專題題目是:白帽的攻擊目標與調查蒐集的實測

White Hat's Attack Target and Investigation Collected By Actaul Measurements

學生：蔡典彤

指導教授：辛錫進

國立聯合大學 資訊工程學系

苗栗市南勢里聯大 2 號

{U0818015}@o365.nuu.edu.tw

hsin@nuu.edu.tw

摘要

攻擊目標的是美國國防部為範例，列為目標的滲透測試包含五項行程，偵察與足跡、掃描網路、列舉分析、弱點分析和系統入侵，以及入侵類型目前只有的惡意軟件工具。磨練練習使用不同系統的指令練習和以此範例為主的進行演練練習來檢測美國國防部的安全性和機密性。

調查蒐集的實測是情蒐關於唐納．約翰．川普的個人資料包含相關所有一切，以了解美國白宮以及美國本土對政治人物前美國總統的網路與資料的保密性，以及以了解美國人的網路隱私的公開保護性的了解程度上，有多容易困難性在取得紀錄。

關鍵詞:情蒐、滲透測試、資訊安全、白帽駭客、美國

Abstract

The target of the attack is the US Department of Defense as an example. The penetration test listed as the target includes five procedures, reconnaissance and footprints, network scanning, enumeration analysis, vulnerability analysis and system hacking, and the intrusion type is currently only a malware tool. Honing exercises test DoD security and confidentiality using command exercises of different systems and practice exercises based on this paradigm.

The actual measurement collected by the investigation is about Donald. John. Trump's personal information contains everything related to understanding the secrecy of the White House and the United States on the network and data of former US presidents of politicians, as well as the degree of public protection of Americans' online privacy. How easy and difficult it is to get the record.

Keywords: intelligence search, penetration testing, information security, white hat hackers,US country

第一章、緒論

白帽是泛指駭客以從事資訊安全、網路檢測、熟知國家在網路法律、從事服務於資安和網路安全為服務的企業和教職工作者為工作職業的駭客。

調查蒐集是一種透過各種方式的蒐集資訊。情報蒐集既是各個國家穩定基礎也是企業第一手資料情報的成功先決條件。情報蒐集罪犯和失蹤人口的用於警偵與白帽的核心技巧之一。

攻擊目標，常見公司委託白帽進行弱點掃描和滲透測試，駭客需要透過專門網頁專門工具選定、鎖定攻擊目標的弱點，並且制定侵入攻擊目標計畫。

1.1 研究背景

白帽是駭客的常見類型裡的一個分類。調查蒐集是一種調查員常常使用的核心技巧。更甚至攻破企業的網站後，駭客撰寫所寫的檢測建議書，推薦改善系統部分的信和電子郵件。也是不少駭客心儀想加入它世界知名百大企業的常常使用的投名狀。知名企業也會舉辦對外競賽，對攻破該公司系統的駭客們提供獎金和獎品，甚至職位。白帽駭客透過系統源代碼工具調查蒐集失蹤人口和嫌疑犯犯罪者。本實測為滲透測試的步驟也是攻擊以前的情蒐，請勿輕易嘗試熟讀相關法律避免觸法。

第二章、系統架構

2.1 Parrot 系統架構

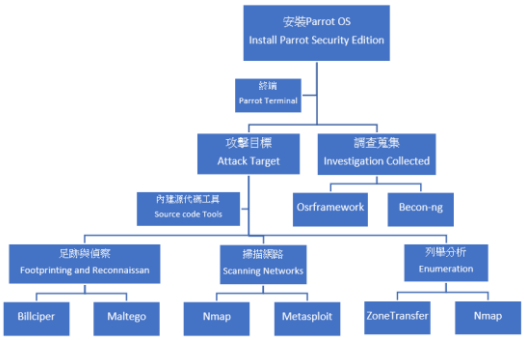

圖 1 Parrot Security Edition (OS) method main flow chart

2.2 Windows 10 系統架構

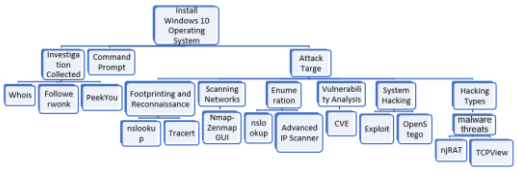

圖 2 Windows 10/11 Windows Operating System's method main flow chart

第三章、調查蒐集實測分析

3.1 ParrotOS 情蒐, Donald Trump 的隱私個人資料

(一)Osrframework

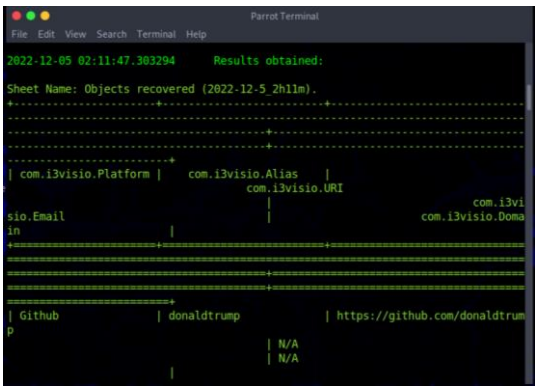

圖 3 (mailfy.py 將為收集資訊 e-mail 帳號的收集資訊的命令。)

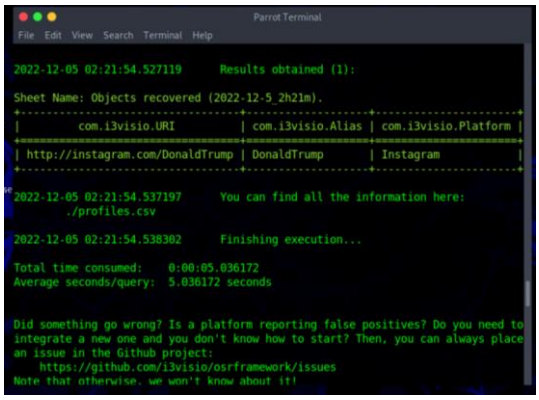

圖 4 (-n 是匿稱列表的過程，-p 是為了給平台查詢使用）（usufy.py 檢查從 instagram（不同）社交網站平台給予的使用者細節的檔案資料的存在性的命令）

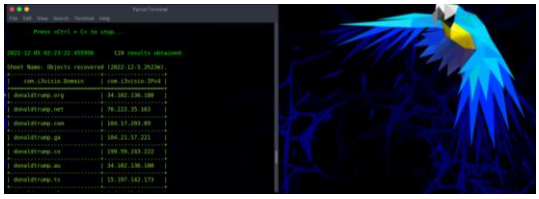

圖 5 (domainfy.py 使用關鍵字 donaldtrump 和匿稱檢查存在的域的存在性的命令。)

(二)Recon-ng 利用人名搜尋 DonaldTrump

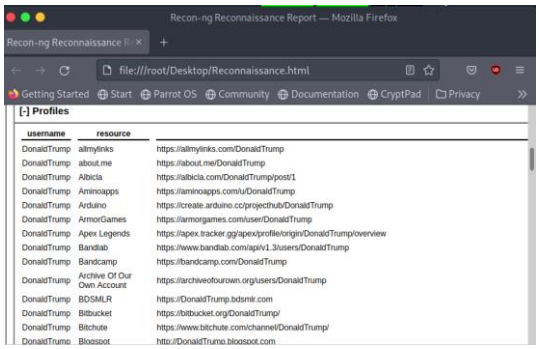

圖 6 使用者名稱 DonaldTrump 在公開網站的來源和網址 URL，儲存於 Desktop 結果報告

3.2 Windows 情蒐, Donald Trump 人名搜尋

(一)PeekYou 利用人名搜查我喜歡的美國前總統川普(Donald . John . Trump)

PeekYou 美國英文名字搜尋美國各地各州的隱私，PeekYou:跟前美國川普同姓的同地區的相似人名叫 Donald T.的個人資料家裡地址, 電話號碼, 社交網路平台關係掃描, 人名的照片, 法院紀錄

(二)Followerwonk

這張 Twitter 圖片為我自己做展示影片素材截圖，為前美國唐納川普在離開 Twitter 還在當美國白宮前對外所發表自己想法的公共社交平台推文

第四章、攻擊目標實測分析

4.1 ParrotOS 滲透測試, 美國國防部 (www.defense.gov)

(一)Billciper 足跡測試:美國 IP 位址, 美國所在地區跟城市, 地圖緯度

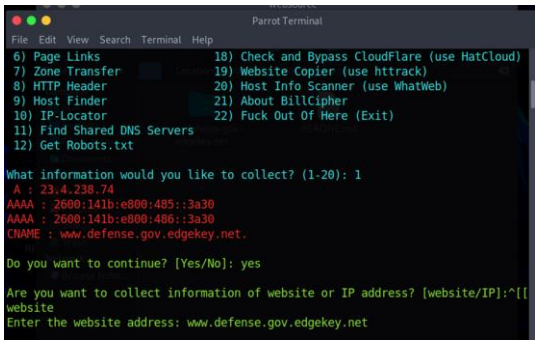

圖 7 DNS 加密過美國國防部

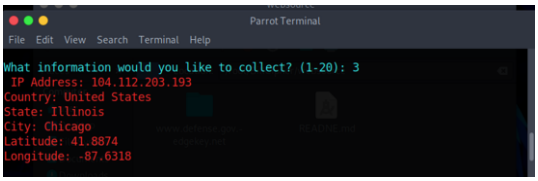

圖 8 美國 IP 位址, 所在地區跟城市, 地圖緯度

(二)Maltego：包含其他像是，DNS Name、電子郵件伺服器、網域名稱，etc

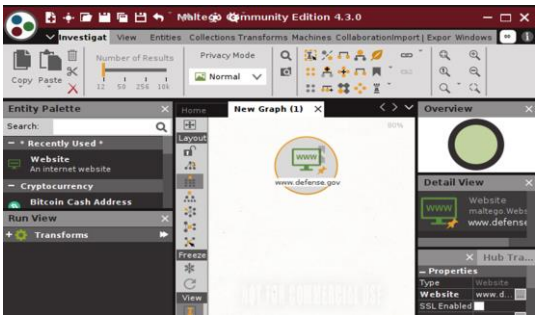

圖 9 Maltego Graph 的圖形主頁

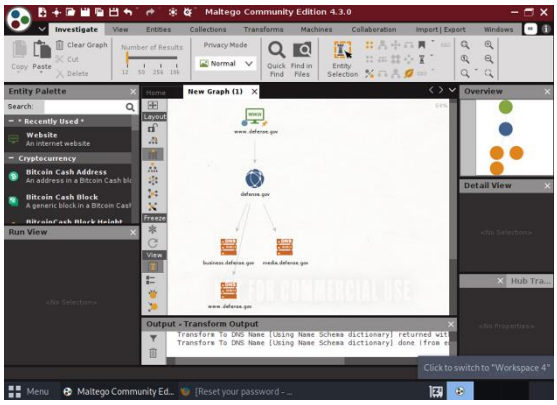

圖 10 Maltego : DNS 名稱（DNS Name）

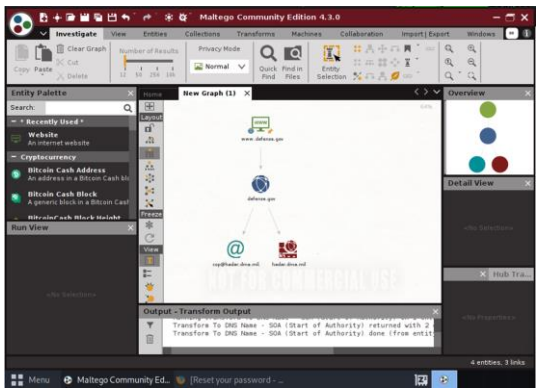

圖 11 Maltego ： 名稱伺服器和電子郵件

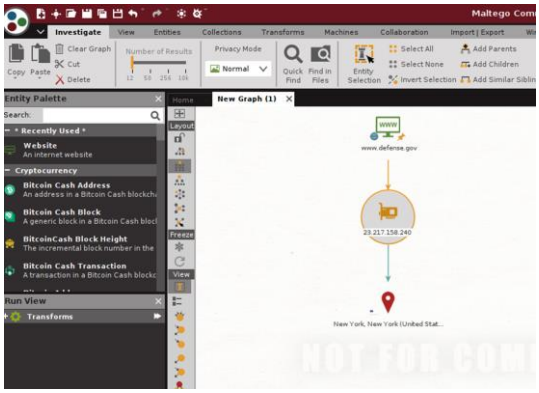

圖 12 Maltego : 美國所在地

(三)Recon-ng 偵查測試：使用暴力破解方法是國防部的主機們 Hosts 和網站主域 Domains 和 Suffix

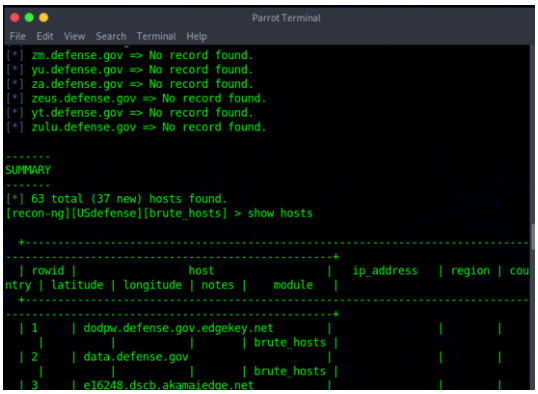

圖 13 [*] 63 total (37 new) hosts found。

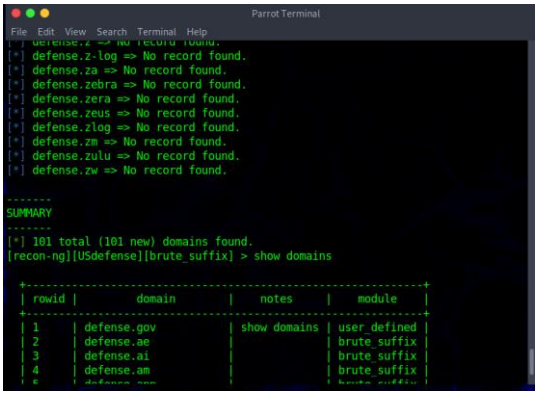

圖 14 [*] 101 total (101 new) hosts found。

(四)Metasploit 掃描網路

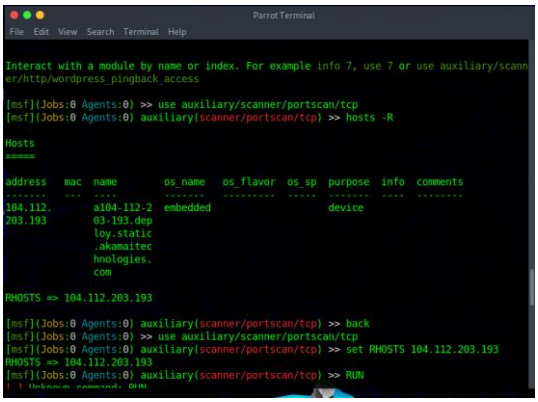

圖 15 網路掃描結果成果(一)，輸入命令 use auxiliary/scanner/ports an/tcp，ENTER。執行 TCP 掃描。

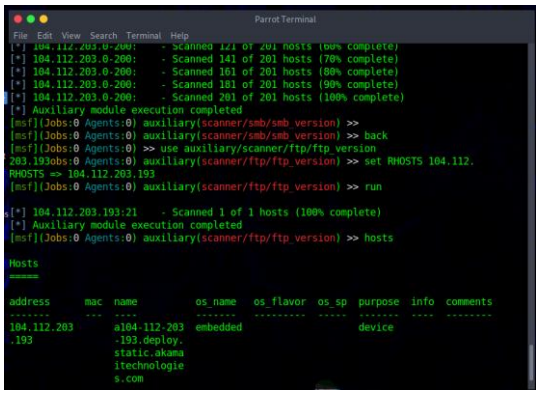

圖 16 網路掃描結果成果(二)，輸入命令 use auxiliary/scanner/ftp/ftp_version，ENTER。執行 FTP 掃描。

(五)Nmap 掃描網路和列舉分析

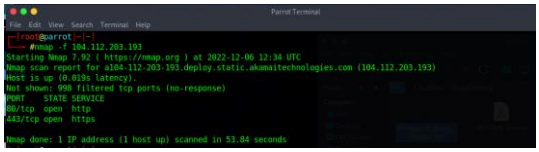

圖 17 逃避的 IDS 和防火牆中間過程(二)

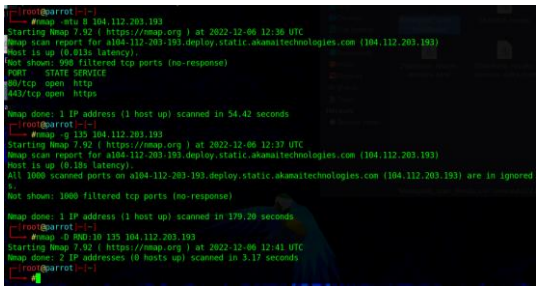

圖 18 逃避的 IDS 和防火牆中間過程(二)

(六)ZoneTransfer 用 DNS 列舉分析的 ns 返回名稱伺服器的結果和區域檢索的報告回應

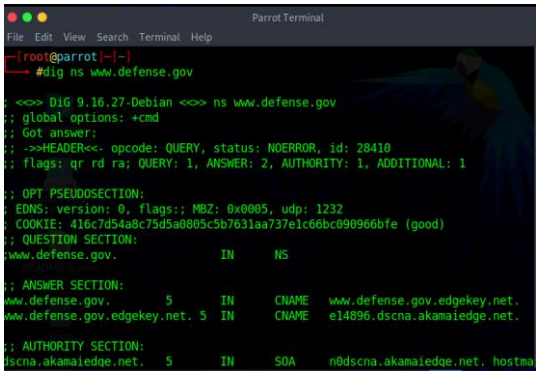

圖 19 dig ns www.defense.gov。(ns 返回名稱伺服器在結果中。)

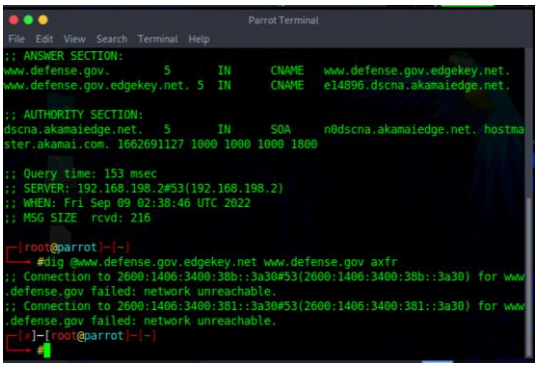

圖 20 @www.defense.gov.edgekey.net www.defense.gov axfr，(axfr 檢索區域信息。)

4.2 Windows10 滲透測試, 美國國防部 (www.defense.gov)

(一)Exploit Site

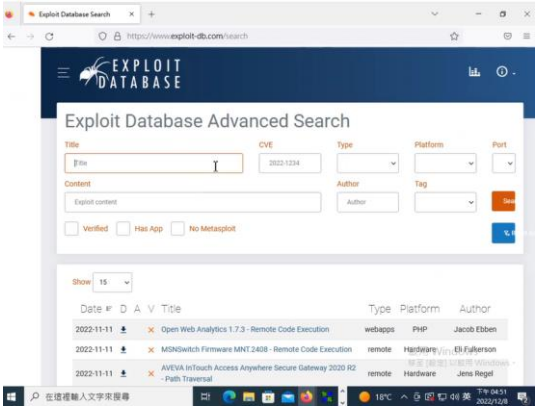

圖 21 ExploitDatabase 搜尋引擎與條件選擇項目

(二)OpenStego

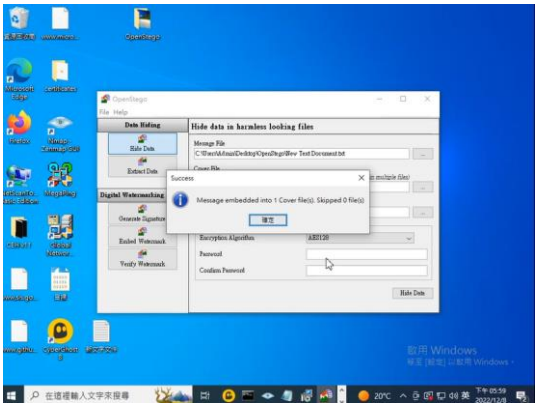

圖 22 OpenStego 原圖片隱寫術資訊信息

(八)njRAT 惡意軟件

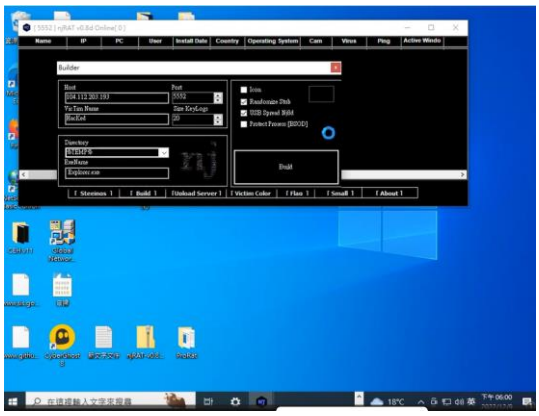

圖 23 njRAT 安裝 Trojan 木馬後門程式的 exe 檔案的 Builder，njRAT 安裝的 Builder 的 run 運行中的後門與病毒檔，njRAT 最後我製造的名字叫 Text.exe 的後門與病毒檔

(三)入侵類型白帽利用 TCPView 查看惡意軟件

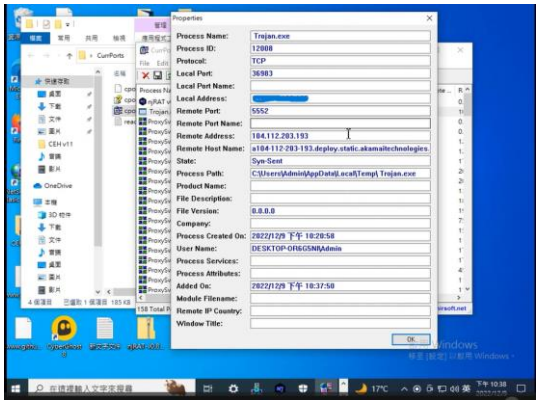

圖 24 找到在本機電腦中已雙擊開啟的已建立 Trojan 後門程式，查看 Trojan 後門程式詳細細節與細部資訊

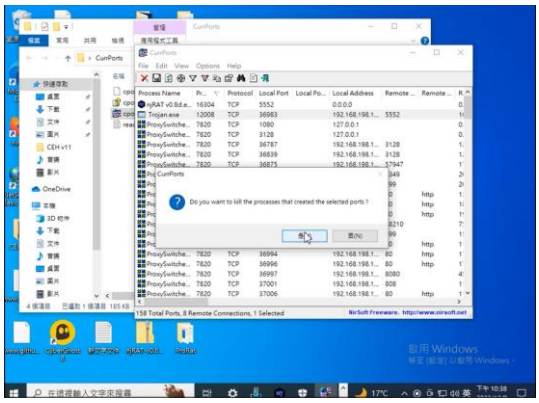

圖 25 KILL THE TROAJAN 在電腦中，自己下製造的後門運行中就是自己殺掉，以後別人在我本機電腦中下的後門我就能殺掉，結束。

第五章、結論

其結論乃是，發現不斷顯示美國國防部(www.defense.gov)的 IP 位址乃加密過並且轉換過的非 Windows 系統桌面應用，乃是 Linux 系統桌面應用的虛擬機器，大部分或者全部端口掃描顯示轉換過 VPN 與 IP 位址，而且其開放 TCP 的端口(Port)的 443/tcp 和 80/tcp 可能性大是假電腦，不是蘋果筆電所使用的 ios 系統以及以及少數韓國的筆電大部分手機所使用運行的 Android 作業系統，而是以古早傳統使用和電腦工程師常見下終端指令的 Linux 作業系統的虛擬機器，也是掃描網路到列舉分析的成果。系統入侵是 Exploit Site 其他駭客所偵查到的公司網站, etc 的各種不同漏洞利用並且允許公開下載免費分享在網路上。其他的實測方法和結果包含，例如：njRAT 建立遠端入侵的後門木馬程式(Trajon)、TCPView 也是白帽所用於偵測到並移出後門木馬程式的方法，最後移出有被安裝後門木馬程式。

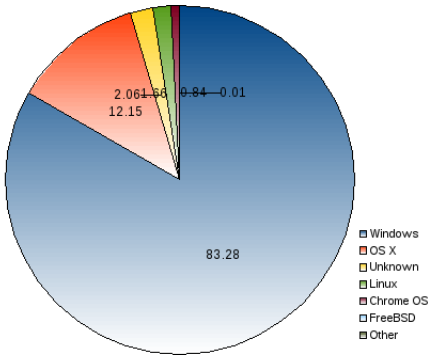

圖 26 2017 年桌電的作業系統市場占有率的全世界比率圓餅圖

調查蒐集的實測是情蒐關於唐納・約翰・川普(英文名，Donald John Trump)的結果在 PeekYou 的數據人名搜尋發現該表面上看似付費的專門英文網站，查看搜尋報告需要先留下信用卡付費資料和收件電子郵件的搜尋者的真實資訊，而且上面只有同類似名 Donald John Trump 的美國人，不知道是否是網路騙錢的以先提供的真假美國人的隱私個資和法院犯罪紀錄，獲取得結果之前美國英文網站他要先取得你的信用卡付錢(姓名、地址、開卡公司)和你的真實電子郵件。

參考文獻

〔1〕CEH v11 Certified Ethical Hacker，Exam 312-50 Certified Ethical Hacker，EC-council，2020(電子書)。

〔2〕bahatiphill/BillCipher: Information Gathering tool for a ... - GitHub，網址：https://github.com/bahatiphill/BillCipher。

〔3〕Maltego 維基百科，網址：https://en.m.wikipedia.org/wiki/Maltego

〔4〕Metasploit 維基百科，網址：https://zh.m.wikipedia.org/zh-tw/Metasploit

〔5〕Maltego 維基百科，網址：https://en.m.wikipedia.org/wiki/Maltego

〔6〕TCPView v4.17，網址：https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview。

〔7〕Advanced IP Scanner 官網，網址：https://www.advanced-ip-scanner.com/。

〔8〕CVE 維基百科，網址：https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures。

〔9〕CVE-Process，網址：https://nvd.nist.gov/general/cve-proces。

〔10〕接尾辭，維基百科:https://zh.m.wikipedia.org/zh-tw/%E6%8E%A5%E5%B0%BE%E8%BE%AD

〔11〕Desktop Operating System Percentage Market Share Worldwide (As of September 2017)，網址：https://stats.areppim.com/stats/stats_osxsnapshot.htm