

6. 被動資訊偵搜

勞動部 產業人才投資計畫
中國文化大學 推廣教育部

張耀鴻 副教授
2022年 暑期班

綱要

- 做筆記
- 網站偵搜
- whois枚舉
- Google hacking
- Netcraft
- Recon-ng
- 開源程式碼
- Shodan
- 安全標頭掃描器
- SSL伺服器測試
- Pastebin
- 使用者資訊搜集
- 社交媒體工具
- 堆疊溢位
- 資訊搜集框架

何謂OSINT

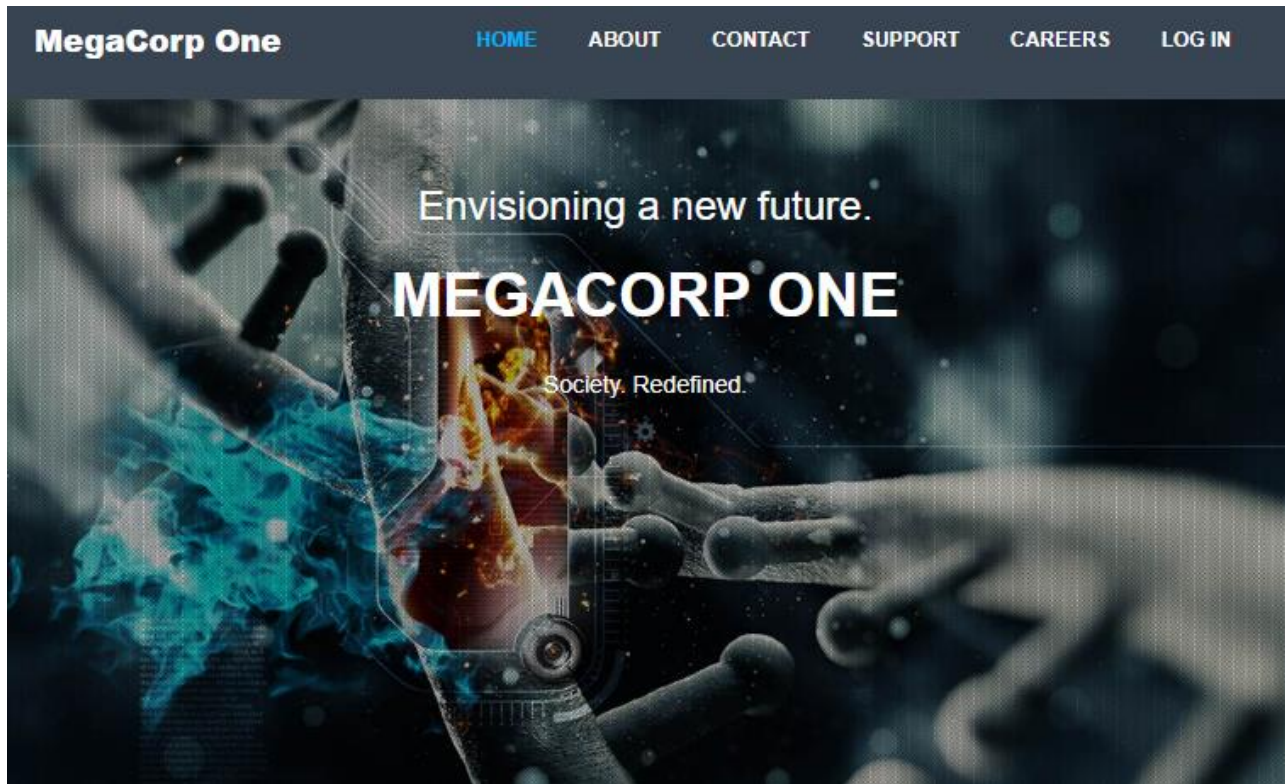
- 被動資訊搜集（也稱為開源情報或OSINT）是收集有關目標的公開可用資訊的過程，通常沒有任何直接與目標互動
- 被動資訊收集的最終目標是獲得清楚的攻擊目標的初步資訊，以便成功開展網路釣魚活動，或支援其他滲透測試步驟(例如密碼猜測)
- 在較為寬鬆的解釋中，所謂「被動」意味著可能會與目標互動，但只能像普通的Internet使用者那樣
- 例如，如果目標網站允許我們註冊帳戶，我們可以這樣做。但是不會在此階段測試網站的漏洞

做筆記

- 資訊搜集活動可以產生大量資料
- 重要的是如何妥善管理這些資料，以便在進一步的探索中利用它，或在以後的階段使用它
- 如果能保持詳細和格式良好的筆記，可能會發現以後更容易檢索資訊

網站偵搜

- 透過單純地瀏覽網站即可搜集基本資訊，以下用 MegaCorp One 這家虛構的公司為例 (<https://www.megacorpone.com/>)




MegaCorp One 網站速覽

- 快速瀏覽網站可得知這是一家奈米科技公司
- 在 **About** 的網頁顯示了一些員工的姓名、email、twitter 帳號等資訊
- 這些資訊可以用來在社交媒體上做進一步資訊收集活動


MegaCorp One [HOME](#) [ABOUT](#) [CONTACT](#) [SUPPORT](#) [CAREERS](#) [LOG IN](#)

About.


MEET OUR TEAM




Joe Sheer
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: [@Joe_Sheer](https://twitter.com/Joe_Sheer)



Tom Hudson
WEB DESIGNER
Email: thudson@megacorpone.com
Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)



Tanya Rivera
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)



Matt Smith
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

企業社交媒體帳號

- 同一頁面上的企業社交媒體帳號也值得進一步研究，這些資訊應該加以記錄：

About

MegaCorp One ©2019. All rights reserved

This is a fictitious company, brought to you by [Offensive Security](#).

Social Media



Location

2 Old Mill St
Rachel, NV 89001
United States.

whois枚舉

- *Whois* 是一種TCP服務、工具和資訊庫，可以提供有關網域名稱的資訊，例如名稱伺服器 and 註冊商
- 這些資訊通常是公開的，因為註冊商對於不公開的帳號會收取額外的費用
- 將網域 `megacorpone.com` 傳給whois 執行標準轉發搜尋可收集有關網域的基本資訊

```
$ whois megacorpone.com
Domain Name: MEGACORPONE.COM
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2021-06-15T17:59:57Z
Creation Date: 2013-01-22T23:01:00Z
Registry Expiry Date: 2024-01-22T23:01:00Z
```


whois揭露了域名

- 從whois的輸出中，可發現一些有價值的資訊
- 首先，揭露了域名是由Alan Grofield所註冊

```
Registry Registrant ID:  
Registrant Name: Alan Grofield  
Registrant Organization: MegaCorpOne  
Registrant Street: 2 Old Mill St
```

- 而在該公司的Contact頁面，可以得知Grofield為IT和資安總監

Name: Alan Grofield

Title: IT and Security Director

Email: agrofield@megacorpone.com

whois揭露了Name Server

- 我們還找到了 MegaCorp One 的名稱伺服器，這是 DNS 的一個元件，應該將這些伺服器添加到筆記

```
Name Server: NS1.MEGACORPONE.COM  
Name Server: NS2.MEGACORPONE.COM  
Name Server: NS3.MEGACORPONE.COM
```

- 除了收集有關 DNS 名稱資訊的標準正向查找之外，whois客戶端還可以執行反向查找
- 反向查找的結果為我們提供了有關IP位址是託管給誰的資訊。這些資訊以後可能會有用，與我們收集的所有資訊一樣，應將其添加到筆記中

whois揭露誰託管IP位址

- 假設我們有一個 IP 地址，我們可以執行反向查找以收集有關它的更多資訊：

```
kali@kali:~$ whois 38.100.19.70
...
NetRange:      38.0.0.0 - 38.255.255.255
CIDR:          38.0.0.0/8
NetName:       COGENT-A
...
OrgName:       PSINet, Inc.
OrgId:         PSI
Address:       2450 N Street NW
City:          Washington
StateProv:     DC
PostalCode:    20037
Country:       US
RegDate:
Updated:       2015-06-04
Comment:       rwhois.cogentco.com
Ref:           https://rdap.arin.net/registry/entity/PSI
```

Exercise 6-1

- 使用whois工具查出MegaCorp One的名稱伺服器

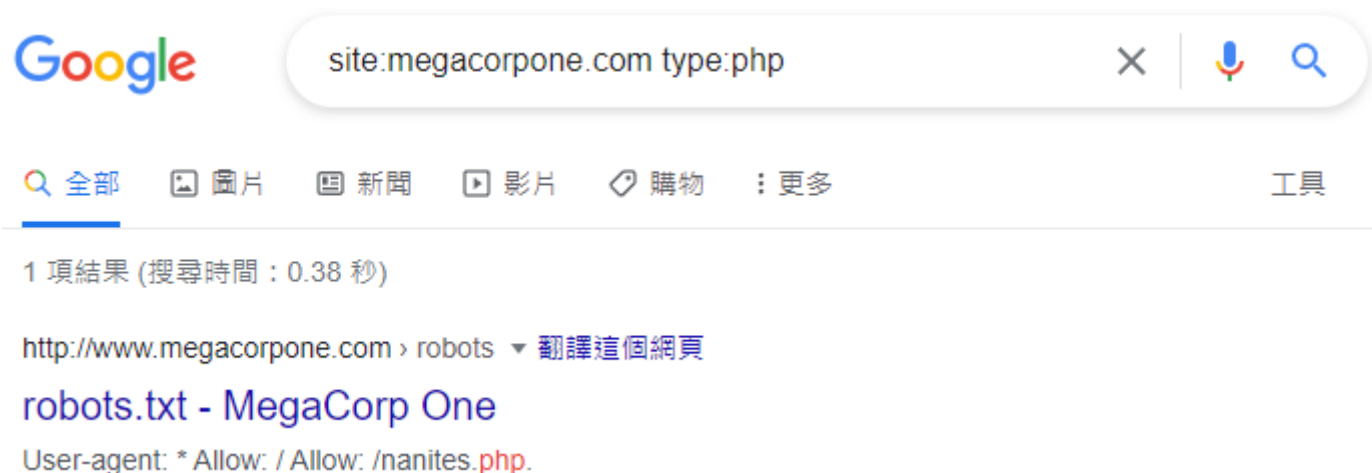
Google Hacking

- Google hacking技術的核心是巧妙的運用搜尋字串和運算子，創造性地改造查詢過程
- 這個過程是疊代反覆進行的，從廣泛的搜尋開始，然後縮小範圍以過濾掉不相關或不感興趣的結果
- **site**運算子將搜尋限制為單一網域。我們可以用這個運算子來大致了解一個組織的網路概觀：



filetype, type

- 我們可以進一步使用其他運算子來縮小搜尋結果
- 例如，檔案類型（**filetype**, **type**或**ext**）運算子將搜尋結果限制為指定的檔案類型。
- 本例結合運算子來找到**www.megacorpone.com**（**site:megacorpone.com**）上的PHP 檔（**type:php**）：



ext

- *ext*運算子也有助於辨別網站上可能使用的程式語言
- 像是*ext:jsp* 、 *ext:cfm* 、 *ext:pl*的搜尋將分別找到索引的Java伺服器頁面、 Coldfusion和Perl頁面
- 還可以用-修改運算子以從搜尋中排除特定的項目，從而縮小結果範圍

"-"運算子

- 例如，要查找有趣的非HTML 頁面，我們可以用 **site:megacorpone.com** 將搜索限制在 megacorpone.com 和子網域，後面跟著 **-type:html** 從結果中排除HTML頁面：



intitle

- 用於搜尋標題內的各種關鍵字，例如，
intitle:"index of" "parent directory"可尋找標題包含"index of"而且內容包含"parent directory"的網頁



Google Hacking Database (GHDB)

- GHDB (<https://www.exploit-db.com/google-hacking-database>) 包含大量創意搜尋與組合運算元的強大功能：



The screenshot shows the Exploit Database website's Google Hacking Database section. The interface includes a sidebar with navigation icons, a header with the Exploit Database logo, and a main content area. The main content area has a title 'Google Hacking Database', a 'Show 15' dropdown, a 'Quick Search' input field, and a table of search results. The table has columns for 'Date Added', 'Dork', 'Category', and 'Author'.

Date Added	Dork	Category	Author
2022-01-12	site:vps-*.vps.ovh.net	Web Server Detection	Chahine Boutighane
2022-01-12	inurl:adminpanel site:gov.*	Footholds	Asheet Turkey
2021-11-19	site:gov.* intitle:"index of" *.csv	Files Containing Juicy Info	Midhun Mohanan
2021-11-19	site:papaly.com + keyword	Files Containing Juicy Info	Gabriel Tarsia

Exercise 6-2

1. 誰是MegaCorp One的法律副總裁，他們的電子郵件地址是什麼？
2. 使用 Google dorks（您自己的或來自 GHDB ）
搜尋 www.megacorpone.com 用於有興趣的文件

Netcraft

- Netcraft提供免費的門戶網站，可以執行各種資訊收集功能
- Netcraft提供的服務是一種被動技術，因為從不直接與目標互動
- 例如，可以用Netcraft 的 DNS搜尋頁面 (<https://searchdns.netcraft.com>)來收集有關megacorpone.com網域的資訊：

Netcraft DNS search

Search Web by Domain

Explore websites visited by users of the Netcraft extensions [↗](#)

Site contains



*.megacorpone.com

Example: site contains [.netcraft.com](#)

Search

[Search tips](#)

Hostnames matching *.megacorpone.com

► [🔍 Search with another pattern?](#)

2 results

Rank	Site	First seen	Netblock	OS	Site Report
61447	www.megacorpone.com ↗	March 2013	OVH Hosting, Inc.	Linux - Debian	📄
807082	intranet.megacorpone.com ↗		OVH Hosting, Inc.	unknown	📄

站點報告



- 站點報告(site report)可為後續的主動資訊收集提供有用的資料，目前只需先記錄下來

Site report for <http://www.megacorpone.com>


► 🔍 [Look up another site?](#)

Share:     

Background

Site title	MegaCorp One - Nanotechnology Is the Future	Date first seen	March 2013
Site rank	53155	Netcraft Risk Rating 	0/10 
Description	Not Present	Primary language	English

Network

Site	http://www.megacorpone.com 	Domain	megacorpone.com
Netblock Owner	OVH Hosting, Inc.	Nameserver	ns1.megacorpone.com

Exercise 6-3

1. 使用 Netcraft 來確定 www.megacorpone.com 上正在運行的應用程式伺服器。

Recon-ng

- *recon-ng* 是一個以模組為基礎的框架，用來收集網站的資訊
- *recon-ng* 將模組的結果顯示到終端機上，同時也儲存在資料庫中
- 識別的大部分功能在於將一個模組的結果反饋到另一個模組中，從而使我們能夠快速擴展資訊收集的範圍
- *recon-ng* 可將一個模組的結果輸入到另一個模組中，使我們能夠快速擴大資訊收集的範圍

執行recon-ng

- 在命令列輸入recon-ng可看到我要需要安裝幾個模組

```
└─$ recon-ng
[*] Version check disabled.

Sponsored by ...

      ^
     /\
    /\  \
   /\  \  \
  /\  \  \  \
 /\  \  \  \  \
//  //  BLACK HILLS  \  \
www.blackhillsinfosec.com

PRACTISEC
www.practisec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.
[recon-ng][default] > █
```

尋找可安裝模組

- 輸入 `marketplace search github`, 可搜尋包含關鍵字 "github" 的模組

```
[recon-ng][default] > marketplace search github
[*] Searching module index for 'github' ...
```

Path	Version	Status	Updated	D	K
recon/companies-multi/github_miner	1.1	not installed	2020-05-15		*
recon/profiles-contacts/github_users	1.0	not installed	2019-06-24		*
recon/profiles-profiles/profiler	1.0	not installed	2019-06-24		
recon/profiles-repositories/github_repos	1.1	not installed	2020-05-15		*
recon/repositories-profiles/github_commits	1.0	not installed	2019-06-24		*
recon/repositories-vulnerabilities/github_dorks	1.0	not installed	2019-06-24		*

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

- 在欄位 K 標有 "*" 的模組需 API 金鑰才能執行，有些模組要另外付費才能使用

取得模組資訊並安裝模組

```
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web
```

```
+-----+
| path          | recon/domains-hosts/google_site_web |
| name          | Google Hostname Enumerator           |
| author        | Tim Tomes (@lanmaster53)             |
| version       | 1.0                                   |
| last_updated  | 2019-06-24                           |
| description    | Harvests hosts from Google.com by using the 'site' search operator.          |
| required_keys | []                                     |
| dependencies  | []                                     |
| files         | []                                     |
| status        | not installed                         |
+-----+
```

```
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > █
```

載入模組

- 用 `module load` 載入模組，再用 `info` 顯示所需參數
- 該模組需要 **SOURCE** 資訊

```
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > info
```

Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the results.

Options:

Name	Current Value	Required	Description
SOURCE	default	yes	source of input (see 'info' for details)

Source Options:

default	SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string>	string representing a single input
<path>	path to a file containing a list of inputs
query <sql>	database query returning one column of inputs

設定目標網域

- 執行結果會儲存到資料庫中(本例被google CAPTCHA阻擋)

```
[recon-ng][default][google_site_web] > options set SOURCE megacorpone.com
SOURCE ⇒ megacorpone.com
[recon-ng][default][google_site_web] > run

_____
MEGACORPONE.COM
_____

[*] Searching Google for: site:megacorpone.com
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[!] Google CAPTCHA triggered. No bypass available.

_____
SUMMARY
_____
[*] 1 total (1 new) hosts found.
```


顯示資料庫內容

- 輸入back返回上一層
- 輸入show顯示命令列選項
- 輸入show hosts顯示資料庫所儲存的主機資訊

```
[recon-ng][default][google_site_web] > back
[recon-ng][default] > show
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	www.megacorpone.com							google_site_web

```
[*] 1 rows returned
```

找到主機IP位址

➤ 安裝 recon/hosts-hosts/resolve模組

```
[recon-ng][default] > marketplace info recon/hosts-hosts/resolve
```

Start New Session		Restore Session
path	recon/hosts-hosts/resolve	
name	Hostname Resolver	
author	Tim Tomes (@lanmaster53)	
version	1.0	
last_updated	2019-06-24	
description	Resolves the IP address for a host. Updates the 'hosts' table with the results.	
required_keys	[]	
dependencies	[]	
files	[]	
status	not installed	

```
[recon-ng][default] > marketplace install recon/hosts-hosts/resolve
```

```
[*] Module installed: recon/hosts-hosts/resolve
```

```
[*] Reloading modules ...
```

載入recon/hosts-hosts/resolve模組

```
[recon-ng][default] > modules load recon/hosts-hosts/resolve
[recon-ng][default][resolve] > info
```

Name: Hostname Resolver
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Resolves the IP address for a host. Updates the 'hosts' table with the results.

Options:

Name	Current Value	Required	Description
SOURCE	default	yes	source of input (see 'info' for details)

Source Options:

default	SELECT DISTINCT host FROM hosts WHERE host IS NOT NULL AND ip_address IS NULL
<string>	string representing a single input
<path>	path to a file containing a list of inputs
query <sql>	database query returning one column of inputs

Comments:
* Note: Nameserver must be in IP form.

執行resolve模組

- 輸入run執行resolve模組

```
[recon-ng][default][resolve] > run  
[*] www.megacorpone.com ⇒ 149.56.244.87
```

- 輸入 show hosts顯示主機IP

```
[recon-ng][default][resolve] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	www.megacorpone.com	149.56.244.87						google_site_web

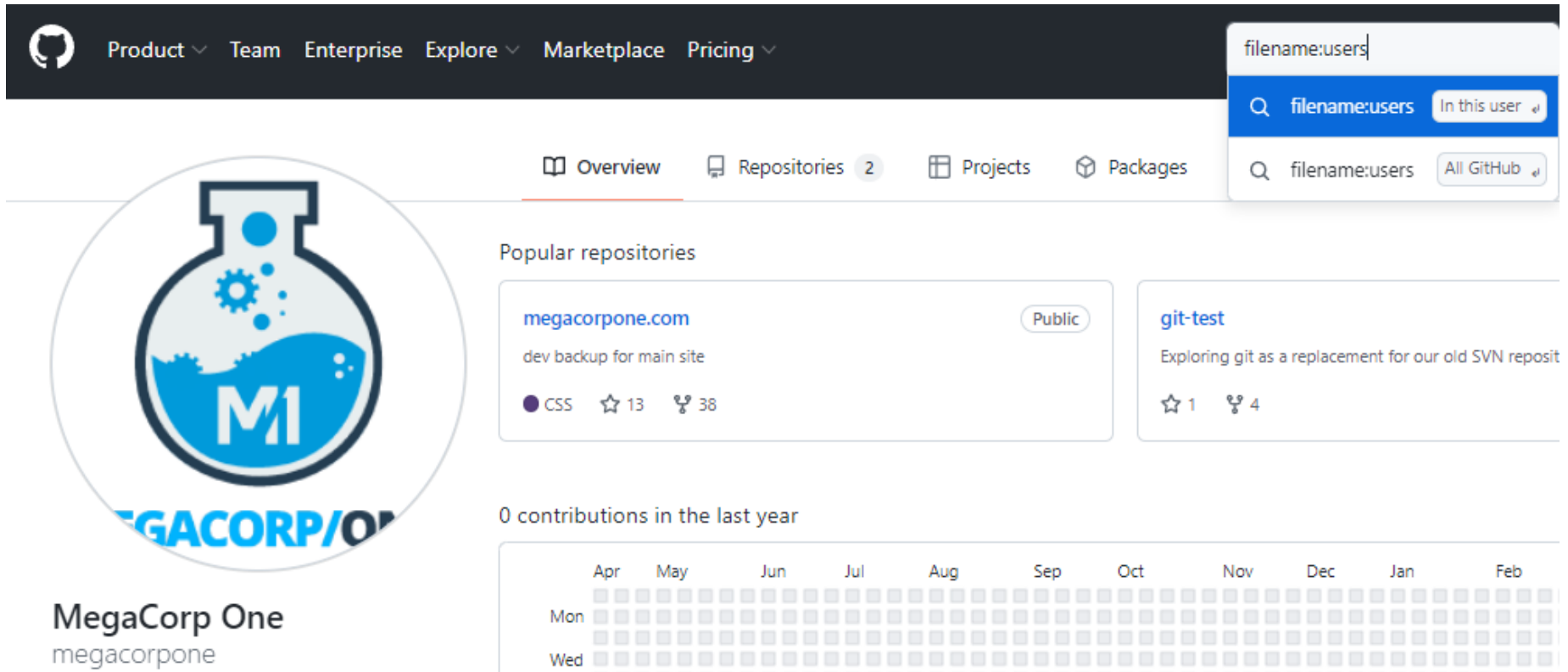
```
[*] 1 rows returned
```

Exercise 6-4

- 使用 `recon/domains-hosts/google_site_web` 和 `recon/hosts-hosts/resolve` 收集 MegaCorp One 的資訊

開源程式庫

- GitHub、GitLab、SourceForge等開源程式碼儲存庫可用於被動搜尋各種線上資訊
- 在網址列輸入<https://github.com/megacorpone>
- 搜尋filename:users



The screenshot shows the GitHub profile page for the user 'megacorpone'. The header includes the GitHub logo and navigation links: Product, Team, Enterprise, Explore, Marketplace, and Pricing. A search bar in the top right corner shows the query 'filename:users' with two filters: 'In this user' and 'All GitHub'. The profile section on the left features a circular avatar with a blue and white logo containing the letters 'M1' and the text 'MEGACORP/ONE' below it. The main content area displays 'Popular repositories' with two entries: 'megacorpone.com' (dev backup for main site, 13 stars, 38 forks) and 'git-test' (Exploring git as a replacement for our old SVN repository, 1 star, 4 forks). Below the repositories, it shows '0 contributions in the last year' with a calendar grid for the months of April through February.

Product Team Enterprise Explore Marketplace Pricing

filename:users

Q filename:users In this user

Q filename:users All GitHub

Overview Repositories 2 Projects Packages

Popular repositories

megacorpone.com Public

dev backup for main site

CSS 13 38

git-test

Exploring git as a replacement for our old SVN repository

1 4

0 contributions in the last year

Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb

Mon

Wed

MegaCorp One
megacorpone

檢視搜尋結果

- 搜尋發現 `xampp.users`，該檔案含有使用者帳號密碼等資訊，可能有助於之後的主動攻擊，可先加到筆記中

1 code result or view all results on GitHub



megacorpone/megacorpone.com

megacorpone/xampp.users



megacorpone/xampp.users

Last indexed on 16 Apr 2021

Exercise 6-5

- 使用github找出Megacorpone的敏感資訊

Shodan

- Shodan是一個搜尋引擎，可用來搜尋伺服器和IoT等設備的資訊
- 在網址shodan.io輸入
`hostname:*.megacorpone.com`

The screenshot displays the Shodan search engine interface. At the top, there is a navigation bar with links: Shodan, Maps, Images, Monitor, Developer, and More... Below this is a header section with the Shodan logo, navigation links (Explore, Downloads, Pricing), a search bar containing the query 'hostname:megacorpone.com', and an Account link. The search results are divided into two main sections. On the left, under 'TOTAL RESULTS', it shows '9' results. Below this, under 'TOP PORTS', there is a table:


TOP PORTS	
22	4
53	3
80	1

On the right, there are links for 'View Report' and 'View on Map'. Below these is a 'New Service' banner for 'Shodan Monitor'. The main search result is for the IP address '66.70.207.180', with a timestamp of '2022-04-13T19:43:45.378425'. The result details include the domain 'ns3.megacorpone.com', the operating system '9.11.5-P4-5.1+deb10u2-Debian', the resolver name 'ns3', the hosting provider 'OVH Hosting, Inc.', and the location 'Canada, Montréal'.

安全標頭掃描器

- 有些專業網站可收集有關網站或網域安全態勢的資訊，其中一些網站模糊了被動和主動資訊收集之間的界限
- Security Headers(<https://securityheaders.com/>)會分析HTTP回應的標頭，並提供目標網站安全態勢的基本分析
- 我們可以根據結果來瞭解組織的編碼和資安實施的狀況


掃描www.megacorpone.com

Security Headers
Sponsored by  Probely

Home About Donate

Scan your site now

☐ Hide results ☐ Follow redirects

Security Report Summary	
	Site: http://www.megacorpone.com/ - (Scan again over https)
	IP Address: 149.56.244.87
	Report Time: 14 Apr 2022 03:54:34 UTC
	Headers: ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy
	Warning: Grade capped at A, please see warnings below.

SSL伺服器測試

- 另一個掃描工具是Qualys SSL Labs的SSL Server Test
(<https://www.ssllabs.com/ssltest>)
- 此工具分析伺服器的 SSL/TLS 配置並將其與目前最佳實務進行比較
- 它還將識別一些與SSL /TLS相關的漏洞，例如 Poodle
(<https://en.wikipedia.org/wiki/POODLE>) 或 Heartbleed
(<https://en.wikipedia.org/wiki/Heartbleed>)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.megacorpone.com

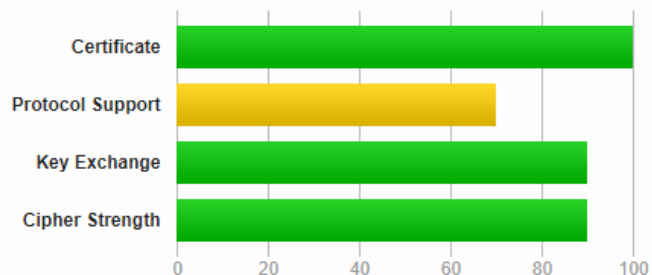
SSL Report: www.megacorpone.com (149.56.244.87)

Assessed on: Thu, 14 Apr 2022 04:18:36 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.3.

Pastebin

- Pastebin (<https://pastebin.com>)是一個用來儲存和共享文字的網站
- 無需註冊帳號即可使用基本功能
- Pastebin無所不在且易於使用
- 由於是公開的服務，可以用來搜尋敏感資訊，或者透過API用於更進階的用途
- 有可能在MegaCorp One上找不到任何新的資訊，但不應忽視搜尋Pastebin以了解收集工作的未來資訊

使用者資訊搜集

- 除了收集目標機構資源的資訊外，還可以收集員工的資訊
- 收集員工資訊的目的是為了建立使用者或密碼資料，為社交工程鋪路，增強網路行銷活動或客戶端攻擊，執行憑證填充(credential stuffing) 等
- 針對使用者列舉的工具：
 - ✓ Email Harvesting
 - ✓ Password Dumps

Email Harvesting

- theHarvester可從多個公開資料來源收集電子郵件、名稱、子網域、IP和URL
- -d: 指定目標網域
- -b: 設定要搜尋的資料來源 (google, all)

```
$ theHarvester -d megacorpone.com -b google

*****
*
* [ASCII Art Logo]
*
* theHarvester 4.0.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: megacorpone.com

Searching 0 results.
Searching 100 results.
Searching 200 results.
```


Exercise 6-6

1. 使用 theHarvester 列舉 megacorpone.com 的電子郵件地址。
2. 嘗試不同的資料來源 (-b)

Password Dumps

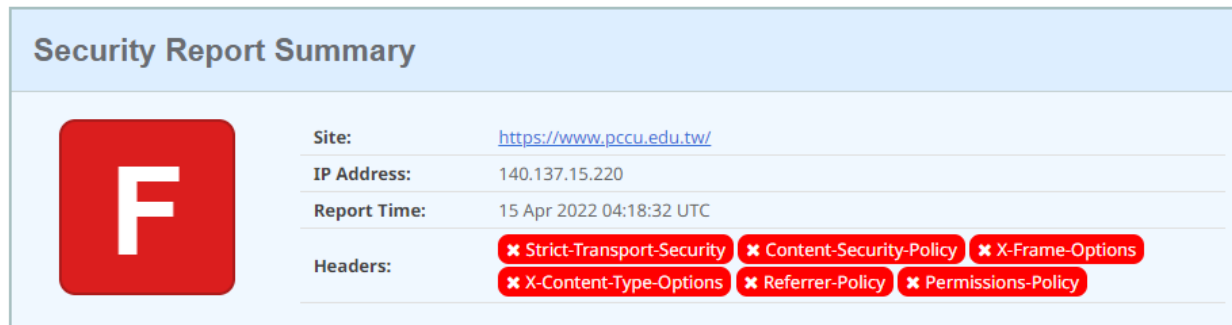
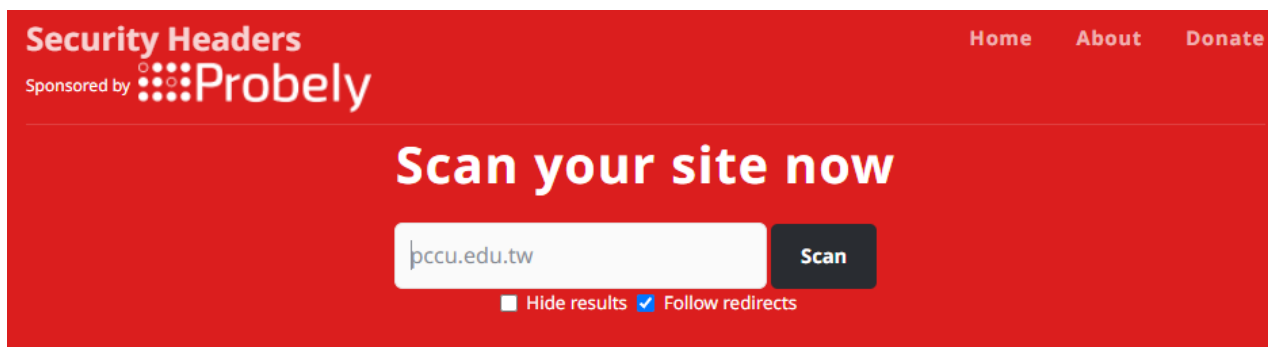
- 惡意駭客經常將洩露的憑據轉存在Pastebin或其他信譽不佳的網站上，這些密碼轉存對於產生字彙表非常有價值
- 例如，Kali Linux 包含了2009 年資料洩露所產生的“rockyou”字彙表
- 檢查電子郵件位址，我們發現在針對密碼轉存的使用者列舉過程中，可以找到可以用於填充攻擊(credential stuffing attack)的密碼

社交媒體工具

- 幾乎所有公司都有用到社交媒體，公司所發布的資訊對我們非常有用
- 例如，這些資訊可以用來識別潛在員工並獲得有關公司及其營運的更多資訊
- 使用recon-ng 和 theHarvester等工具可收集這些公開資訊

Social-Searcher

- Social-Searcher (<https://www.social-searcher.com/>) 是社交媒體網站的搜尋引擎
- 免費帳戶可允許每天進行有限次數的搜尋
- 可在伺服器上設置API密鑰



網站特定工具

- Twofi 掃描使用者的Twitter推文，並產生用於針對該使用者進行密碼攻擊的個性化詞彙表
- 雖然在被動資訊收集期間不會執行任何攻擊，但可以針對我們確定的任何Twitter帳號執行此工具，以便在需要時準備好單字列表
- Twofi需要有效的 Twitter API密鑰
- *linkedin2usemame*是一個基於LinkedIn資料產生使用者名稱清單的腳本
- *linkedin2username*需要有效的LinkedIn帳號，並且依賴與目標組織中的個人LinkedIn連接
- *linkedin2username*腳本可輸出幾種不同格式的使用者名稱

Stack Overflow

- Stack Overflow (<https://stackoverflow.com/>) 是一個供開發人員提問和回答與寫程式相關問題的網站
- 從資訊收集的角度來看，該網站的價值在於查看使用者提出或回答的問題類型
- 如果能夠合理地確定 Stack Overflow 上的使用者也是目標組織的員工，那麼或許能夠根據員工的問題和答案推斷出有關該組織的一些資訊
- 例如，如果我們發現一個使用者總是在詢問和回答有關 Python 的問題，那麼可以合理地假設他們每天都使用該程式語言，並且很可能在他們所在的組織中使用
- 更糟糕的是，如果我們發現員工在這類論壇上討論敏感資訊（例如漏洞修復），我們可能會在此階段發現未修補的漏洞

資訊搜集框架

- OSINT Framework (<https://osintframework.com/>)和Maltego (<https://www.paterva.com/buy/maltego-clients.php>) 包含了我們討論過的許多技術，還有一些其他的功能
- 對於實驗室中要完成的工作，這些工具通常過於笨重，但它們在現實世界的評估中很有價值

OSINT Framework

- OSINT Framework 在一個集中的地方包括資訊收集工具和網站
- 框架中列出的一些工具涵蓋了比資訊安全更多的範疇

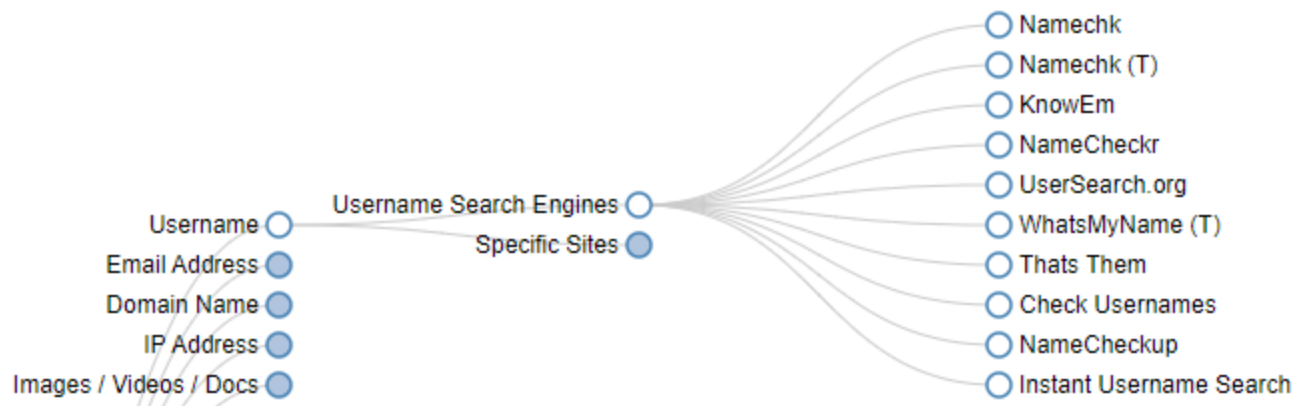
OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally

(D) - Google Dork, for more information: [Google Hacking](#)

(R) - Requires registration

(M) - Indicates a URL that contains the search term and the URL itself must be edited manually



Maltego

- Maltego是一個非常強大的資料探勘工具，提供了無數種搜尋工具和策略的組合
- 學習曲線可能很陡，對於本單元來說過於龐大，但仍然值得介紹
- Maltego 搜尋數千個線上次資料來源，並使用極其巧妙的“轉換”將一條資訊轉換為另一條資訊
- 例如，如果我們正在執行使用者資訊收集，可以提交一個電子郵件地址，並透過各種自動搜尋，將其轉換為相關的電話號碼或街道地址
- 在組織資訊收集活動中，我們可以提交一個網域名稱，然後將其轉換為網路伺服器，然後是電子郵件地址列表，然後是相關社交媒體帳號的列表，然後是該電子郵件帳戶的潛在密碼列表

