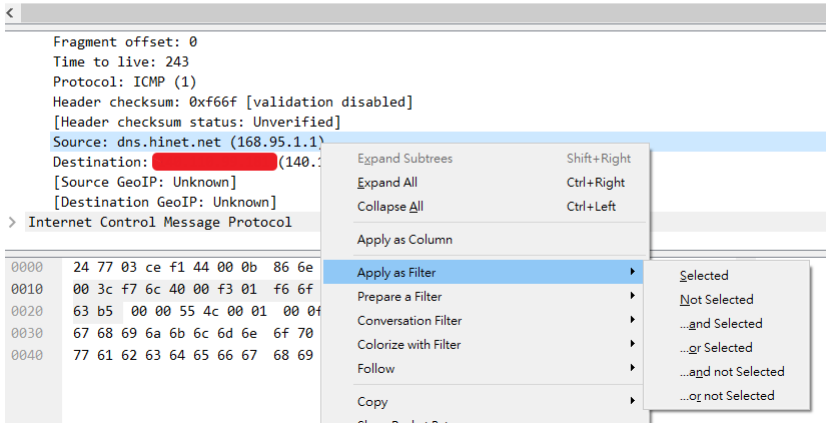
- 為什麼要過濾封包?
- 如何過濾封包



封包過濾-條件

- ip.addr == 192.168.1.1
- ip.src == 168.95.1.1
- ip.addr == 2001:db8:85a3::1016
- ip.host == dns.hinet.net
- eth.addr 11:22:33:44:55:66
- tcp.port == 80
- tcp.port != 80
- tcp.srcport == 12345
- tcp.dstport == 80





封包過濾-條件

- icmp
- icmp.type == 8 || icmp.type == 0
- icmp[0] == 3
- tcp.flags == 0x002(SYN)
- tcp.flags == 0x011 (FIN,ACK)
- tcp.flags == 0x010 (ACK)
- tcp.flags == 0x012 (SYN,ACK)
- tcp.flags == 0x018 (PSH,ACK)

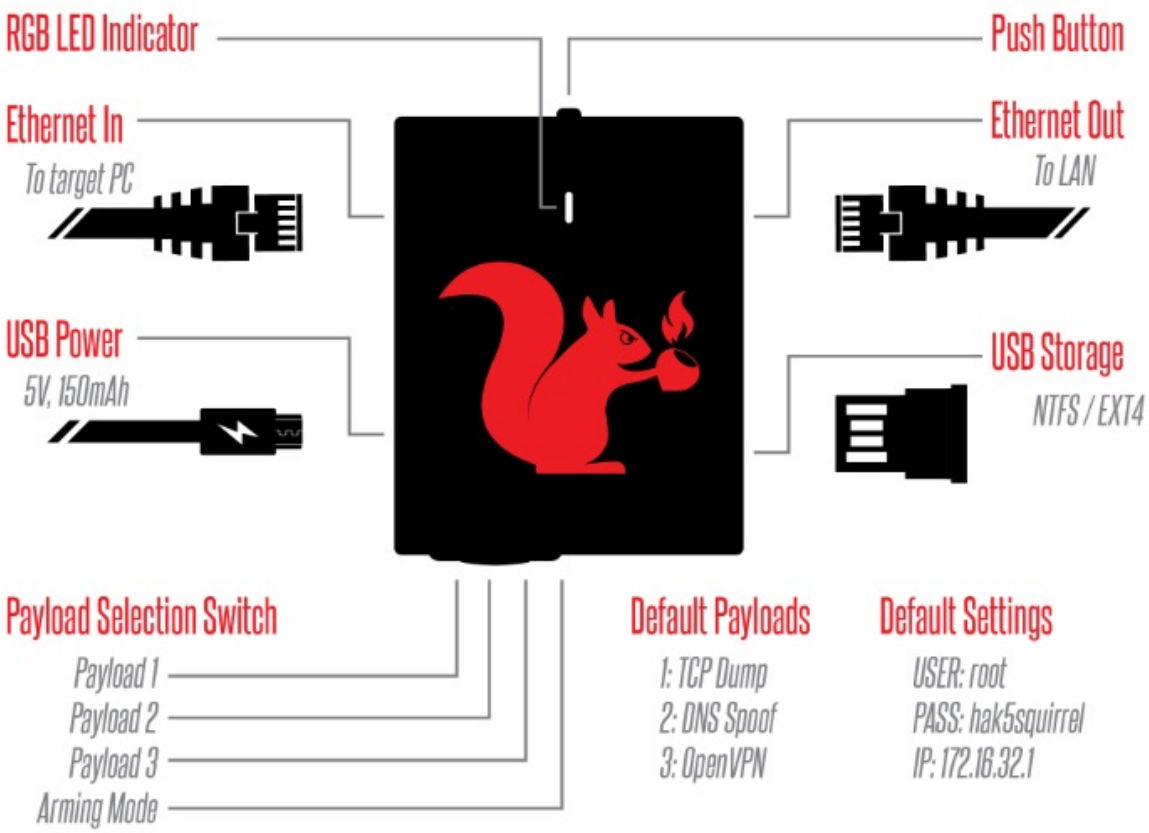
- http://rapid.web.unc.edu/resources/tcp-flag-key/

封包過濾-條件

- tcp.port != 3389 <清除 RDP 流量>
- tcp.flags.syn == 1 <含有syn flag 的封包>
- tcp.flags.rst == 1 <含有rst flag 的封包>
- !arp 清除 ARP 流量
- smtp || pop || imap 查看 email 流量

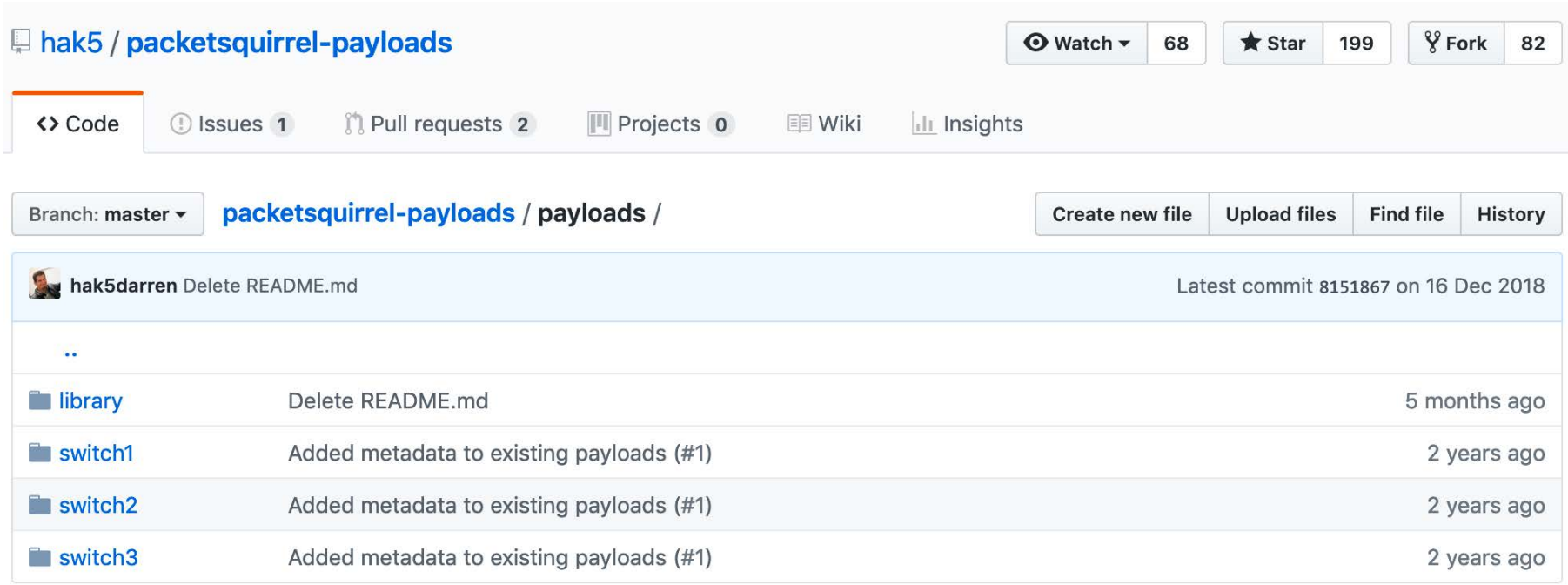
Packet Squirrel

- The man-in-the-middle that's nuts for networks



Packet Squirrel

- Payload
  - TCP Dump
  - DNS Spoof
  - OpenVPN



Workshop – 網路封包分析練習

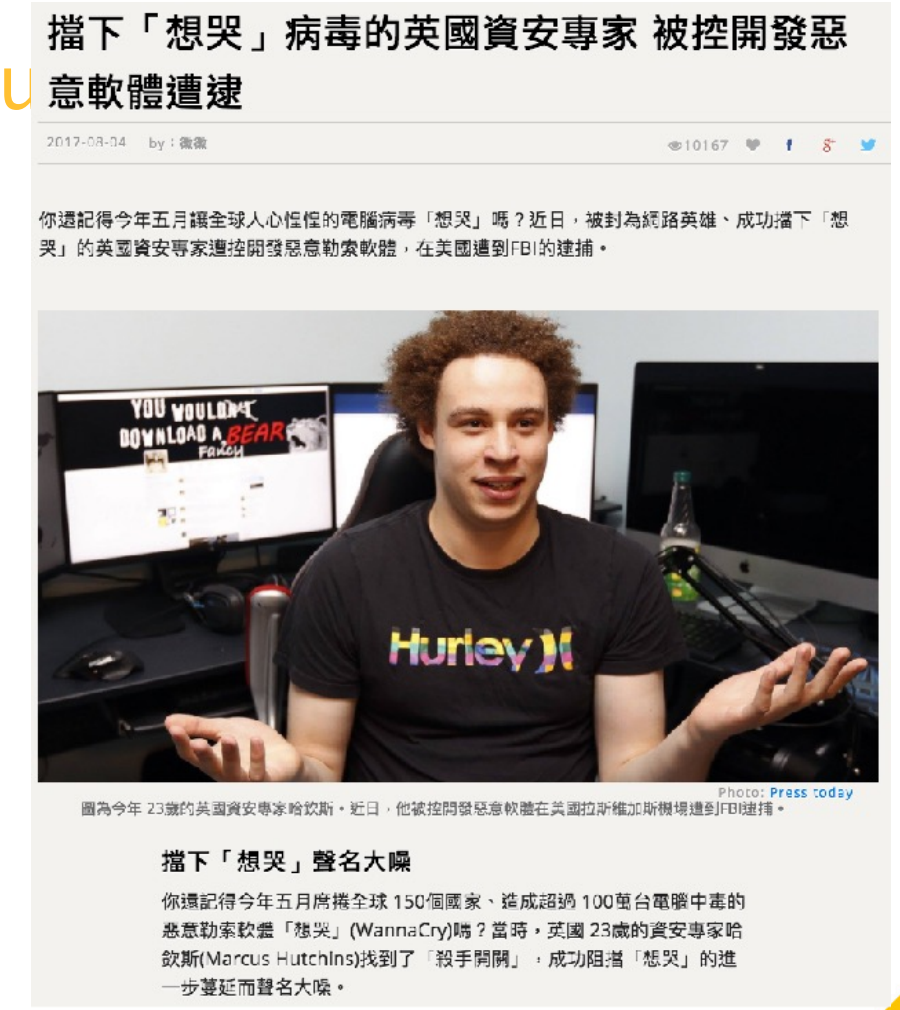
- 本練習在 X-Range 上進行實作

WannaCry大規模來襲

- 惡意程式加上勒索，針對系統重大弱點進行自動化攻擊與散佈

WannyCry造成的影響

- 資安研究，有時候是一體的兩面
- 特殊的網域名稱iuqerfsodp9ifjaposdfjhgosu



擋下「想哭」病毒的英國資安專家 被控開發惡意軟體遭逮

2017-08-04 by：薇薇 10167

你還記得今年五月讓全球人心惶惶的電腦病毒「想哭」嗎？近日，被封為網路英雄、成功擋下「想哭」的英國資安專家遭控開發惡意勒索軟體，在美國遭到FBI的逮捕。

Photo: Press today

圖為今年 23歲的英國資安專家哈欽斯。近日，他被控開發惡意軟體在美國拉斯維加斯機場遭到FBI逮捕。

擋下「想哭」聲名大噪

你還記得今年五月席捲全球 150個國家、造成超過 100萬台電腦中毒的惡意勒索軟體「想哭」(WannaCry)嗎？當時，英國 23歲的資安專家哈欽斯(Marcus Hutchins)找到了「殺手開關」，成功阻擋「想哭」的進一步蔓延而聲名大噪。

https://dq.yam.com/post.php?id=8002

DNS記錄與WannaCry

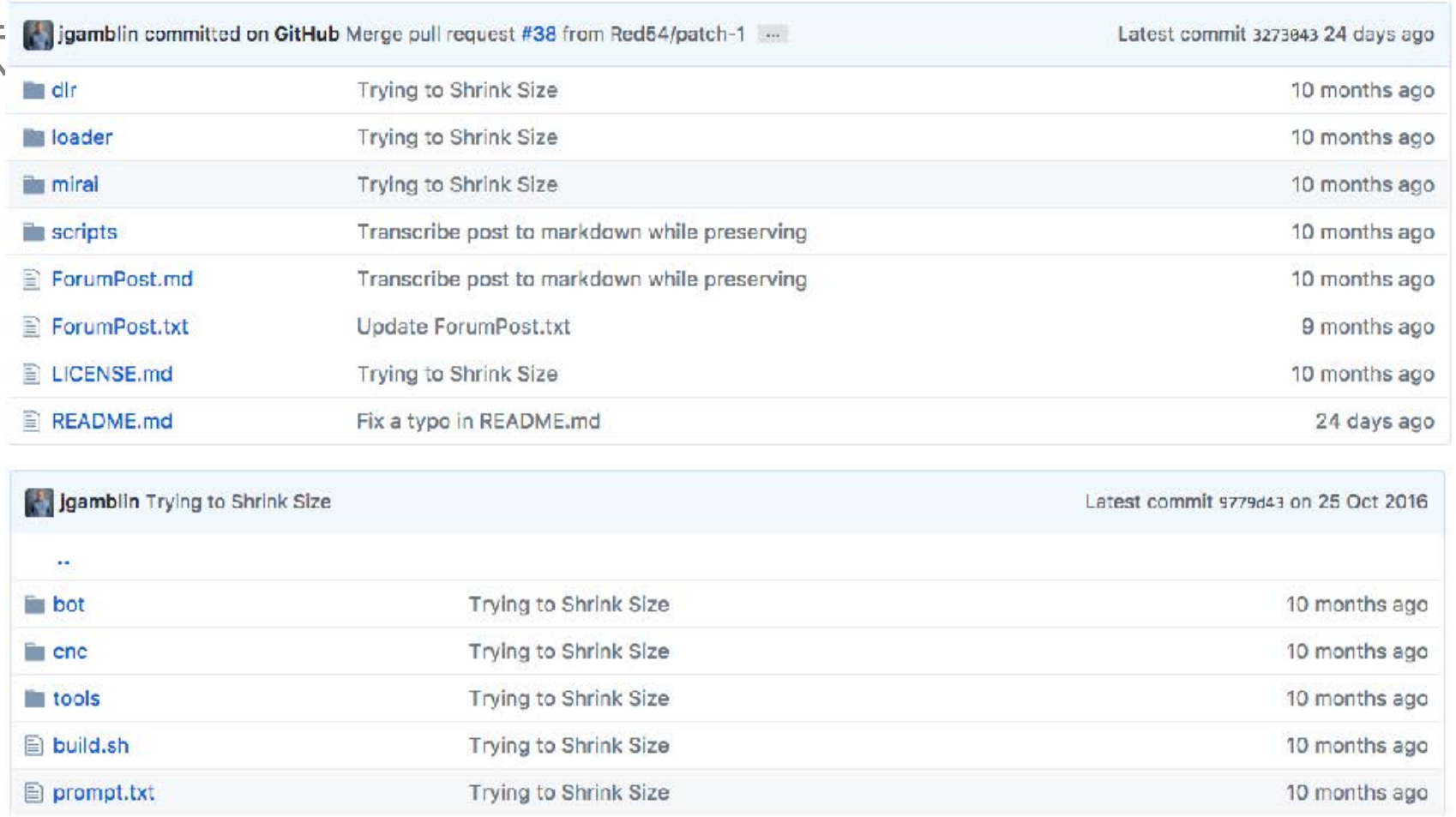
>	17/07/05 23:14:17.000	Jul 05 15:14:17 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87026 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14323232?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.38.137 end=Jul 05 2017 23:13:47 CST externalId=14323232 proto=TCP sourceDnsDomain=78-user127.cc.ncut.edu.tw src=140.128.78.127 start=Jul 05 2017 23:13:47 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline
>	17/07/05 21:26:42.000	Jul 05 13:26:42 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=86756 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312974?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:26:12 CST externalId=14312974 proto=TCP sourceDnsDomain=95-user169.lib.ncut.edu.tw src=140.128.95.169 start=Jul 05 2017 21:26:12 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline
>	17/07/05 21:21:25.000	Jul 05 13:21:25 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87049 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312456?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:20:48 CST externalId=14312456 proto=TCP sourceDnsDomain=t2.ba.dep-appoint.static.012.ippool.cyut.edu.tw src=120.110.27.12 start=Jul 05 2017 21:20:48 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline
>	17/07/05 21:21:13.000	Jul 05 13:21:13 10.0.1.18 CEF:0|Lastline|Enterprise|7.10|signature-match|IDS Signature Match|6|act=LOG cat=sinkhole/Sinkhole.Tech cn1=65 cn1Label=impact cn2=87049 cn2Label=IncidentId cn3=65 cn3Label=IncidentImpact cnt=1 cs1=e92b3400:30fbe7df:665e1ca2 cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/2870691410/4107789788/14312456?event_time\=2017-07-05 cs2Label=EventDetailLink cs3=http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ cs3Label=EventUrl deviceExternalId=2870691410:4107789788 dpt=80 dst=104.17.37.137 end=Jul 05 2017 21:20:48 CST externalId=14312456 proto=TCP sourceDnsDomain=t2.ba.dep-appoint.static.012.ippool.cyut.edu.tw src=120.110.27.12 start=Jul 05 2017 21:20:48 CST host = 10.0.1.28 source = udp:666 sourcetype = syslog-for-lastline

Mirai Botnet

- Mirai可以讓執行Linux的計算系統成為被遠端操控的「殭屍」，以達到通過殭屍網路進行大規模網路攻擊的目的
- Mirai的主要感染物件是可存取網路的消費級電子裝置，例如網路監控攝錄影機和家庭路由器等。
- Mirai構建的殭屍網路已經參與了幾次影響廣泛的大型分散式阻斷服務攻擊，包括2016年9月20日針對電腦保安撰稿人布萊恩・克萊布斯個人網站的攻擊、對法國網站代管商OVH的攻擊，以及2016年10月Dyn公司網路攻擊事件
- Mirai的原始碼已經以開源的形式發布，其中的技術也已被其他一些惡意軟體採用

Mirai Botnet

- 當軍火庫被打開時
- 開發攻擊用的惡意



jgamblin committed on GitHub Merge pull request #38 from Red64/patch-1 ... Latest commit 3273843 24 days ago

dlr	Trying to Shrink Size	10 months ago
loader	Trying to Shrink Size	10 months ago
mirai	Trying to Shrink Size	10 months ago
scripts	Transcribe post to markdown while preserving	10 months ago
ForumPost.md	Transcribe post to markdown while preserving	10 months ago
ForumPost.txt	Update ForumPost.txt	9 months ago
LICENSE.md	Trying to Shrink Size	10 months ago
README.md	Fix a typo in README.md	24 days ago

jgamblin Trying to Shrink Size Latest commit 9779d43 on 25 Oct 2016

..

bot	Trying to Shrink Size	10 months ago
cnc	Trying to Shrink Size	10 months ago
tools	Trying to Shrink Size	10 months ago
build.sh	Trying to Shrink Size	10 months ago
prompt.txt	Trying to Shrink Size	10 months ago

https://github.com/jgamblin/Mirai-Source-Code

VirusCheck

- Virus Check相較於僅進行靜態分析之國際檢測系統，更增添了動態分析之優勢，補足了防毒軟體的不足之處，以獲得完整之分析成果。除此之外，此系統可透過上傳之檔案，建構專屬於台灣之惡意程式資料庫，完整國家資安防線
- 使用者上傳檔案後，系統會以防毒軟體進行靜態分析，同時交予沙箱進行動態分析，將靜態與動態分析同時且互補地檢驗，以達到最佳檢測成效
- 待檢驗完畢後，系統會透過風險值告知使用者該檔案可能為惡意程式之風險為多少，並提供完整檢測報告供使用者下載

惡意檔案檢測服務

Virus Check

Integrate static and dynamic cybersecurity analyzing skills;

Detect hidden malware in a comprehensive manner

https://viruscheck.tw/

Workshop – 惡意程式分析練習

- 本練習在 X-Range 上進行實作