1 重新安裝（修復）flashplugin-nonfree 和 meld 套件。

```
apt reinstall flashplugin-nonfree meld
```

2.4.2 利用 dpkg 安裝套件

某些套件是貯庫裡所沒有的，需要自行下載 .deb 檔，此時便可用 dpkg 安裝，除了安裝離線套件外，dpkg 也可以查詢目前系統上安裝的套件資訊，常用的 dpkg 指令如下表：

表格 2-2：dpkg 常用指令

命令	功能說明
dpkg --install	安裝 .deb 檔，--install 可用 -i 代替。
dpkg -l	列出系統中已安裝的所有套件。
dpkg --get-selections	顯示所有套件的安裝狀態（未安裝、正確安裝、被移除、完整移除、安裝失敗等）。
dpkg --search	查詢某個檔案屬於哪一個套件，需使用完整路徑的檔案名稱。
dpkg --listfiles	列出某個套件有哪些檔案安裝到系統裡。
dpkg --status	列出某個套件的狀態描述，--status 可用 -s 代替。
dpkg --remove	移除已安裝的 .deb 檔，但保留組態資料，--remove 可用 -r 代替。
dpkg --purge xxx.deb	完整移除已安裝的 .deb 檔，包括組態檔也移除，--purge 可用 -p 代替。

dpkg 的檔案比對方式和 apt 或 apt-get 不同，dpkg 是採用萬用字元比對，星號（＊）表示任意長度的文字。底下是幾個 dpkg 的使用範例：

1 列出套件名稱開頭是 im 的套件。

```
dpkg --get-selections im*
```

2 列出套件名稱結尾是 im 的套件。

```
dpkg --get-selections *im
```

3 列出套件名稱中含有 im 的套件。

```
dpkg --get-selections *im*
```

（參考圖 2-32 之⑨），然後在 Firefox 圖示點擊滑鼠右鍵，從彈出清單中選擇「加入喜好」即可。

筆者曾經遇到 Firefox 無法啟動，在終端機直接執行「/opt/firefox/firefox-bin」，結果出現「Couldn't load XPCOM.」，遇到這種情形，可以先試著安裝 libdbus-glib-1-2：

```
apt install libdbus-glib-1-2
```

如果安裝 libdbus-glib-1-2 之後仍然無法啟動 Firefox，只好將 Firefox 完全移除，再重新安裝：

```
apt purge firefox-mozilla-build
apt update && apt upgrade -y
apt reinstall firefox-mozilla-build libdbus-glib-1-2
```

NOTE：初安裝的 Firefox 應該是英文界面，若想要改成中文界面，請從右上方「≡」鈕的 Preferences（偏好設定）進入，在 General（一般）頁的 Language（語言）段切換成 Chinese(Taiwan)，然後套用並重新啟動 Firefox，就可以換成中文界面了。

2.7.2 安裝 Chrome

安裝 chrome 也很簡單，只要執行下列指令即可：

```
1. apt update
2. cd /tmp/
3. wget -c https://dl.google.com/linux/direct/google-chrome-stable_current
     _amd64.deb
4. dpkg -i google-chrome-stable_current_amd64.deb
   ## 如果發生套件未滿足相依關依，請先執行「apt-get install -f」後，再重新執行步驟 3.
```

安裝完成後，在「應用程式＼常用程序＼網際網路」會多一個「Google Chrome」選項，若要將 Chrome 釘選在工作列，只要利用工具列的顯示應用程式鈕顯示所有程式（參考圖 2-32 之⑨），然後在 Chrome 圖示點擊滑鼠右鍵，從彈出清單中選擇「加入喜好」即可。

Chrome 安裝完成後若無法執行，此乃因 Chrome 基於安全因素，不允許以特權身分（root）執行，但我們拿 kali 做滲透測試，卻常需要使用 root 權限，為此只好修改 /opt/google/chrome/google-chrome，在最後一列「exec -a "$0" "$HERE/chrome"

"$@"」的後面加入「 --user-data-dir --test-type --no-sandbox」，修正後的文字如下所示：

```
exec -a "$0" "$HERE/chrome" "$@" --user-data-dir --test-type --no-sandbox
```

2.8 無線網卡管理

Kali 已預先安裝無線網卡管理工具（參考圖 2-33），當插入 USB 網卡後，如果有偵測到，就會出現在管理清單中（圖 2-46）。

要設定 Wi-Fi 連線資訊，可以點開無線網路項目，從選單中選擇「Wi-Fi 設定值」進入設定作業。選擇待連線的熱點（AP）並輸入密碼（如需要），即可完成連線設定。

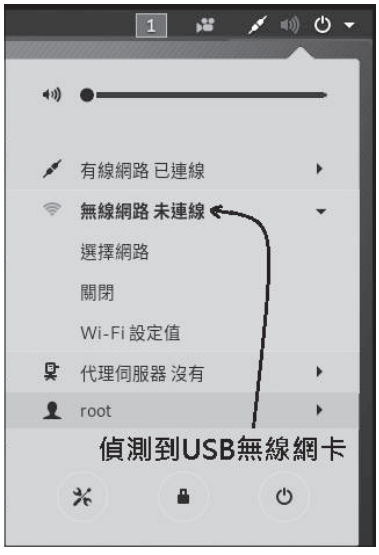

圖 2-46：Kali 內建的 Wi-Fi 管理工具

2.9 設定 SSH 遠端登入功能

Kali 本身已完裝 SSH 服務，但預設是未啟動，想要啟動 ssh 服務，請在終端機執行：

```
service ssh start
```

如果想讓 SSH 服務在開機時就自動啟動，可以將 /etc/init.d/ssh start 這列指令放到 /etc/rc.local 檔案之中，讓它在開機時即自動載入。或者執行下列指令，以服務方式啟動。

```
update-rc.d ssh enable
```

如果你的 Kali 上沒有 rc.local，就自行用文字編輯器建一個吧！將下列內容儲存到 /etc/rc.local：

```
#!/bin/sh -e
service ssh start
exit 0
```

建立 rc.local 後，記得賦予執行權限「chmod +x /etc/rc.local」。

如果不指定選項，只會顯示目前終端機執行的程式。可比較圖 3-14 和圖 3-15：

```
root@kali-2019-64:~# ps
   PID TTY          TIME CMD
  8928 tty3     00:00:00 login
  8933 tty3     00:00:00 bash
  8942 tty3     00:00:00 ps
root@kali-2019-64:~#
```

圖 3-14：tty3 中的程式

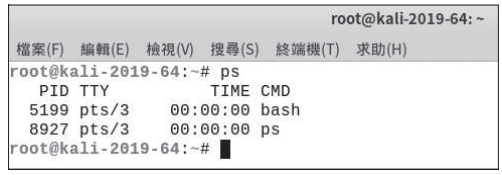

圖 3-15：X-window 虛擬終端機中的程式

在 3 號終端機（tty3）執行 ps，可看到 TTY 欄位的值是 tty3，執行中程序有 3 組。

在 X-Window 的虛擬終端機執行 ps 的結果，TTY 欄位顯示 pts/3，執行程序有 2 組。

如果執行「ps -e」則可以看到所有終端機上的程式。

- **kill PIDs**

強制結束執行程序，通常搭配 ps 使用，利用 ps 查出程序的 pid，再利用 kill PIDs 將指定的程式結束掉，可以指定多個 pid，多個 pid 請用空白字元隔開。

範例 結束 pid 為 259、732 及 3386 三組程序。

```
kill 259 732 3386
```

- **killall PROC_NAME**

終止指定名稱的程序。kill 是終止指定 pid 的程序，但有時同樣的程序執行了好幾組，每組都有自己的 pid，如果想要一次將這些程序終止掉，使用 killall 比較方便。在 Linux 中，程序名稱大小寫有別，如果不想區分大小寫，可以加上 -I 參數。（i 的大寫字母）

- **service --status-all**

查看系統服務（Services）狀態，執行後可以看到目前已安裝的服務及目前狀態。

```
[ + ]  pcscd
[ + ]  postgresql
[ ? ]  pppd-dns
[ - ]  procps
[ + ]  pulseaudio
```

在顯示服務前頭的 +（加號）表示服務作用中、-（減號）表服務已終止、?（問號）表無法得知服務狀態。

```
intitle:"index of" htpasswd
intitle:"index of" data
```

若想進一步探索 Google Hacking 應用，可參考拙編、碁峰資訊出版的《Google Hacking 精實技法》，或者想要使用現成的 Google Hacking 語法，可以參考下列網址：

https://www.exploit-db.com/google-hacking-database

6.1.2 Bing

目前來看，說 Google 是地表最強的搜尋引擎，應無異議，但其他搜尋引擎能夠存活，一定有 Google 所不及的特色，其中微軟 Bing 就是 Google 的競爭者之一。

Bing 有許多功能和 Google 類似，譬如利用 Bing 和 Google 分別搜尋「台灣大學」，回傳的結果畫面就非常神似，圖 6-4 左邊是 Bing、右邊是 Google 回傳的結果，包括搜尋框的位置、下方的搜尋類別欄、右邊的附屬資訊的布置方式都雷同，或許行有餘力也該關注一下 Bing。

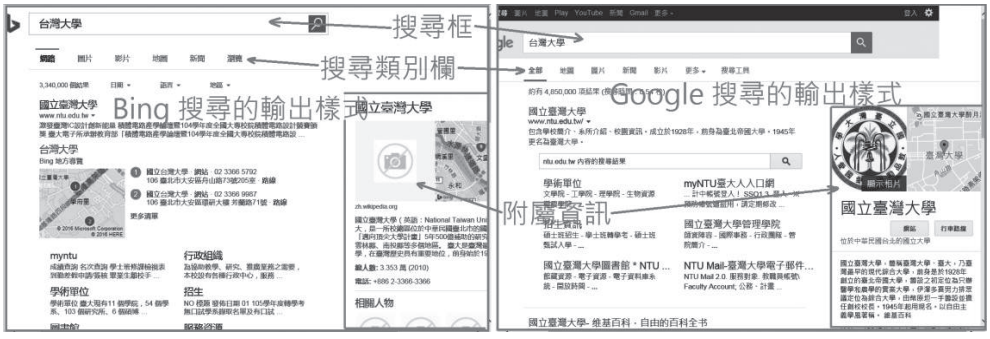

圖 6-4：Bing 與 Google 的外觀比較

仿照研究 Google 搜尋 URL 方式，把 Bing 的搜尋 URL 照樣翻來瞧一瞧，其主要部分和 Google 的搜尋 URL 也一樣，連搜尋的詞彙也是利用 q 參數指定。下式是 Bing 搜尋 URL 的主要部分：

```
http://www.bing.com/search?q= 台灣大學
```

如果把「http://www.bing.com」換成「https://www.google.com」不就成了 Google 的搜尋式，下式是 Google 搜尋 URL 的主要部分：

```
https://www.google.com/search?q= 台灣大學
```

來源網站 \ 可查詢的屬性	IP	hostname	MD5 或 SHA1
totalhash_ip	V	V	
totalhash_md5			V
unshortme		V	
urlvoid		V	
virustotal			V
vtpDNSDom		V	
vtpDNSIP	V		
vxvault			V

從上表內容可知，automater 能夠利用檔案的 MD5 檢查是否為惡意程式、檢查是否為惡意 IP 或惡意網站，還能標示出 IP 的地理座標。

範例

❶ 檢查 37.221.161.215 這組 IP，並將查詢結果以 html 格式儲存到 root 的家目錄之 result.htm 檔。

```
automater 37.221.161.215 -w ~/result.htm
```

❷ 類似上例，但檢查一個範圍的 IPs。

```
automater 37.221.161.1-255 -w ~/result.htm
```

❸ 檢查給定的 MD5 是否為惡意檔案的雜湊值。

```
automater 44A6A7D4A039F7CC2DB6E85601F6D8C1
```

❹ 以 root 家目錄下的 auto.in 清單檔做為輸入，查詢裡頭項目的資訊。

```
automater ~/auto.in
```

6.1.6 dmitry

dmitry 是一款多功能的訊息收集工具，可蒐集指定網域中的子網域、電子郵件、伺服器的服務類型、端口掃描、whois、…等。

-dnsfile LIST_FILE：想執行多網域猜解時，可先將網域記錄到文字檔中，每一列為一網域，再將清單檔交由 fierce 處理。

-connect HEADER：利用指定的 HEADER 檔案（見底下的「header 檔案的簡易範例」）嘗試對網域裡的網站進行 http 連線，並記錄該網站的回應（如有），要注意，如果目標網域有許多開放網址，此選項將耗費許多連線時間。

header 檔案的簡易範例

```
GET / HTTP/1.0
User-Agent: Mozilla/5.0
Host:
Expect: <script src=http://ha.ckers.org/xss.js></script>
```

在 HEADER 檔案裡，「Host:」這一列是要連結的主機，fierce 會自動利用暴力猜解得到的主機填入其中。

-delay SEC：每次發送暴力查詢的間隔秒數。

-dnsserver DNS_SERVER：指定要向哪一臺 DNS 伺服器查詢。

-file OUT_FILE：指定要儲存結果的輸出檔，如果不指定，猜解結果只會顯示在螢幕上。

-suppress：當搭配 -file 選項時，可利用 -suppress 抑制訊息輸出到螢幕。

-fulloutput：配合 -connect 選項，除了傳送的 header 外，也會記錄受測對象回傳的結果。

-search NAMEs：配合 -dns 指定的 DOMAIN，當 fierce 利用 nearby IP 找到其他不同 DOMAIN 的 server，利用此 -search 選項所指定的名稱清單，可以將不同的 DOMAIN 包含到查詢的名單中，這樣可以挖掘到更多的 Server 資訊。NAMEs 清單若有多筆者，請以逗點（,）分隔。

-tcptimeout SEC：如果遇到 DNS 反應慢或網路通訊遲緩時，可以調增逾時的秒數。預設 10 秒。

-threads N：指定在猜解時要用幾個執行緒（預設為 1，建議使用 8）。

-travers N：當執行 nearby IP 猜測時，往上、往下的 IP 個數，預設是 5。

-wide：對整個 C class 的 IP 範圍進行猜解。

-range IP-RANGE：指定 IP 範圍，例如：1.2.3.0-255，-range 選項要搭配 -dnsserver 選項使用。

-f：顯示 NBT 服務的完整內容，類似 nbtscan 的 -vh 參數。

-v：輸出詳細的除錯訊息。

-n：不要執行 IP 位址的名稱反向解析。

-m：輸出回應內容的 MAC 位址，不能和 -f 一起使用，否則會被抑制。

-T SEC：等待回應的逾時秒數（預設 2 秒）。

-w MS：發送掃描封包之間的間隔，單位毫秒，預設 10ms。

-t N：對每個位址嘗試探測的次數（預設 1）。

-P：以 perl 的 hashref 格式來格式化結果。

範例

❶ 查詢區域網路中有哪些機器啟用 NetBIOS 協定。

```
nbtscan-unixwiz 192.168.18.0/24
```

❷ 查看 HP440G2 啟用哪些服務。

```
root@kali-2019-64:~# nbtscan-unixwiz -f HP440G2
192.168.18.1    WORKGROUP\HP440G2              SHARING
  HP440G2         <00> UNIQUE Workstation Service
  WORKGROUP       <00> GROUP  Domain Name
  HP440G2         <20> UNIQUE File Server Service
  WORKGROUP       <1e> GROUP  Browser Service Elections
  WORKGROUP       <1d> UNIQUE Master Browser
  ..__MSBROWSE__.<01> GROUP  Master Browser
  00:50:56:c0:c0:c8   ETHER
```

既生瑜，何生亮？ nbtscan 與 nbtscan-unixwiz 功能幾乎一樣，但還是有些許差異，例如 nbtscan-unixwiz 可以同時列出服務代碼及服務名稱，但 nbtscan 只能擇一。另一方面，nbtscan 只能以 IP 位址做為掃描目標，nbtscan-unixwiz 則可以使用電腦名稱。因此，視需求不同，nbtscan 與 nbtscan-unixwiz 各有其特點。

6.8.4 enum4linux

enum4linux 是以 Perl 寫成的 SMB 資訊枚舉工具，藉由封裝 smbclient、rpclient、net 和 nmblookup 功能，只要是支援 Samba 協定的 Unix-liked 或 Windows 主機，透過指定欲枚舉的類型及主機 IP 就能輕易取得對方的資訊。

6.10.1 onesixtyone

onesixtyone（161）是一款高速的 SNMP 掃描程式，用來挖掘網路上的 SNMP 設備類型。知道網路上有哪些 SNMP 設備，便可嘗試讀取網路管理資訊，或修改 SNMP 設備的組態內容，讓該設備（如防火牆）的防衛能力失效。

- **執行路徑**：01- 信息收集 \ SNMP 分析 \ onesixtyone
  05- 密碼攻擊 \ 在線攻擊 \ onesixtyone
  由終端機執行 onesixtyone
- **語法**：**onesixtyone [*OPTIONs*] {*HOST* | -i *HOST_FILE*} {*COMMUNITY* | -c *COMMUNITY_FILE*}**
- **參數說明**

  HOST：即待則目標網址，它可以是單一位址或以 CIDR 表示的 IP 範圍，例如 192.168.18.0/24

  -c COMMUNITY-FILE：其實就是指定密碼清單。

  -i HOST-FILE：指定待測目標的位址清單。

  -o OUT-FILE：執行結果的紀錄檔。

  -w N：設定兩封包間間隔的時間（ms），預設 10，如果網路速度緩慢時，可酌為調大些。

範例

底下是刺探網路上某臺 Windows 10 的結果，這臺電腦使用常見的 public 及 private 做為社群名稱。

圖 6-45：onesixtyone 執行範例

```
          server_name
              host_name: www.moj.gov.tw
          extended_master_secret
          application_layer_protocol_negotiation
          status_request
          signature_algorithms
1 2  0.0883 (0.0550)  S>C  Handshake    ❹
      ServerHello
        Version 3.3
        session_id[32]=
          b5 1a 00 00 45 52 36 6f 3b b8 e3 4d b9 7f 1f fd
          b5 11 85 d0 22 fe 51 b7 8b 6b 99 0f dd ba 51 87
        cipherSuite         TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   ❺
        compressionMethod                   NULL
   ~~ 以下訊息省略 ~~
```

① 瀏覽器嘗試向 Web 伺服器建立連線。

② 協商加密協定，以確認後續的加密方式。

③ 瀏覽器提出能支援的加密套件清單。

④ Web 伺服器回應瀏覽器的交握請求。

⑤ Web 伺服器回應將使用的加密套件類型。

❷ 解密與不解密所呈現的結果：

未解密前，**ssldump** 只能判斷封包類型。

```
4 5    0.1018   (0.0000)    C>S      Handshake
4 6    0.1317   (0.0298)    S>C      ChangeCipherSpec
4 7    0.1317   (0.0000)    S>C      Handshake
4 8    0.1317   (0.0000)    S>C      application_data
1 9    0.3283   (0.2093)    C>S      application_data
1 10   0.3291   (0.0007)    C>S      application_data
2 9    0.2635   (0.1338)    C>S      application_data
3 9    0.2348   (0.1157)    C>S      application_data
```

解密後，**ssldump** 會輸出封包內容。

```
2 3    0.0714   (0.0014)    C>S    Handshake
        ClientKeyExchange
          DiffeHellmanClientPublicValue[32]=
            98 0c b9 ae 88 81 1e 3c d5 90 0c 3c 65 2a 1f 33
            2e d8 a4 bc 8e 34 25 52 49 b8 af eb d1 fe 51 43
2 4    0.0714   (0.0000)    C>S    ChangeCipherSpec
2 5    0.0714   (0.0000)    C>S    Handshake
        Finished
```

-i INTF：指定發送封包的網路介面，如不指定，會自動從 routing table 找相關的介面。

-f TTL：在第一組發送的封包設定初始的封包存活時間（TTL，即閘道跳數），預設 1。

-l LEN：設定封包的總長度（Byte）。

-q N：探測每一跳路由器所發送的封包次數，預設 3。

-m TTL：探測封包的最大跳數，預設 30。當逾最大跳數仍未能到達目前主機，即視為無法到達目的地。

-s SR_IP：設定封包發送端的 IP，欺騙對方，但也收不到回應封包，或者有兩張網卡時，可以一張傳、一張收。若不指定，即以發送封包的網卡之 IP 做為來源 IP。

-p SR_PORT：設定追蹤封包的送發端口。

-w SEC：指定等待對方回應的逾時秒數，預設 3.0，如果網路速度比較慢時，可以酌增 WAITTIME。

範例

利用 tcptraceroute 描繪到達臺灣大學網站的路徑，執行結果如圖 6-52。

```
tcptraceroute www.ntu.edu.tw
```

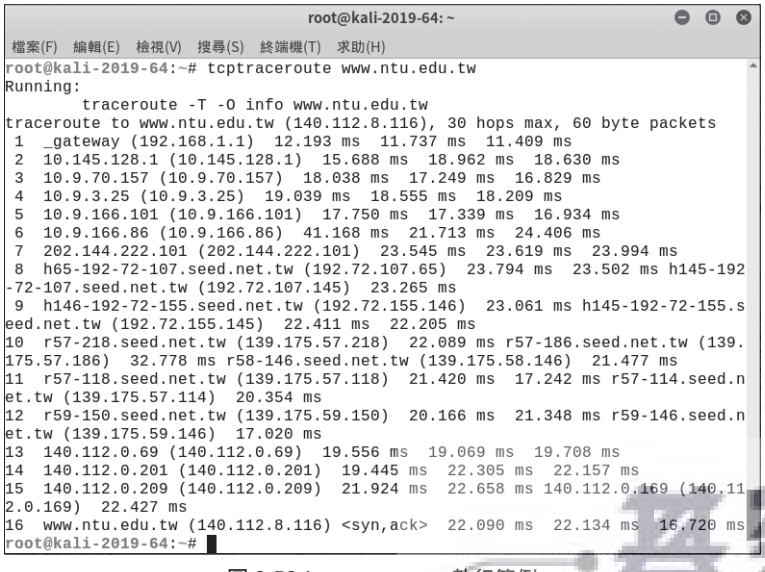

圖 6-52：tcptraceroute 執行範例

❼ 將檔案或網頁（網址）附加到指定的實體上。若要附加檔案，也可以直接將檔案拖拉到實體上。

❽ 將所選的實體傳送到某個網址，筆者不清楚這項功能的用途。

❾ 針對此實體執行某個動作，例如將實體的值傳給 Google 搜尋，或用瀏覽器開啟實體的 URL。

❿ 清理或重整實體的圖片。

實體分類及加註

當滑鼠移到實體上，可以發現圖示的右邊會顯現三個圖示（圖 6-68），其中顏色書籤方便做醒目提示，只要以滑鼠點擊該圖示即可切換顏色，例如需要再進一步追查的實體，可以標示為紅色，或者利用書籤顏色來分類實體。若要增加說明文字，可以點擊中間的便條紙，就可以開啟備註編輯器。

若覺得在實體上直接操作不夠全面，也可以雙擊實體，開啟實體詳細資料維護視窗。

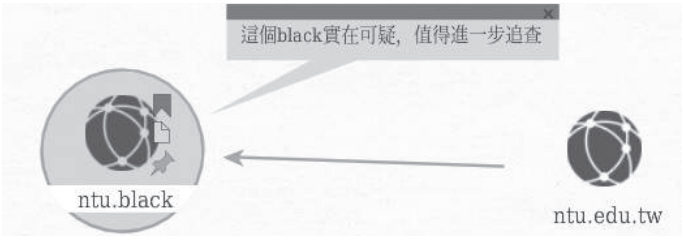

圖 6-68：實體的書籤及備註說明

詳細的 Maltego 操作說明可參閱：https://docs.paterva.com/

6.15.3 CaseFile

CaseFile 是 Maltego 的閹割版，單純提供離線的資料編製及分析功能，不能執行線上情資收集。還好可以將 Maltego 的資料餵給 CaseFile，它可以導入各類資料，包括 Maltego 匯出的資料。簡單地說，CaseFile 就是 Maltego 的畫布編輯器。

相較於 Maltego 社群版，CaseFile 的強處在於它的資料可用在商業行為，也就是它的產出可以做為滲透測試報告的內容。