物聯網設備（Wi-Fi）保安研究

2020 年 3 月

hkpc 生產力局

HKCERT

免責聲明

香港電腦保安事故協調中心及香港生產力促進局保留不時修改檔的權利而無須另行通知。

我們雖已盡力確保本文件所含資料均來自可靠來源，但香港電腦保安事故協調中心對任何錯誤或遺漏或使用相關資料所招致的結果概不負責。 本檔上的所有資料均以當時情況提供，不擔保其完整性、準確性、及時性、或使用相關資料所招致的結果，亦不作任何明示或隱含的保證，包括但不限於其性能保證、適售性和特定用途的適用性。

本檔包含的資料僅供參考。 信賴或使用相關資料由讀者自行承擔風險。 本文件的任何內容均不得在任何程度上替代讀者的獨立調查和合理的技術和商業判斷。 在任何情況下，香港電腦保安事故協調中心、香港生產力促進局、或其合作夥伴、員工或代理商，均不對你或任何人信賴本文件相關資料做出的任何決定或行動，或任何後果性，特殊或類似的損害承擔責任。

版權

目錄

1. 背景

無線技術急速發展，物聯網的應用亦越來越廣泛。每種物聯網設備會因應各自的應用要求採用合適的無線技術，當中以 Wi-Fi 最受歡迎，主要由於具備傳輸速率快，設置簡易等優點，所以在家用及商用設備皆十分普遍，用戶可以方便快捷地使用個人電腦、手機連接 Wi-Fi 上網。

Wi-Fi 最顯而易見的優點是它幾乎能滿足所有物聯網設備的聯網要求，所以許多日常生活中常見的物聯網設備，都具有 Wi-Fi 功能，例如網絡攝影機、智能家居電器等；惟它們的網絡保安風險亦不容忽視。任何透過 Wi-Fi 連接互聯網的物聯網設備都會面對網絡安全威脅。同時，Wi-Fi 技術的認證和加密方法也存在各式各樣的保安漏洞。固此，Wi-Fi 的網絡保安引起了一般用戶、IT 營運商和產品開發者的廣泛關注。

物聯網設備的保安防護程式相對較少，加上用戶經常會忽略更新設備的網絡保安修補程式，大大增加設備受網絡攻擊的機會。攻擊者可以通過破解 Wi-Fi 密碼等方式入侵用戶的 Wi-Fi 網絡，然後利用不當的設備配置或漏洞進行攻擊，竊取敏感資訊、遠程執行程式碼等。

HKCERT 以 Wi-Fi 網絡配置及 Wi-Fi 物聯網設備進行保安測試及研究，期望測試結果能夠闡述有關保安問題，從而提高一般用戶和開發人員對物聯網設備的保安意識。

2. Wi-Fi 保安研究

Wi-Fi 在智能家居領域的應用相當廣泛，譬如網絡攝影機、智能家居電器等都可以通過 Wi-Fi 在智能家居環境中連接到互聯網，讓用戶使用手機應用程式或電腦應用程式來監控設備 (Fig. 2.1)。攻擊者可以通過破解 Wi-Fi 密碼等方式入侵用戶的 Wi-Fi 網絡，然後利用設備的配置不當或保安漏洞進行網絡攻擊，從而竊取敏感資訊或者遠程執行程式碼等。

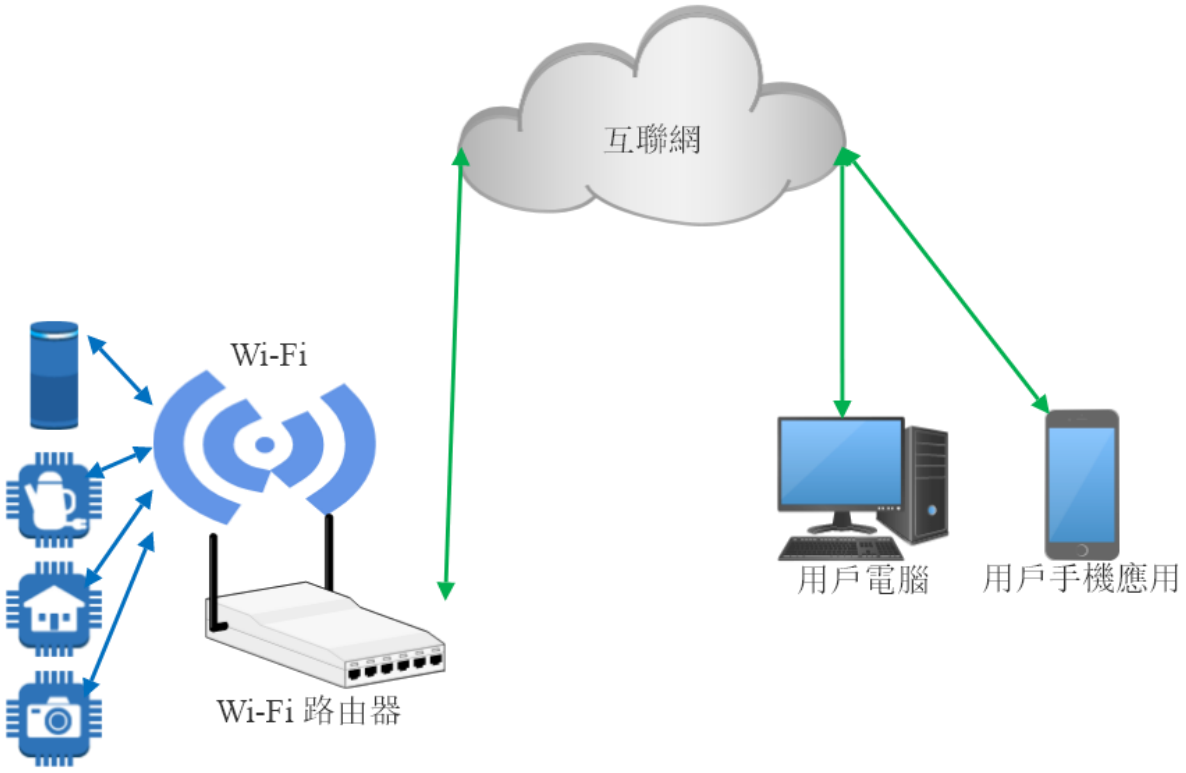

Fig. 2.1 用戶 Wi-Fi 物聯網設備使用範例

為保證 Wi-Fi 物聯網環境及設備的網絡安全，需要做好並嚴格執行以下兩方面，包括：

1. 正確配置 Wi-Fi 物聯網環境，防止網絡被入侵，同時將物聯網設備的網絡與電腦和手機使用的網絡分隔；以及
2. 確保連接 Wi-Fi 的物聯網設備的保安，及時修補設備漏洞。

本文將從配置 Wi-Fi 物聯網環境及 Wi-Fi 物聯網設備兩個方面進行網絡保安研究，並會為設備的一般用戶和開發人員提供 Wi-Fi 物聯網環境及設備的網絡保安建議。

3. 配置 Wi-Fi 物聯網環境保安研究

在 Wi-Fi 技術的領域，Wi-Fi 的保安有以下兩方面的涵義：

1. 控制誰可以連接並配置 Wi-Fi 網絡和設備；及
2. 防止通過 Wi-Fi 網絡無線傳輸的資料被未經授權查看。

要做到以上兩點，就需要通過認證才可連接無綫網絡和對無綫傳輸的數據進行加密。本文會介紹和分析 Wi-Fi 認證加密協議，同時為設備用戶在配置 Wi-Fi 物聯網環境時提供保安建議。

3.1 Wi-Fi 認證加密方式保安分析

Wi-Fi 協議的認證加密方式有五種，分別是：

- 開放式網絡；
- 有線等效保密（WEP）；
- Wi-Fi Protected Access（WPA）；
- Wi-Fi Protected Access 2（WPA2）；及
- Wi-Fi Protected Access 3（WPA3）。

在上述加密方式中，WPA 和 WPA2 有 TKIP 和 AES 兩種加密方式，TKIP 多會配合 WPA 使用。另一方面，由於 WPA2 需使用 AES 加密算法，因此 AES 會配合 WPA2 一起使用。下表介紹各種 Wi-Fi 協議認證加密方式的保安程度及使用建議。

Wi-Fi 協議 認證加密方式	**保安程度**	**使用建議**
開放網絡	不安全，無驗證及加密，存在數據被竊取及設備被攻擊的風險。	不建議使用。
WEP	不安全，WEP 密碼可被自動破解工具於數分鐘內破解。	不建議使用。
WPA+TKIP	不安全，TKIP 可讓攻擊者解密網絡上的數據包並注入任意數據到無線網絡中。	不建議使用。
WPA2+AES	存在風險，會被暴力破解，存在 KRACK 漏洞以及 KrØØk 漏洞，使用受影響的 Wi-Fi 晶片的設備的加密傳輸可能會被未經授權的解密，造成資料洩漏。	在 WPA3 普及前建議使用。需要及時更新補丁修補漏洞。
WPA3	安全。WPA3 修復 WPA2 上的漏洞，不再能被暴力破解，同時亦不會受到 KRACK 和 KrØØk 漏洞的影響。	建議使用，但 WPA3 尚未普及。

Fig. 3.1.1 Wi-Fi 協議認證加密方式的保安程度及使用建議

由 Fig. 3.1.1 可見，儘管 WPA3 是目前保安程度最好和最值得推薦的 Wi-Fi 認證和加密方法，它的普及度仍處於起步階段。雖然目前已經有支援 WPA3 的 Wi-Fi 設備上市，而 Windows 10、iOS 13 和 Android 10 亦增加了對 WPA3 的支持，但大部分物聯網設備並不支持 WPA3，所以目前要配置 Wi-Fi 物聯網環境時，仍建議使用 WPA2+AES 模式。

WPA2+AES 同時存在密碼被暴力破解的風險和可導致資料外洩的漏洞。HKCERT 會對 WPA2+AES 進行保安分析，並提供保安建議。

物聯網設備的保安防護程式相對較少，加上用戶經常會忽略更新設備的網絡保安修補程式，大大增加設備受網絡攻擊的機會。攻擊者可能入侵有漏洞的物聯網設備，進而攻擊位處同一網絡內的電腦和手機。為了避免這種情況，我們建議在配置 Wi-Fi 物聯網環境時，分隔物聯網設備的網絡與電腦和手機使用的網絡。

3.2 WPA2+AES 保安分析

由於 WPA2+AES 密碼存在被暴力破解的漏洞，所以保安強度較弱的密碼可能會在短時間內成功地被暴力破解。WPA2+AES 密碼要求最少 8 位，但沒有要求密碼設置得複雜，因此以 8 位數字作為密碼的情況亦很常見，例如使用電話號碼作為密碼。本中心使用測試平臺對 8 位數字這類保安程度較弱的密碼進行暴力破解，結果在一分鐘內密碼就被成功破解 (Fig 3.2.1)，可見 8 位數字的密碼形同虛設。

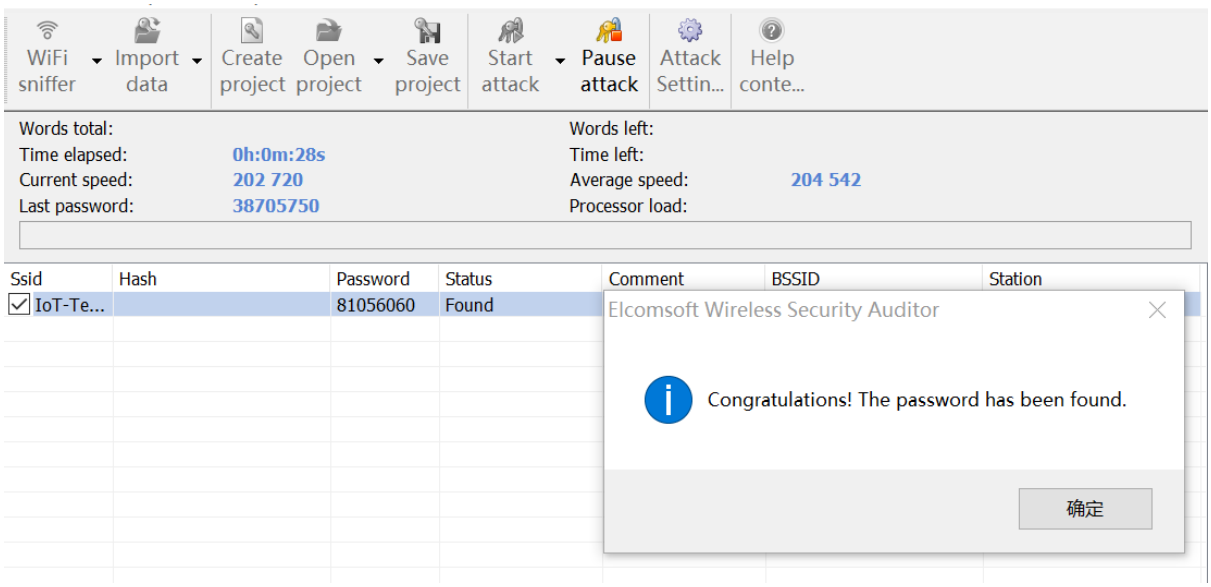

Fig. 3.2.1 暴力破解 WPA2+AES 密碼

Wi-Fi 保護設置（WPS）功能是為了解決 WPA/WPA2 認證步驟過於繁雜而設，但由於其 PIN 碼的強度有限，可以在短時間內被破解。PIN 碼被破解後，即使用戶更改了 Wi-Fi 密碼，攻擊者仍可以利用 WPS PIN 碼連接 Wi-Fi。因此，用戶應停用 WPS 功能，而改用 WPS 按鍵連接功能。後者可以讓用戶在有需要時才開啓 WPS，然後當成功連接設備或連接時限完結時，WPS 會自動關閉，以避免 WPS 被暴力破解。

除了密碼能被暴力破解外，WPA2+AES 還存在 KRACK 和 KrØØk 兩個保安漏洞。設備使用受影響 Wi-Fi 晶片進行的加密傳輸可能遭受未經授權的讀取及解密，造成資料外洩。用戶需要及時更新設備廠商推出的修補程式，堵塞漏洞。

3.3 配置 Wi-Fi 物聯網環境的保安建議

以下是 HKCERT 給用戶配置 Wi-Fi 物聯網環境的保安建議：

- 最好使用 WPA3 認證加密方式。然而在 WPA3 進一步普及前，建議使用 WPA2+AES 認證加密方式，使用位元數多及較複雜的密碼，類似「dfgP94$Zwdngf!」等包含大小寫的字母、數字及非字母字符；
- 關閉 WPS 功能或者使用 WPS 按鍵才可連接功能；
- 關注 Wi-Fi 的漏洞情況，及時更新補丁修補漏洞；及
- 分隔物聯網設備的網絡與電腦、手機使用的網絡。

4. Wi-Fi 物聯網設備保安研究

除了 Wi-Fi 物聯網環境安全外，Wi-Fi 物聯網設備本身的保安亦是影響使用 Wi-Fi 物聯網設備時的保安程度之重要因素。即使攻擊者能入侵用戶的 Wi-Fi 物聯網網絡，只要網絡內的物聯網設備沒有保安漏洞，攻擊者亦無從下手。是次研究中，我們使用 Wi-Fi 路由器、智能加濕器（智能家居）、家庭保安監控設備的控制中心及網絡攝影機，模擬一個家用的 Wi-Fi 物聯網環境 (Fig 4.1.1)，通過上一個章節提及的暴力破解方式破解了 Wi-Fi 密碼，然後對網絡內的物聯網設備進行保安測試，找尋這些設備是否存在漏洞。下圖是我們測試的示意圖。

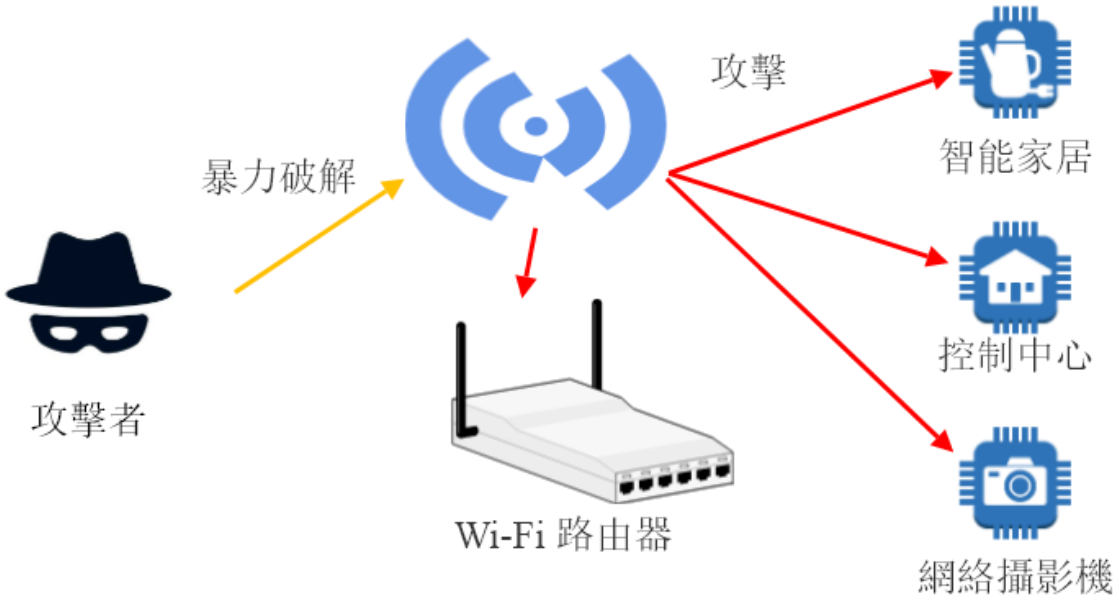

Fig. 4.1.1 物聯網設備測試示意圖

通過測試，我們發現 Wi-Fi 物聯網設備存在三個保安漏洞，包括：

- 設備通訊埠弱管理漏洞
- 傳輸無加密漏洞
- 設備身份驗證弱管理漏洞

以下我們會對這三個漏洞進行分析。

4.1 設備通訊埠弱管理漏洞

物聯網設備通過通訊埠提供連接服務，我們對以下物聯網設備的通訊埠進行掃描 (Fig. 4.1.2)，查看通訊埠開放的情況。下表是設備的通訊埠開放情況。

設備	開放的通訊埠
Wi-Fi 路由器	21, 22, 23, 53, 80, 2000, 8291
智能加濕器	6668
監控設備控制中心	23, 53, 80
網絡攝影機	80, 554, 2020, 8080, 8081, 8088

Fig. 4.1.2 物聯網設備通訊埠開放情況

從圖表可見，除了智能加濕器外，其他三個設備皆預設開放過多無必要的通訊埠，而這些開放的通訊埠亦存在管理漏洞，讓攻擊者可以通過攻擊通訊埠入侵設備。在各通訊埠中，我們發現控制中心開放的通訊埠 23 所運行的 Telnet 服務存在漏洞，允許毋須賬戶及密碼直接登錄，並且使用的是管理者權限，即是假如攻擊者入侵該設備後就可以遠端執行惡意程式碼，可以把該設備變成他們的殭屍網絡設備。（測試詳情可參考章節 6.1）

4.2 傳輸無加密漏洞

最新發現的 KrØØk 漏洞會造成 WPA2+AES 加密的資料被非法解密，使傳輸中的資料外洩。惟該漏洞只會造成 Wi-Fi 網絡的 WPA2+AES 加密失效，而不會解密已利用物聯網設備應用程式加密的資料。因此，對於傳輸敏感資料的物聯網設備，其傳輸的加密十分重要，例如網絡攝影機。

測試發現網絡攝影機未有加密傳輸，更可以在傳輸的明文數據中找到設備的賬戶密碼等敏感資料，攻擊者能竊聽數據，從而登陸該網絡攝影機進行監控及操作（測試詳情可參考章節 6.2），因此建議在設備管理界面中使用 HTTPS 協議代替沒有加密的 HTTP。

4.3 設備身份驗證弱管理漏洞

不少物聯網設備譬如 Wi-Fi 路由器，網絡攝影機等，都設有一個用賬戶密碼登入的管理界面，以便用戶對設備進行管理。如果攻擊者破解設備的賬戶密碼，入侵設備的管理界面，就可以觸發遠端執行程式碼、資料外洩等攻擊。因此物聯網設備必須有身份驗證的保護措施，譬如強制要求應用複雜密碼、防止暴力攻擊、使用雙重認證等。

測試發現 Wi-Fi 路由器和網絡攝影機皆有身份驗證薄弱的管理漏洞，它們的部分通訊埠沒有針對暴力破解密碼的保護措施，可以通過暴力破解便取得設備密碼，而由於設備沒有使用雙重認證，我們可以通過破解取得的賬戶密碼登入設備的管理界面進行監控及操作。我們會以 Wi-Fi 路由器為例子演示暴力破解過程。詳細測試細節可參考章節 6.3。

4.4 Wi-Fi 物聯網設備的保安測試結果摘要和風險

設備	通訊埠弱管理漏洞	傳輸無加密保安漏洞	身份驗證弱管理漏洞	保安風險
Wi-Fi 路由器	有	沒有	有	存在被攻擊者登陸監控及操作的風險，攻擊者可以將設備變成殭屍網絡。
智能加濕器	沒有	沒有	不適用	如果用戶的設備雲端賬戶被盜，會導致設備被攻擊者操控。
監控設備控制中心	有	沒有	不適用	存在被完全控制的風險，導致設備失去監控功能以及變成殭屍網絡。
網絡攝影機	有	有	有	存在泄露個人敏感資料的風險。

Fig. 4.4.1 Wi-Fi 物聯網設備的保安測試結果摘要和風險

4.5 配置和設計 Wi-Fi 物聯網設備的建議

一般用戶

- 首次使用設備時更改預設管理員名稱和密碼；
- 首次使用設備時，關閉不必要的網絡通訊埠；
- 要使用位元數多及足夠複雜的密碼作為設備密碼；
- 如果設備有雙重認證功能，啓用該功能；
- 定期檢查物聯網設備設定，如果設定意外地被更改，請立即重置設備賬戶並繼續監控；
- 將物聯網設備固件更新至最新版本；以及
- 注意網上公布物聯網設備的保安問題。

產品開發人員

- 把「保安從設計做起」原則應用於軟件開發生命週期；
- 強制在默認情況關閉不必要的網絡通訊埠，對開放的網絡通訊埠進行身份認證及權限管理；
- 確保傳輸時需要加密數據和密碼；
- 強制首次使用設備需更改預設密碼；
- 設備密碼需符合複雜性要求，如長度至少 8 個字元，必須包括大小寫字母、數字和特殊字元；
- 在系統上配備防止暴力攻擊機制，如密碼嘗試失敗 10 次後鎖定賬戶；
- 在系統上配備雙重認證功能；
- 提供保安漏洞的透明度，並持續為設備提供保安補丁，第一時間修補關鍵漏洞；以及
- 使用 HKCERT 的《物聯網保安最佳實踐指引》對產品進行評估。

5. 總結

- 在 WPA3 認證加密方式普及前，建議用戶使用 WPA2+AES 認證加密方式，惟需要注意使用正確的配置並及時更新程式以修補漏洞；
- 在 WPA3 認證加密方式普及後，要盡快改用 WPA3；
- 配置 Wi-Fi 物聯網環境時，分隔物聯網設備的網絡與電腦、手機使用的網絡；
- 開發人員應第一時間修補 Wi-Fi 物聯網設備的漏洞，推出修補安全性的更新程式；以及
- 開發人員可做更多改善工作，譬如參考 HKCERT 的《物聯網保安最佳實踐指引》對產品進行評估，提高產品的安全。

6. 附錄 - 保安測試

6.1 設備通訊埠管理漏洞保安測試

我們首先使用測試平臺掃描一款家庭保安監控設備的控制中心開放的通訊埠。

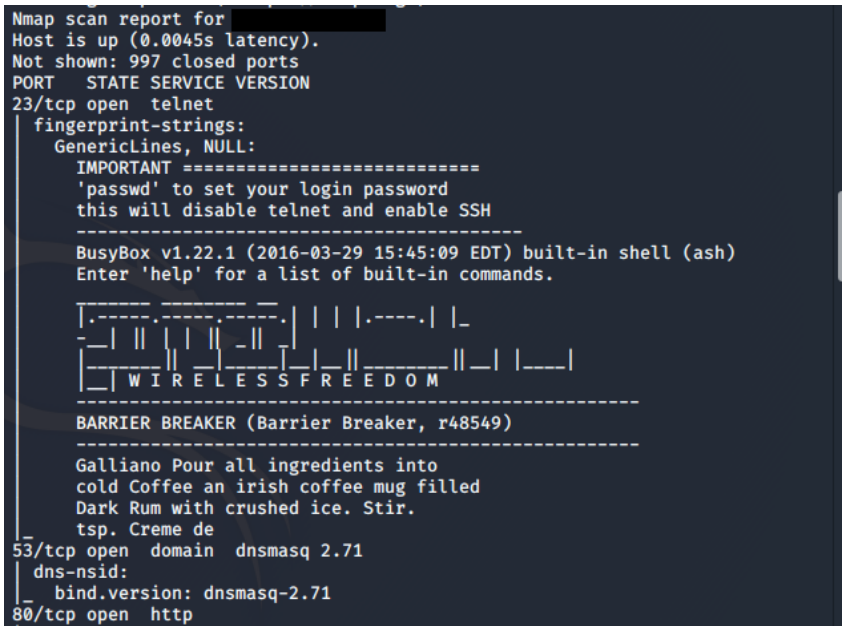

Fig 6.1.1 控制中心開放的通訊埠

可以看到，通訊埠 23、53、80 是開放的。通訊埠 23 是用於 Telnet 服務，傳統 Telnet 會話所傳輸的資料並未加密，帳號和密碼等敏感資料容易會被竊聽。所以我們選擇通訊埠 23 進行測試。

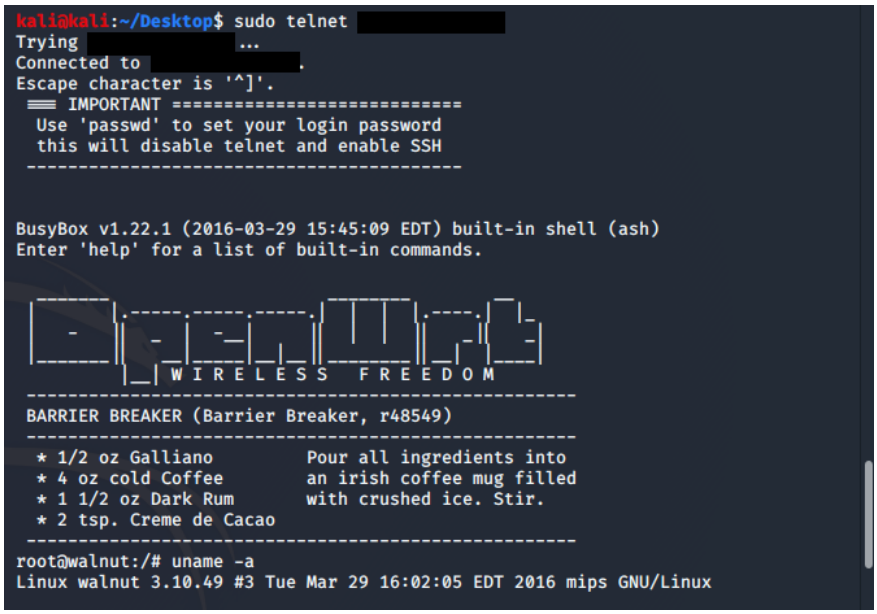

Fig 6.1.2 通訊埠 23 測試

我們用 telnet 指令連接控制中心，預設的設備密碼是空的，不需要輸入密碼即可登入設備，並且是擁有最高權限的 root 賬戶，可以在設備上讀寫數據和執行程式碼。這種漏洞非常容易被駭客利用，例如物聯網殭屍網絡 Mirai 惡意軟件就可以通過通訊埠 23 傳播，一旦該設備暴露在互聯網，就非常容易遭受攻擊，導致惡意軟件感染。

6.2 傳輸無加密漏洞保安測試

我們使用手機應用程式登陸網絡攝影機，通過測試平臺截取手機與網絡攝影機之間的通訊數據，在獲取的數據中發現網絡攝影機沒有對設備賬戶密碼等敏感資料進行加密。

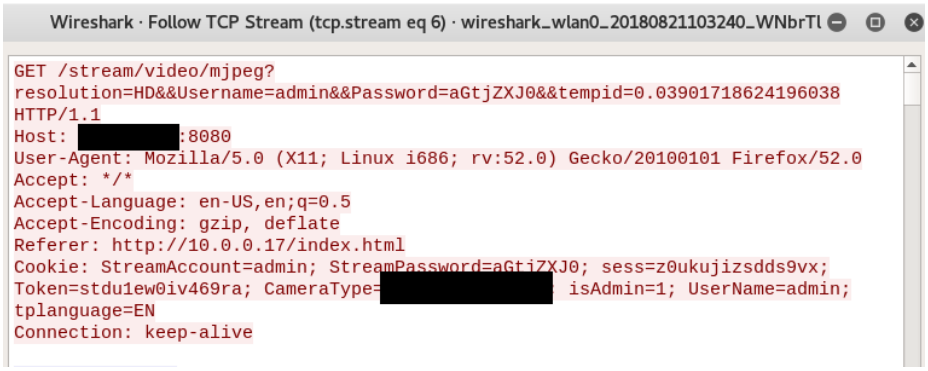

Fig 6.2.1 網絡攝影機明文傳輸數據

可以看到，網絡攝影機的賬戶密碼是明文傳輸的，網絡攝影機的密碼用 Base64 進行了編碼，Base64 可以通過解碼工具解碼，並不能起到保護的作用。

Fig 6.2.2 Base64 解密得到密碼

解密後，我們得到網絡攝影機的密碼，就可以通過賬戶密碼登陸設備的管理界面進行操作。

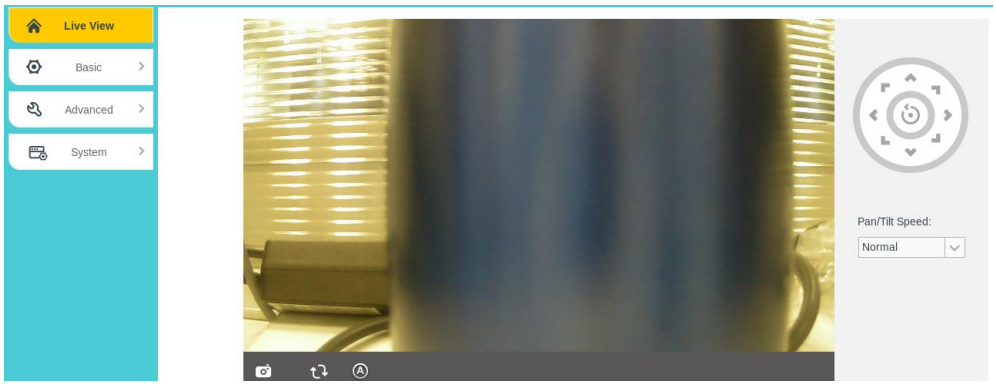

Fig 6.2.3 登陸網絡攝影機管理界面進行監控及操作

6.3 設備身份驗證保安測試

我們通過測試平臺掃描 Wi-Fi 路由器開放的通訊埠。

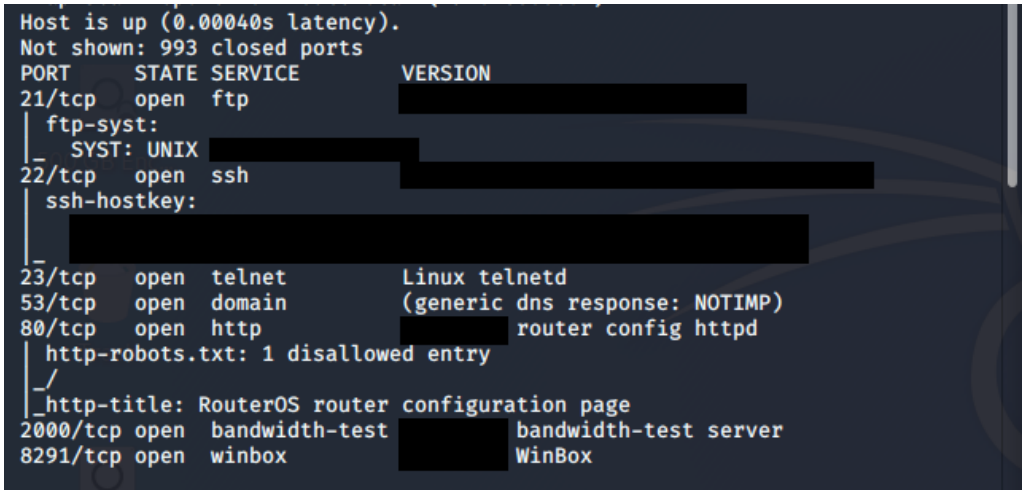

Fig 6.3.1 Wi-Fi 路由器開放的通訊埠

通過搜尋發現，該版本固件的通訊埠 8291 存在暴力破解的漏洞，可以使用預先準備的字典進行暴力破解。

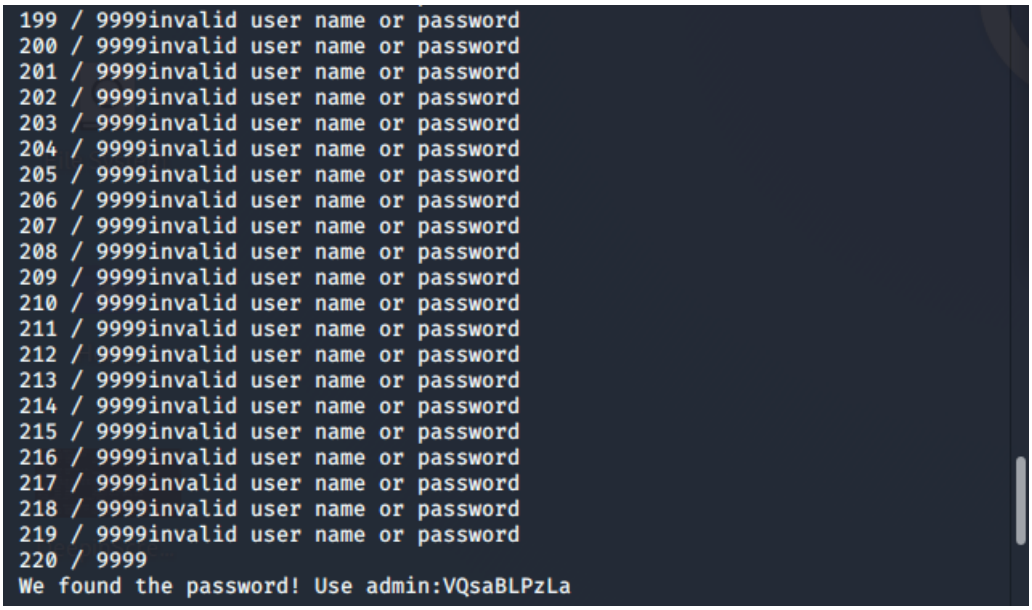

Fig 6.3.2 通訊埠 8291 暴力破解

破解密碼後，我們就可以用破解取得的密碼登陸 Wi-Fi 路由器的管理界面進行監控及操作。

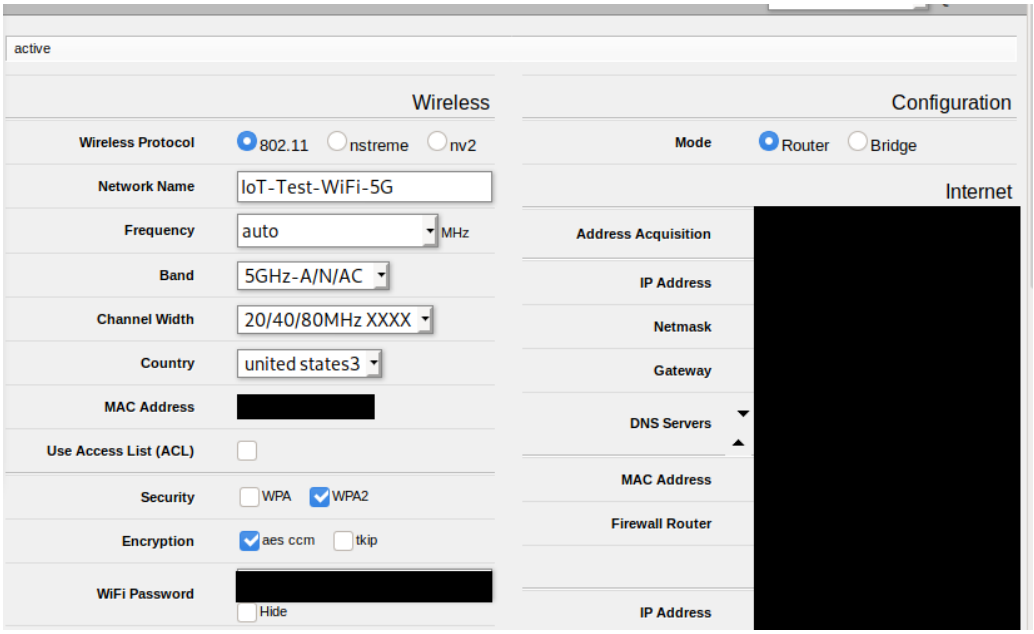

Fig 6.3.3 登陸 Wi-Fi 路由器管理界面進行監控及操作