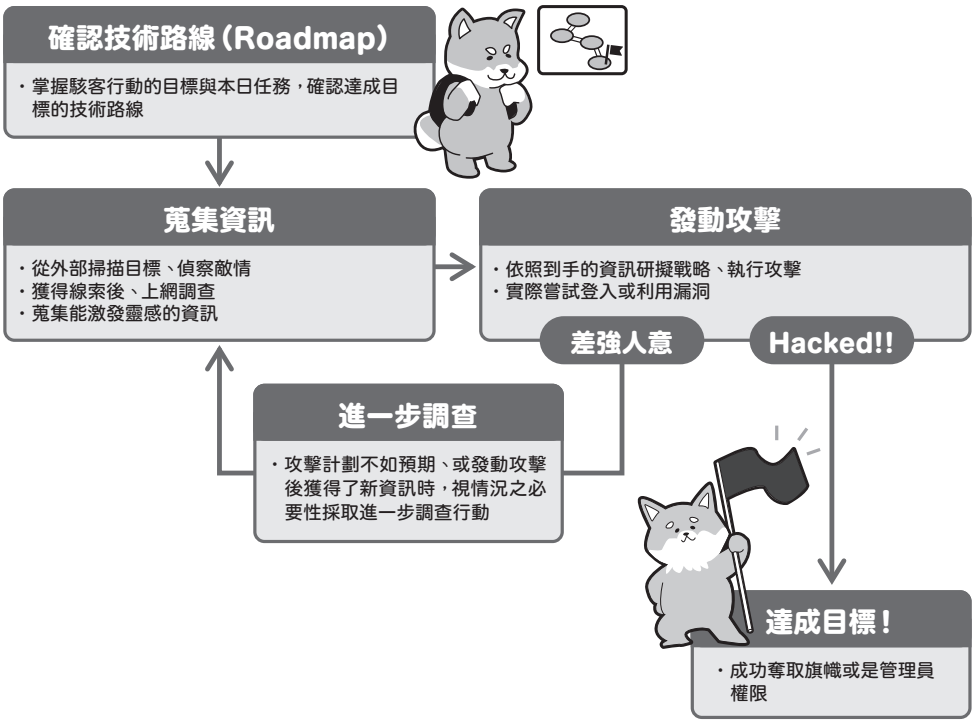
享受學習駭客技術的過程

每天的駭客技術教學，會依照下方的流程圖來進行。



先確認好技術路線上的本日目標，重複蒐集資訊與發動攻擊，直到達成目標。

這並非是一條單行道，重點是「在蒐集資訊跟發動攻擊兩者之間不斷來回繞行，直到達成目標」。也就是依據蒐集而來的資訊展開攻擊行動，然後進一步調查攻擊時獲得的資訊、從不同角度再發動攻擊，力求收穫更大成果。

為了便於理解，我們會將技術路線當中的行動分成「蒐集資訊」與「發動攻擊」兩個區塊。等實際操作難免後會發現這種太過簡化的區分方式可能難以傳達某些細節上的區分，不過，書中之所以決定特意採用這種方式來描述，是期待能使讀者輕鬆理解「雖然事情不簡單，但混亂過程中蘊含無窮樂趣」的駭客世界。

Day 1

準備登入駭客任務

講了這麼多，讓我們快點開始學習駭客技術吧！……先等等，有道是：工欲善其事、必先利其器。

在課程開始的第一天，我們先一步步準備好學習駭客技術所需的執行環境吧。不過，如果您手邊已經有 Kali Linux 或 Parrot OS 等環境的話，可選擇性地跳過 1.2 節跟 1.3 節的內容。

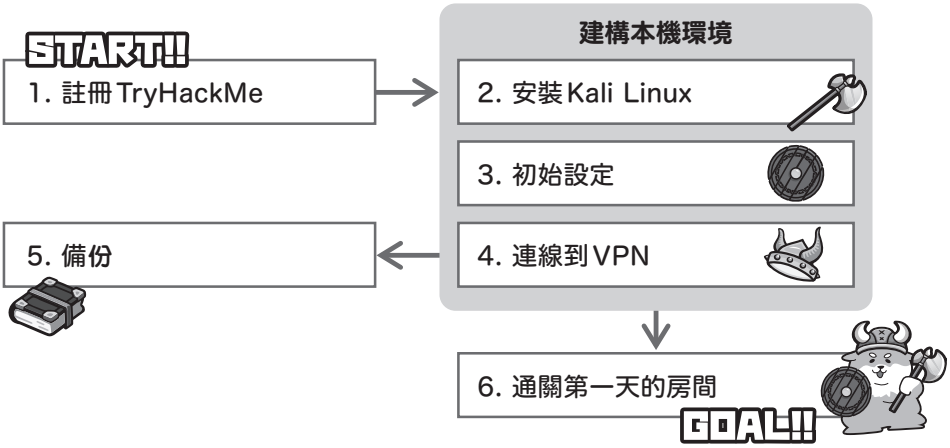
本日目標

Tutorial Room

https://tryhackme.com/room/tutorial

本日技術路線

目標	Tutorial Room
本日任務	做完學習駭客技術的準備，並順利通關第一天的房間

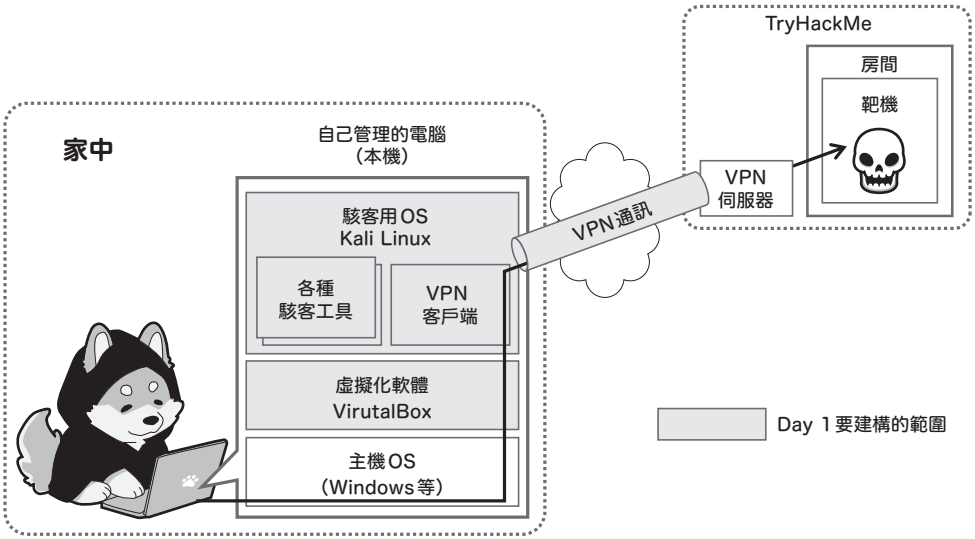


今天的目標是要做完學習駭客技術的準備。雖然註冊 TryHackMe、架設環境這些事情難免令人感到麻煩，不過今天沒做好，明天就沒辦法繼續學習後續了。再者，建構屬於自己的專用環境，也會讓自己更有參與感，學起來更有心得。

此外，接下來會大量運用 Kali Linux 這個具備豐富駭客技術工具的 Linux 作業系統，還沒習慣 Linux 的話可以在補充學習的房間裡加深印象，務必盡快熟悉喔！

今天要架構的環境示意圖

書中的駭客技術學習環境會如下圖的概念來進行架構。



灰色區塊的部分是我們今天要建構環境的範圍。安裝虛擬化軟體後，然後運行內建多種駭客工具的作業系統 **Kali Linux**。並透過 VPN 技術，使 Kali Linux 連線到 TryHackMe。

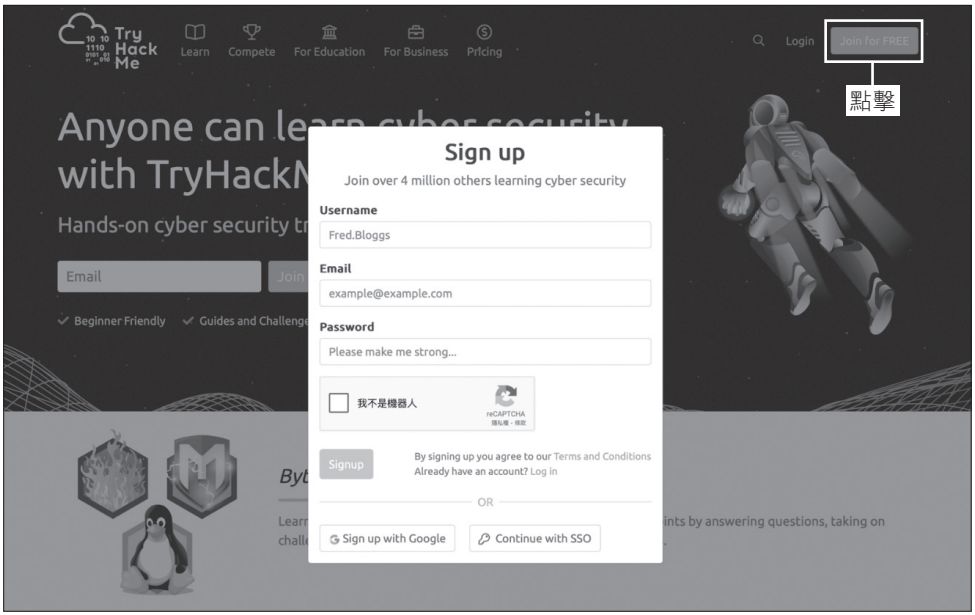
圖的左邊是自己可以控制的環境，稱為**本機環境或本機電腦（Local Machine）**，而 TryHackMe 這端則稱為**目標環境或靶機（Target Machine）**。這是非常重要的概念，請先牢記。

今天的學習過程中會接陸續出現許多新的用語，有些用語暫時不懂也沒關係，只要邊動手操作邊學習，就能夠慢慢進入狀況。放下擔憂，勇往直前吧！

1.1 註冊 TryHackMe

如昨天所提，書中是以 TryHackMe 平台作為「靶機環境」進行教學。所以我們今天就先來註冊 TryHackMe 吧！

前往 tryhackme.com



進到 TryHackMe 的網站 ※1，點擊右上角的〔Join for FREE〕，註冊帳戶。

請詳閱使用條款 ※2，同意條款內容後再註冊帳戶。

填寫問卷，進行註冊

註冊 TryHackMe 時需要填寫簡單的問卷，這份問卷沒有標準答案，就照實回覆即可。

不同時期問卷的問題數量跟內容可能不同。

▶ What is your current goal in cyber?

它問：「您目前在網路領域的目標是什麼呢？」。

※1 TryHackMe https://tryhackme.com/
※2 Terms of Use https://tryhackme.com/r/legal/terms-of-use

1.6 通關第一天的房間

從 Tutorial Room 試水溫

第一天的學習，就差最後一哩路。今天要挑戰通過在 TryHackMe 上的第一個房間，一起完成今天的任務吧！

正好「Tutorial Room」最適合用來確認連線狀態，別擔心，真的只是確認一下就會立刻結束了。

▶ 連線到 TryHackMe

從 Kali 的瀏覽器登入 TryHackMe，順便連線 VPN。

光是這邊可能就會需要重新啟動好幾次，如果有「不曉得 VPN 是否已經連線成功？」的疑問的話，可以再回到第 45 頁的「檢查連線狀態」，看看瀏覽器是否已經連上 VPN。

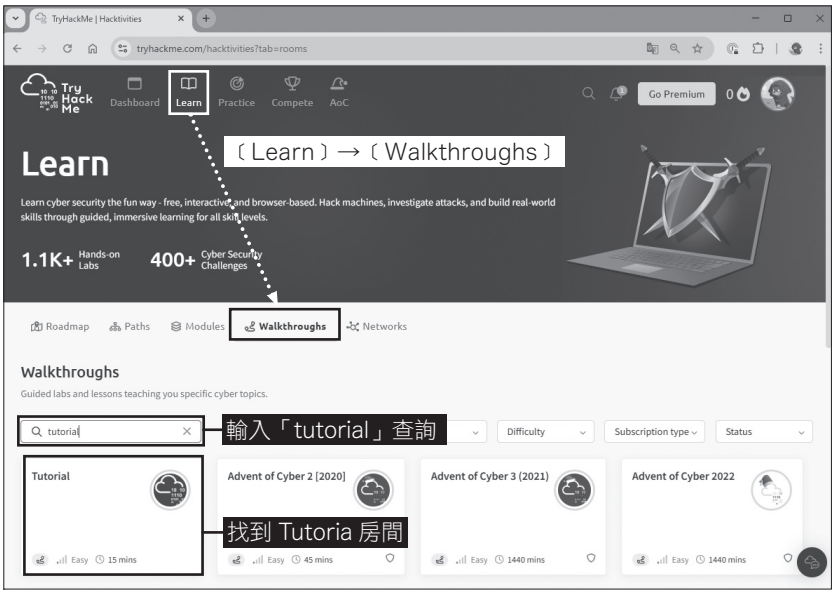
在使用 TryHackMe 時，幾乎都是在連線到 VPN 的狀態下來挑戰房間（除了極少數情況可能不需要）。所以，以下這 4 個步驟是每次必須執行的基本流程，後面就不再贅述，希望各位記得。就這麼說定囉！

❶ 開啟 VirtualBox
❷ 啟動 Kali Linux
❸ 登入 TryHackMe
❹ 開啟終端機、連線到 VPN

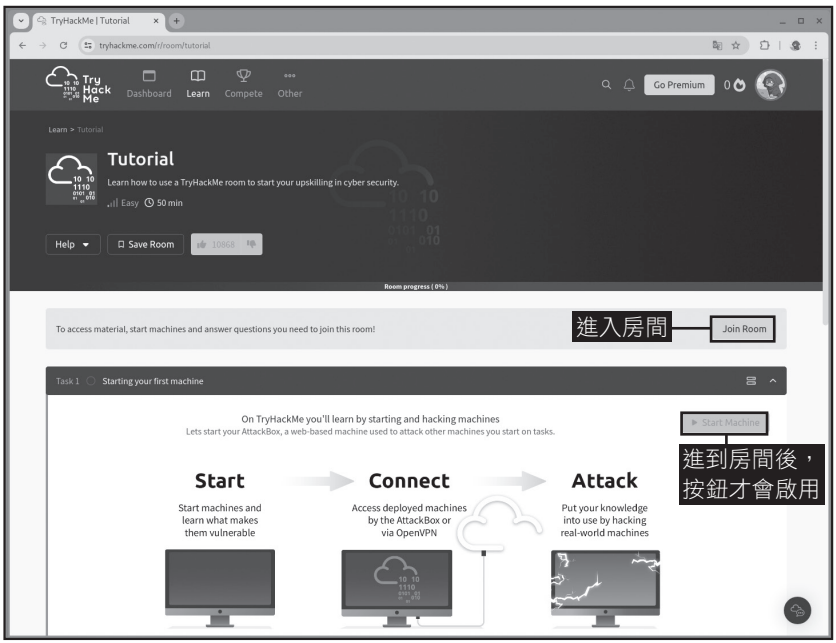
啟動 Tutorial Room 的靶機

我們也可以自由進出目前註冊的學習路徑之外的房間（詳見第 57 頁的 Column）。

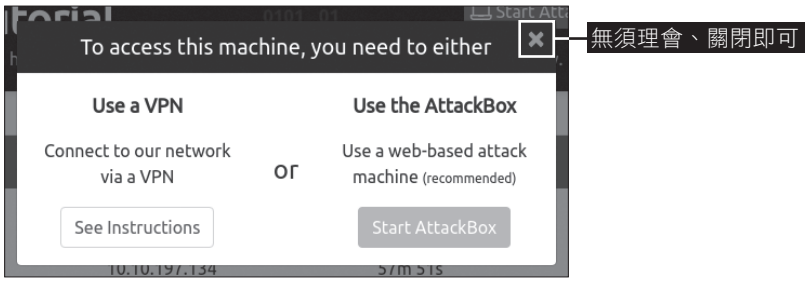
從上方選單中依序點擊〔Learn〕→〔Walkthroughs〕，在搜尋視窗裡輸入 tutorial，找到 Tutorial Room。如果 VPN 斷線了，請重新連線後再繼續執行後續步驟。



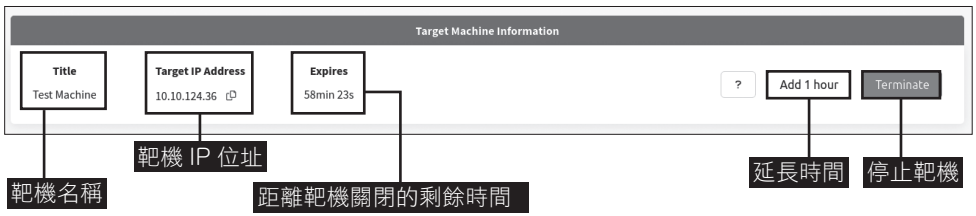
進到顯示房間的畫面後，點擊〔Join Room〕就能進到想要的房間，開始挑戰。接著，點擊 Start Machine。



此時會出現確認存取環境的視窗，直接關閉即可。



稍待片刻，靶機就會啟動、並且在畫面最上方的紅框中顯示靶機資訊。啟動後的第一步都要確認靶機的 IP 位址。



〔Expires〕顯示的倒數時間可能令人在意，其實，第一次使用靶機的時間會限制在 1 小時（有付費的話則是 2 小時）。

如果發現在時間內無法完成，可按延長時間按鈕、每按一次多加 1 小時。延長次數沒有上限，只是得要每隔一小時就按一次（且無法連續點擊）。此外，如果過度延長，系統則會催促您結束當前任務。

時間結束、或按下停止按鈕時，靶機會自動關機。

也可重新啟動，但要注意 IP 位址可能改變。

使用 ping 指令檢查啟動狀態

用 **ping** 指令確認靶機是否已經順利啟動。

ping 會針對我們指定的 IP 位址或網域名稱傳送特殊的封包（資料），依據是否收到回應來確認對方的運行狀態。

對靶機的 IP 位址，執行下圖的動作。

▼ 終端機

```
# 檢查與靶機之間的通訊狀態
┌──(kali㉿kali)-[~]
└─$ ping 10.○.○.○
PING 10.○.○.○ (10.○.○.○) 56(84) bytes of data.
64 bytes from 10.○.○.○: icmp_seq=1 ttl=60 time=303 ms
64 bytes from 10.○.○.○: icmp_seq=2 ttl=60 time=300 ms
（後略）
```

看到連續顯示 64 bytes from ～的訊息，就表示已經收到回應，連線成功。這個指令不會自動停下，因此可在適當的時機點按下〔Ctrl〕＋〔C〕中斷處理。

雖說這裡的測試有順利收到 Tutorial 靶機的回應，但有些靶機可能會被設定為不要回應 ping 指令，所以 ping 沒收到回應不完全代表靶機沒在運作。因此僅供參考。

連線靶機，奪得旗幟

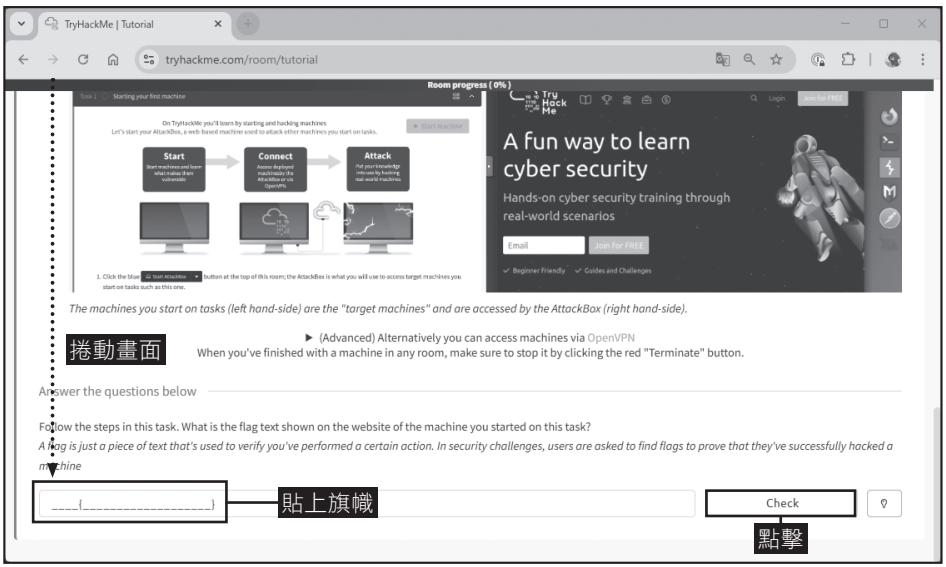
開始解任務吧！這個靶機的任務只是「連線到 VPN、使用瀏覽器存取靶機」而已，經過初始設定後，應該已經做好了所有的準備。

在瀏覽器的網址列輸入剛剛確認過的靶機 IP 位址，按下〔Enter〕。接著就會看到網站顯示出來，並且可以看到旗幟（flag）。

旗幟指的是解答時必備的字串。大致上都會遵守規定，以 **flag{○○○}** 或者 **THM{×××}** 的形式出現。將整段字串複製下來後，回到 Tutorial Room。

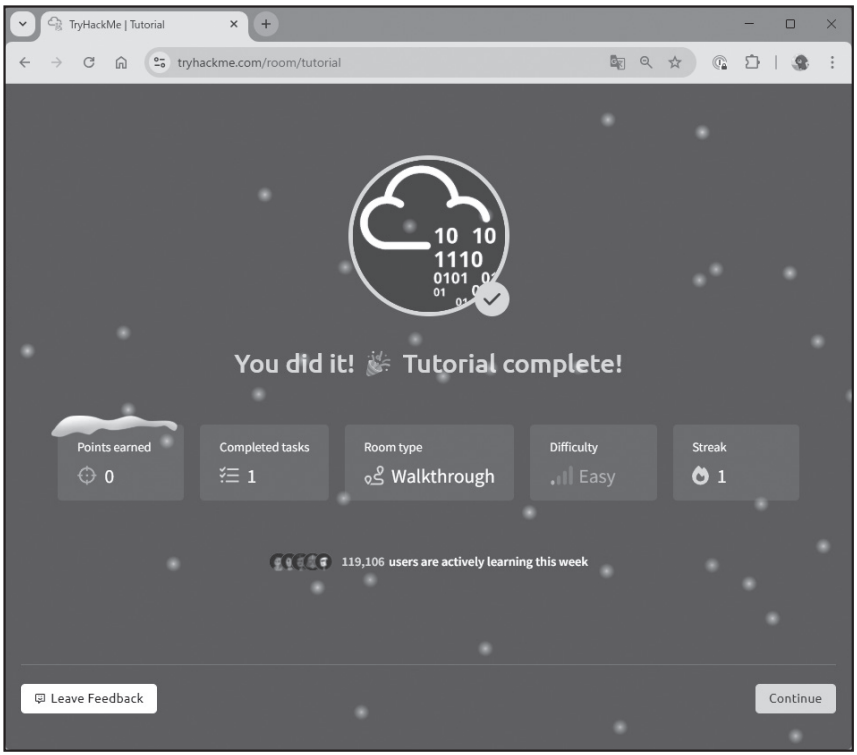
領取旗幟時，必須全部複製 flag 或 THM 這些前綴詞、大括號（{　}）及其後的內容。

稍微捲動畫面，抵達任務的解答表單，將旗幟貼上後、點擊〔Check〕。



當答案正確時會顯示「Correct Answer」，表示任務完成。我們已經順利完成這間房間唯一的任務，恭喜達成第一天的目標。

畫面上也會出現「恭喜！」，這只有第一次通關成功才會顯示喔！不害臊的話可以分享到社群上，一邊享受成果與掌聲、一邊繼續學習下去吧！



請再次給踏出勇敢的第一步的自己，最大的讚美！

成功攻下靶機之後，點擊房間的〔Terminate〕按鈕，關閉靶機。

總結

先再次恭喜您過關，辛苦了！

我們準備好了駭客技術學習所需要的環境，並且順利通關了第一個挑戰的房間。倘若還覺得有點意猶未盡的話，接下來還有加碼補充學習，希望讓大家滿載而歸。

書中會為每天學過的內容，額外附上補充學習。無須追求完美，等有時間或有動力的時候，再依照自己的步調嘗試即可。期待能為大家的好奇心帶來更完整的體驗。

加碼補充學習內容

▶ Linux Fundamentals Part 1

https://tryhackme.com/room/linuxfundamentalspart1

對操作 Linux 較沒信心的讀者、時間上還有餘裕的讀者，期待您們一起來挑戰 Linux Fundamentals Part 1（Linux 基礎）的房間。

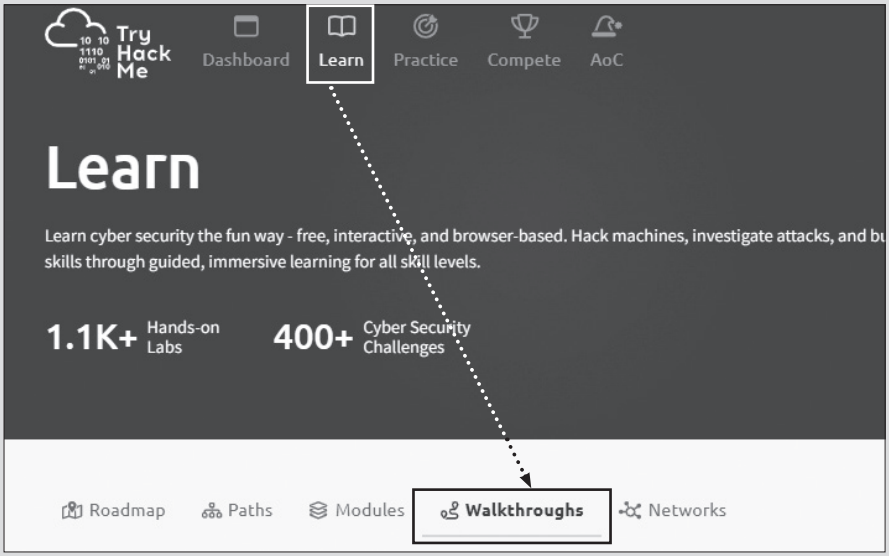
只需要使用今天設定好的 Kali，過程中將學會複製、移動檔案，在目錄內的查詢方法等 Linux 基本功，讓您跟小黑窗（終端機）變成好朋友。過關之後絕對已經學會接下來 7 天旅程路上的必備技能。等您來挑戰！

column

如何查找有興趣的房間

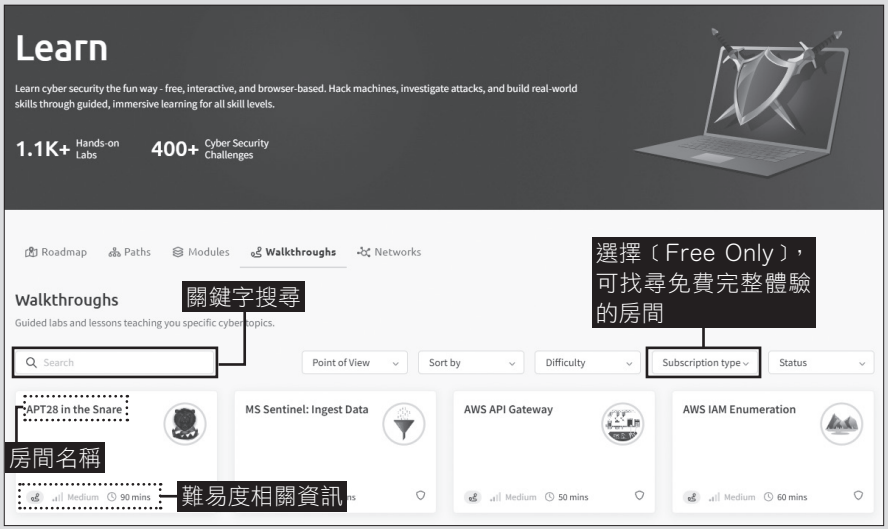
本書以一天為單位，依照順序挑戰不同房間。不過，TryHackMe 上已有 800 個以上的房間（截至本書撰寫時間點），從中挑選自己有興趣的房間也會相當有趣。

從 TryHackMe 網站上的選單依序點擊〔Learn〕→〔Walkthroughs〕，進入到可查找 Wolkthroughs 類型的房間或者其他學習內容的搜尋畫面。



從 Walkthroughs 當中右邊數來第二個下拉式選單裡選擇〔Free Only〕，可單純顯示免費房間的查詢結果，如果您並非付費的話，此篩選動作可以幫助您過濾不必要的資訊（付費相關內容請參閱第 87 頁的 Column）。

也可以任意使用其他有興趣的關鍵字查找，發現更多令人玩味的房間吧！



此外，從上方選單當中依序點選〔Practice〕→〔Challenges〕，可挑選 Challenges（CTF）類型的房間。在 TryHackMe 裡，房間主要可分為〔Challenges（CTF）〕跟〔Walkthroughs〕兩種，請依據喜好選擇。

房間類型	含義
Challenges（CTF）	自行思考步驟進行攻略，遊戲元素較強的房間
Walkthroughs	如教學演練般、依照步驟解任務的學習房間

順帶一提，進入房間後若想要中途棄權，並不會受到懲罰。所以說，稍微試看看之後發現「啊，這不是我要的……」時，可直接擱著不管、轉而挑戰其他房間也沒問題。平常心看待，盡力而為吧！