教育單位
弱點檢測平台介紹

南投區網中心 楊世偉

110.10.12

Content

1. 弱點掃描簡介
2. 物聯網安全
3. EVS平台使用說明
4. 教育單位資安弱掃服務說明

弱點掃描

簡介

1. 甚麼是弱點掃描？
2. 弱點掃描的目的
3. 弱點掃描的途徑

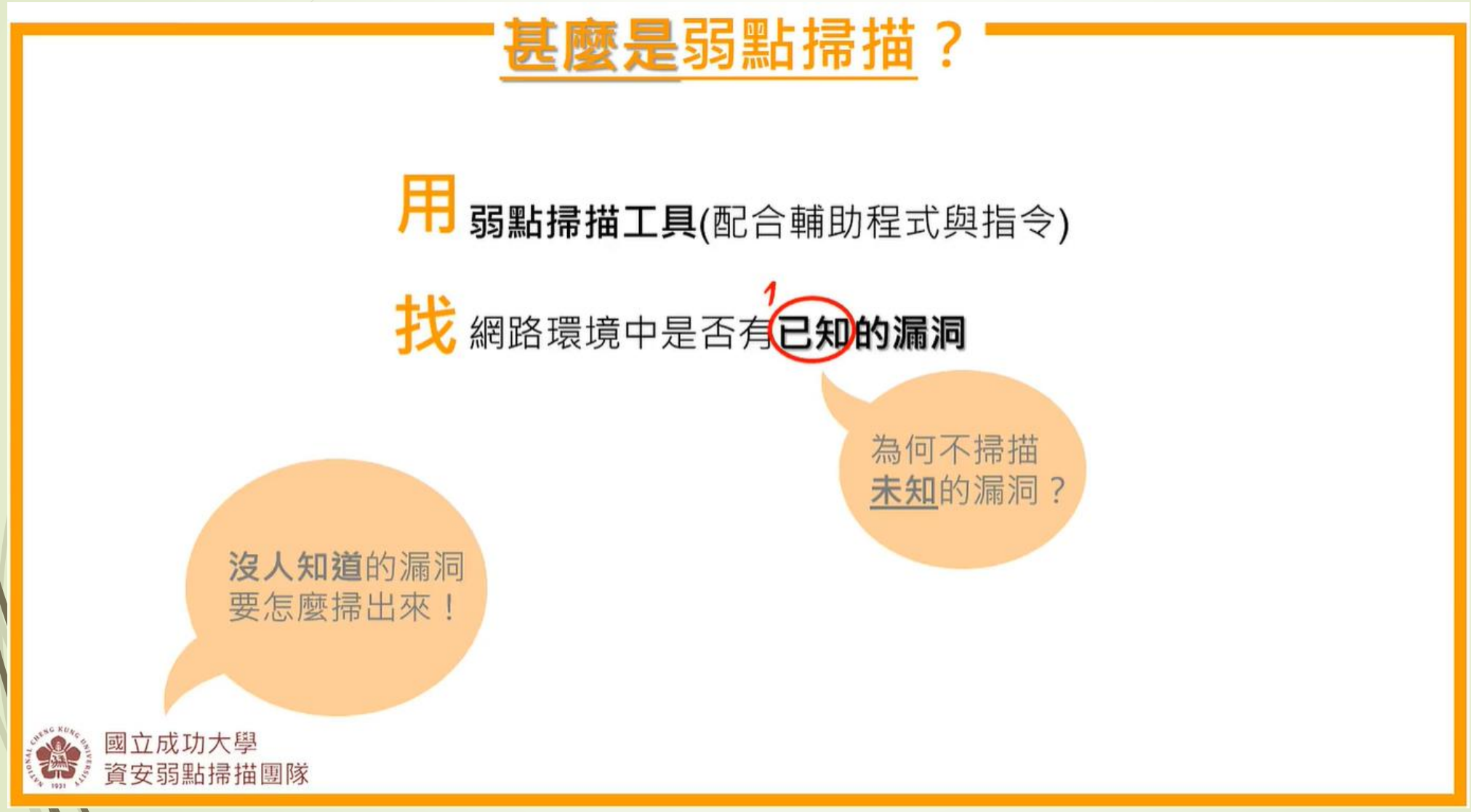
1.弱點掃描簡介

甚麼是弱點掃描？

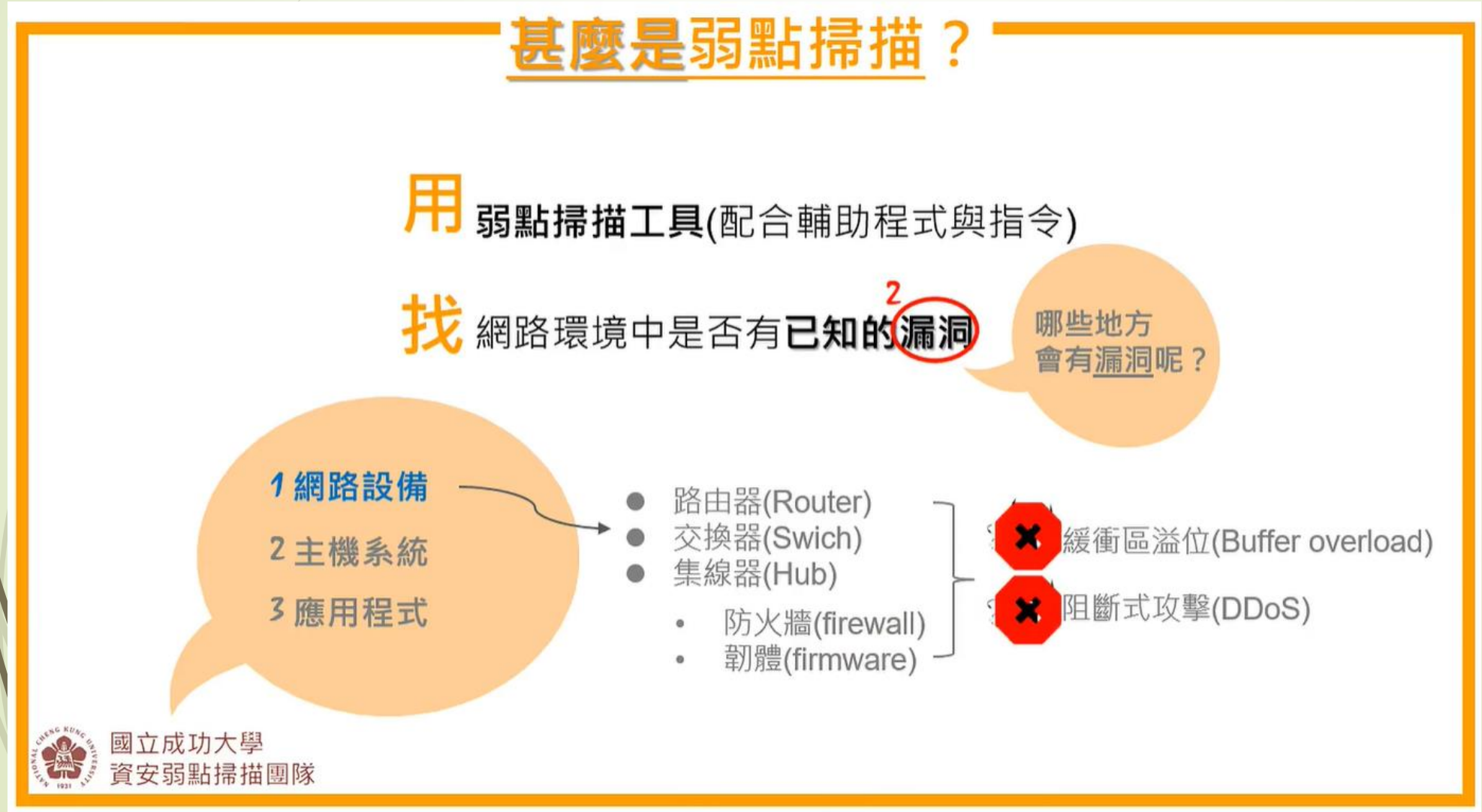
用 **弱點掃描工具**(配合輔助程式與指令)

找 網路環境中是否有**已知的漏洞**

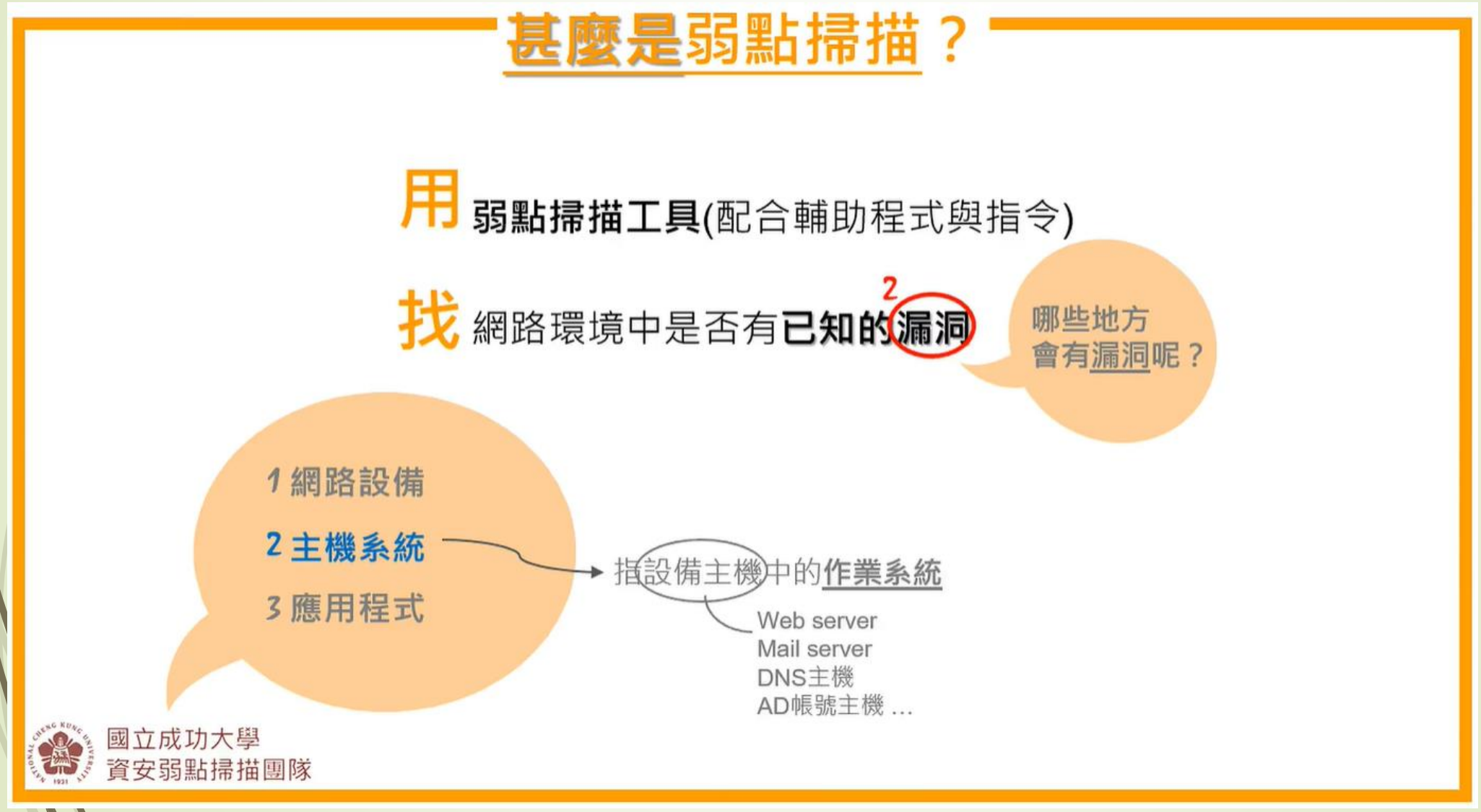
1.弱點掃描簡介


甚麼是弱點掃描？
用 弱點掃描工具(配合輔助程式與指令)
找 網路環境中是否有已知的漏洞
1
為何不掃描
未知的漏洞？
沒人知道的漏洞
要怎麼掃出來！
國立成功大學
資安弱點掃描團隊

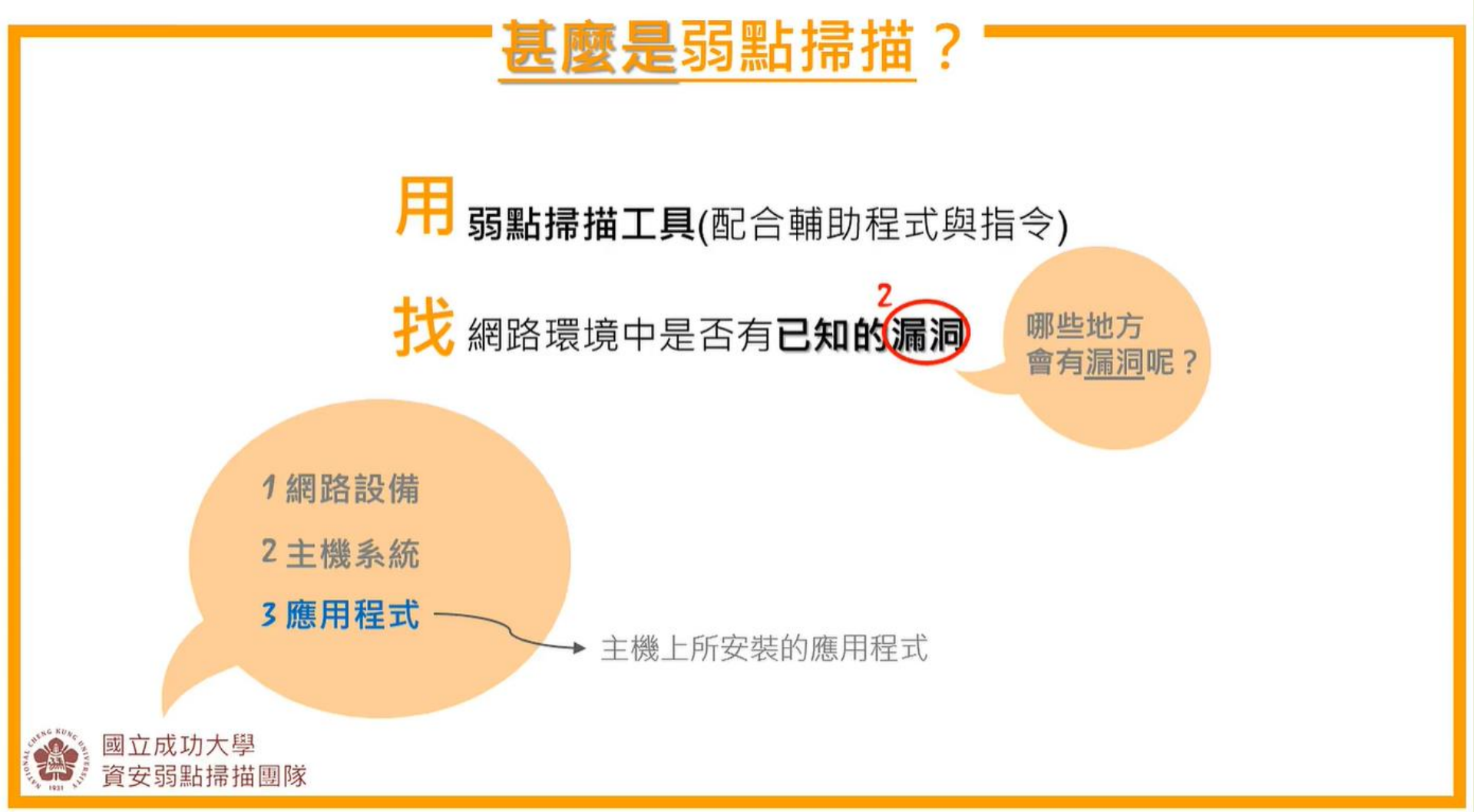
1.弱點掃描簡介


甚麼是弱點掃描？
用 弱點掃描工具(配合輔助程式與指令)
找 網路環境中是否有已知的漏洞
2
哪些地方
會有漏洞呢？
1 網路設備
2 主機系統
3 應用程式
路由器(Router)
交換器(Swich)
集線器(Hub)
防火牆(firewall)
韌體(firmware)
緩衝區溢位(Buffer overload)
阻斷式攻擊(DDoS)
國立成功大學
資安弱點掃描團隊

1.弱點掃描簡介


甚麼是弱點掃描？
用 弱點掃描工具(配合輔助程式與指令)
找 網路環境中是否有已知的漏洞
2
哪些地方
會有漏洞呢？
1 網路設備
2 主機系統
3 應用程式
指設備主機中的作業系統
Web server
Mail server
DNS主機
AD帳號主機 …
國立成功大學
資安弱點掃描團隊

1.弱點掃描簡介


甚麼是弱點掃描？
用 弱點掃描工具(配合輔助程式與指令)
找 網路環境中是否有已知的漏洞
2
哪些地方
會有漏洞呢？
1 網路設備
2 主機系統
3 應用程式
主機上所安裝的應用程式
國立成功大學
資安弱點掃描團隊

1.弱點掃描簡介

1.弱點掃描簡介

弱點掃描的目的

了解 入侵者可能利用的漏洞

提供 設備廠商**修補**與**改善**的方案

評估 是否**需要**購買設備、購買設備的**成效**

降低資安風險

1.弱點掃描簡介

1.弱點掃描簡介

1.弱點掃描簡介

弱點掃描的途徑

同樣掃描步驟、方法、工具軟體

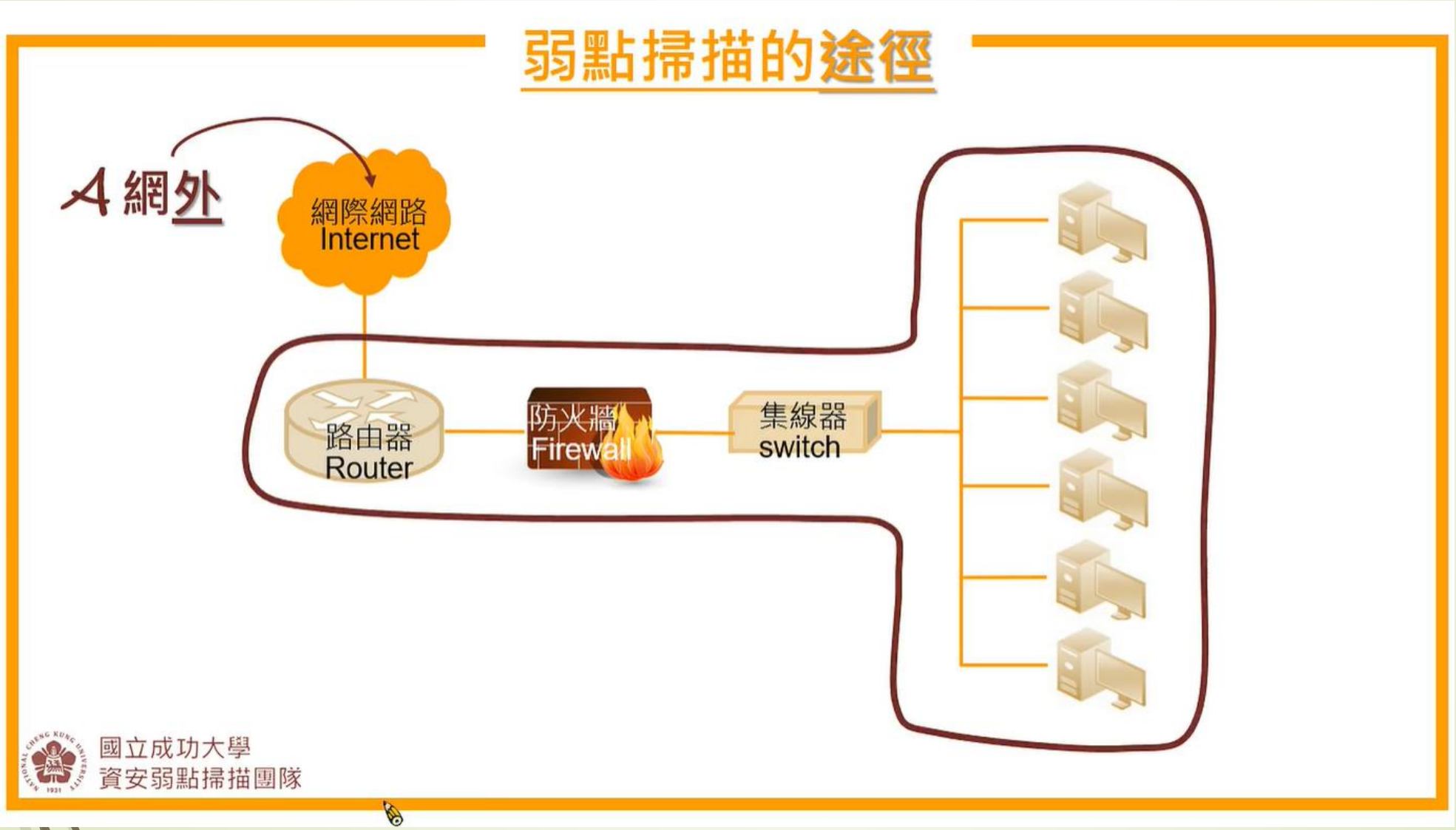
在不同「節點」展開掃描，結果會不一樣

A區域網路外

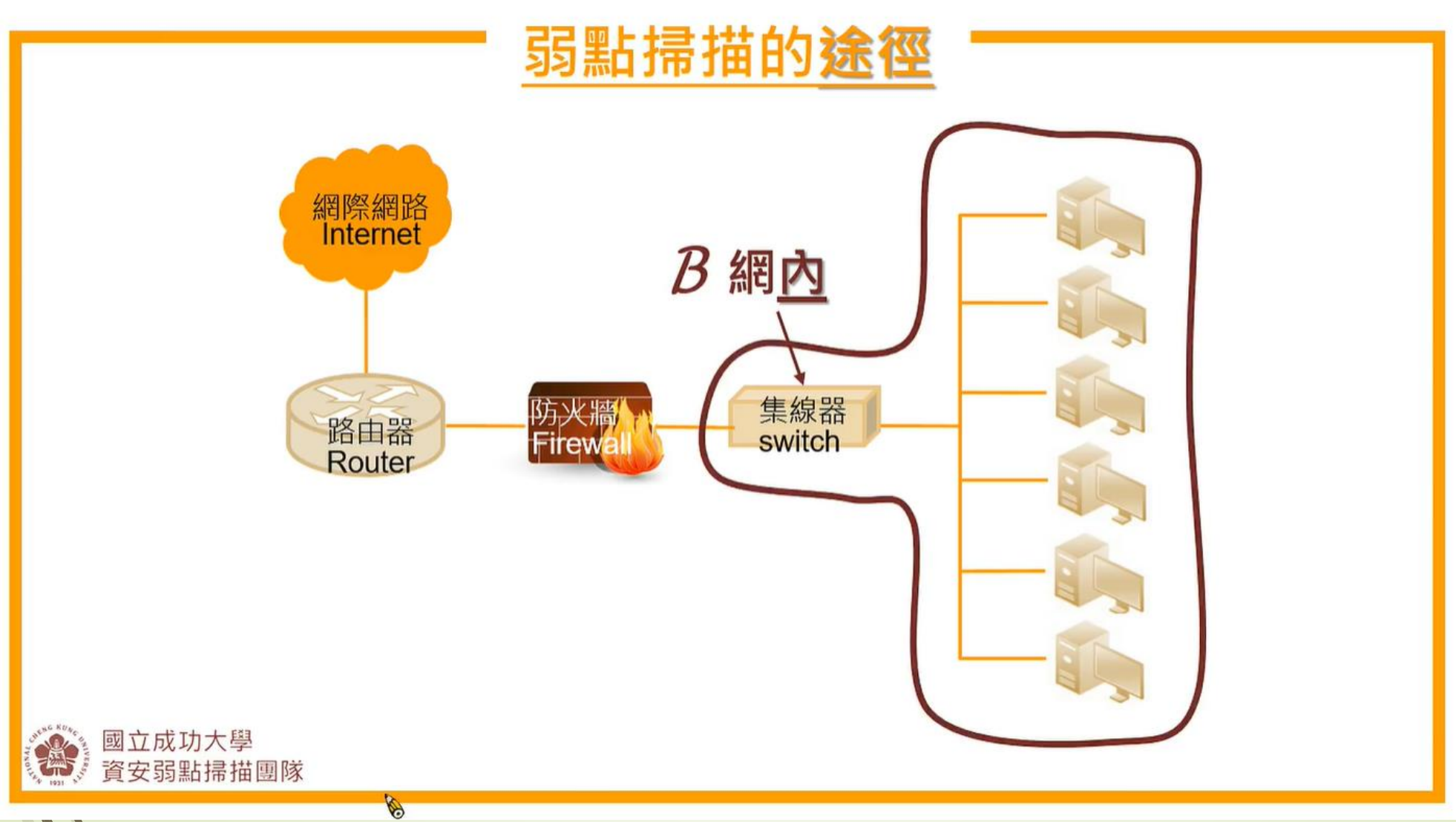
B區域網路內

C主機本身

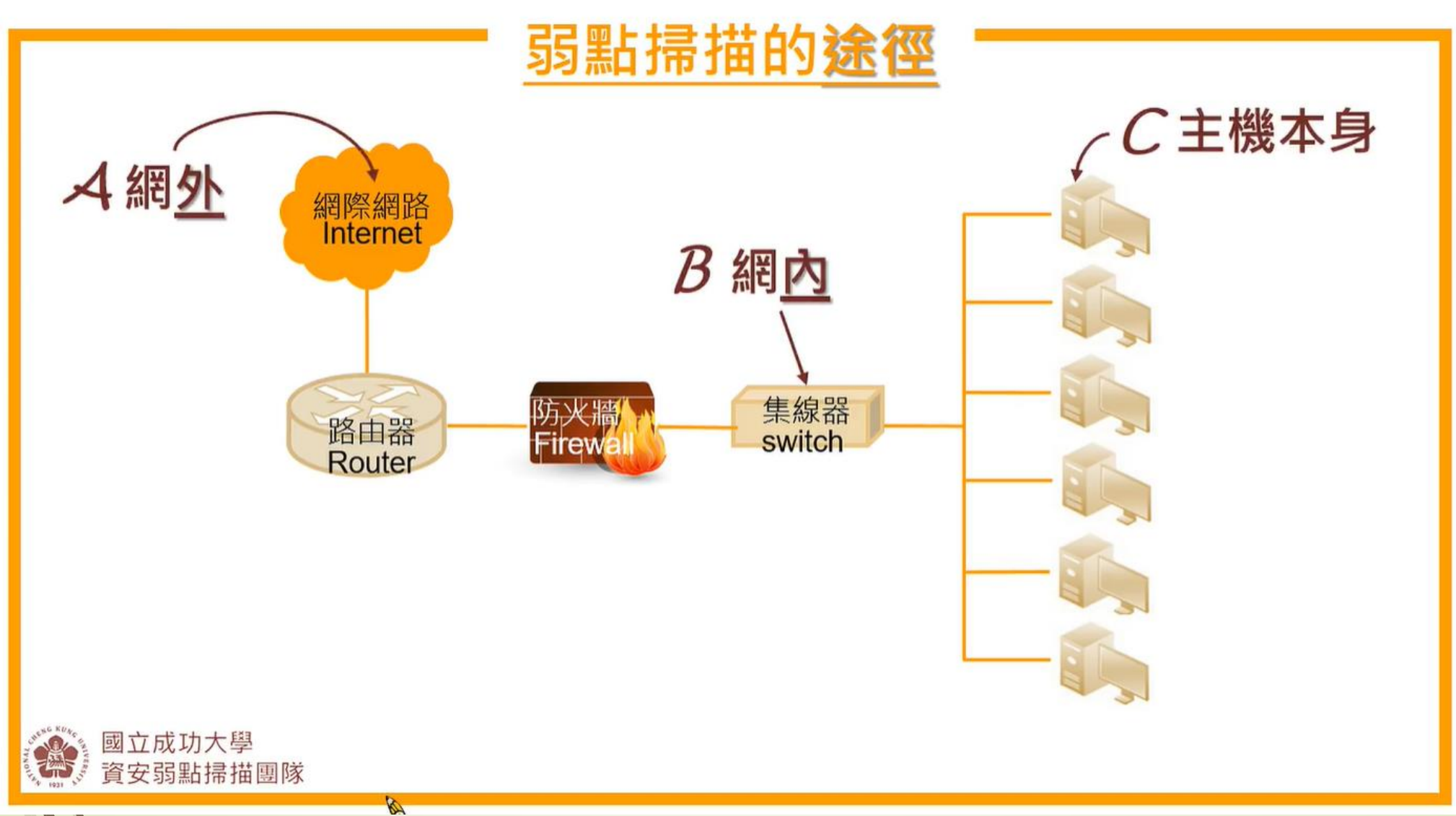
1.弱點掃描簡介


弱點掃描的途徑
網外
網際網路
Internet
路由器
Router
防火牆
Firewall
集線器
switch
國立成功大學
資安弱點掃描團隊

1.弱點掃描簡介


弱點掃描的途徑
網際網路
Internet
路由器
Router
防火牆
Firewall
B 網內
集線器
switch
國立成功大學
資安弱點掃描團隊

1.弱點掃描簡介


弱點掃描的途徑
A 網外
網際網路
Internet
路由器
Router
防火牆
Firewall
B 網內
集線器
switch
C 主機本身
國立成功大學
資安弱點掃描團隊

1.弱點掃描簡介

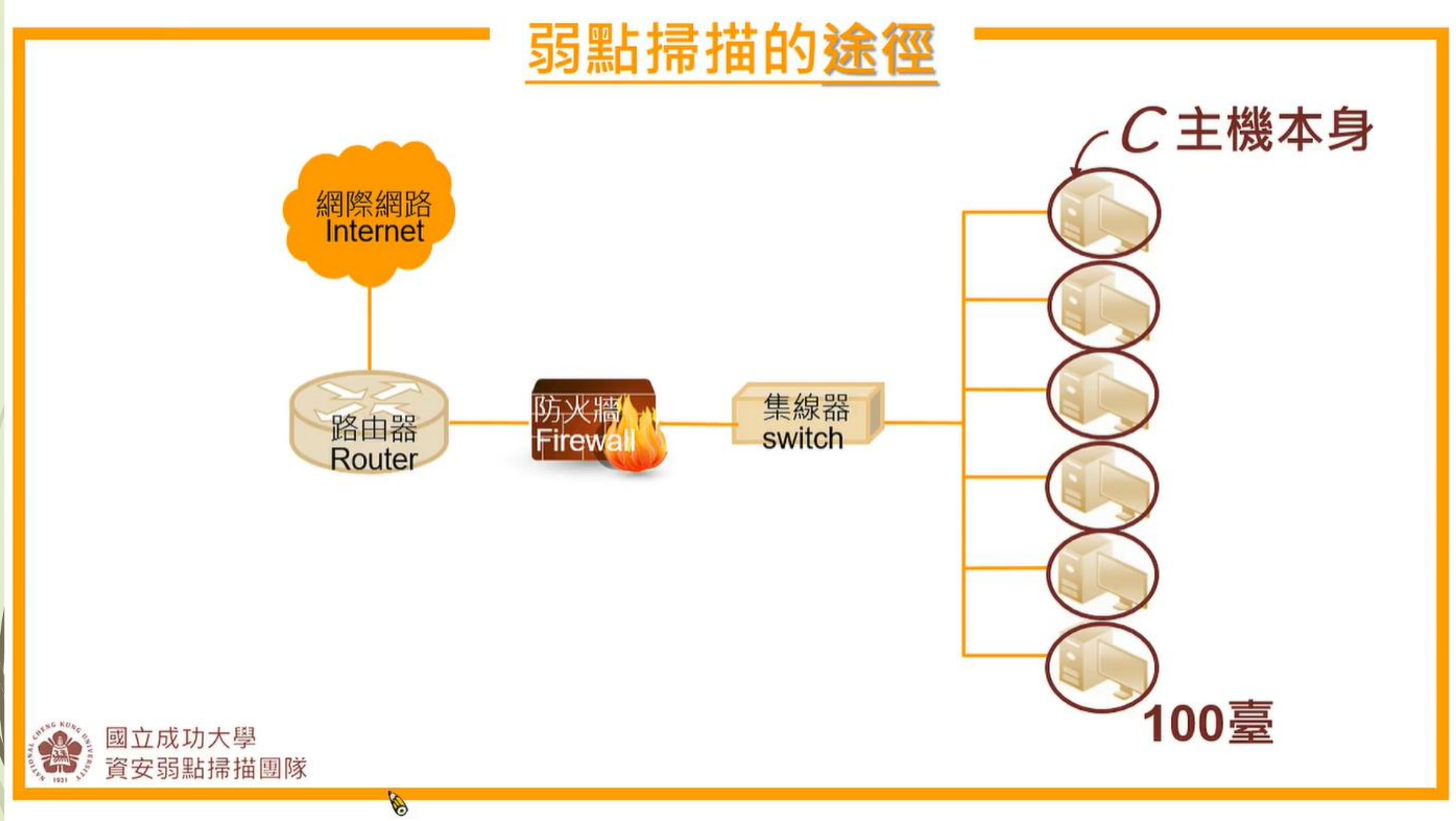
弱點掃描的目的

想想看

在哪個節點掃描，較能完整掃瞄出所有的漏洞呢？

國立成功大學
資安弱點掃描團隊

1.弱點掃描簡介


弱點掃描的途徑
C主機本身
網際網路
Internet
路由器
Router
防火牆
Firewall
集線器
switch
100臺
國立成功大學
資安弱點掃描團隊

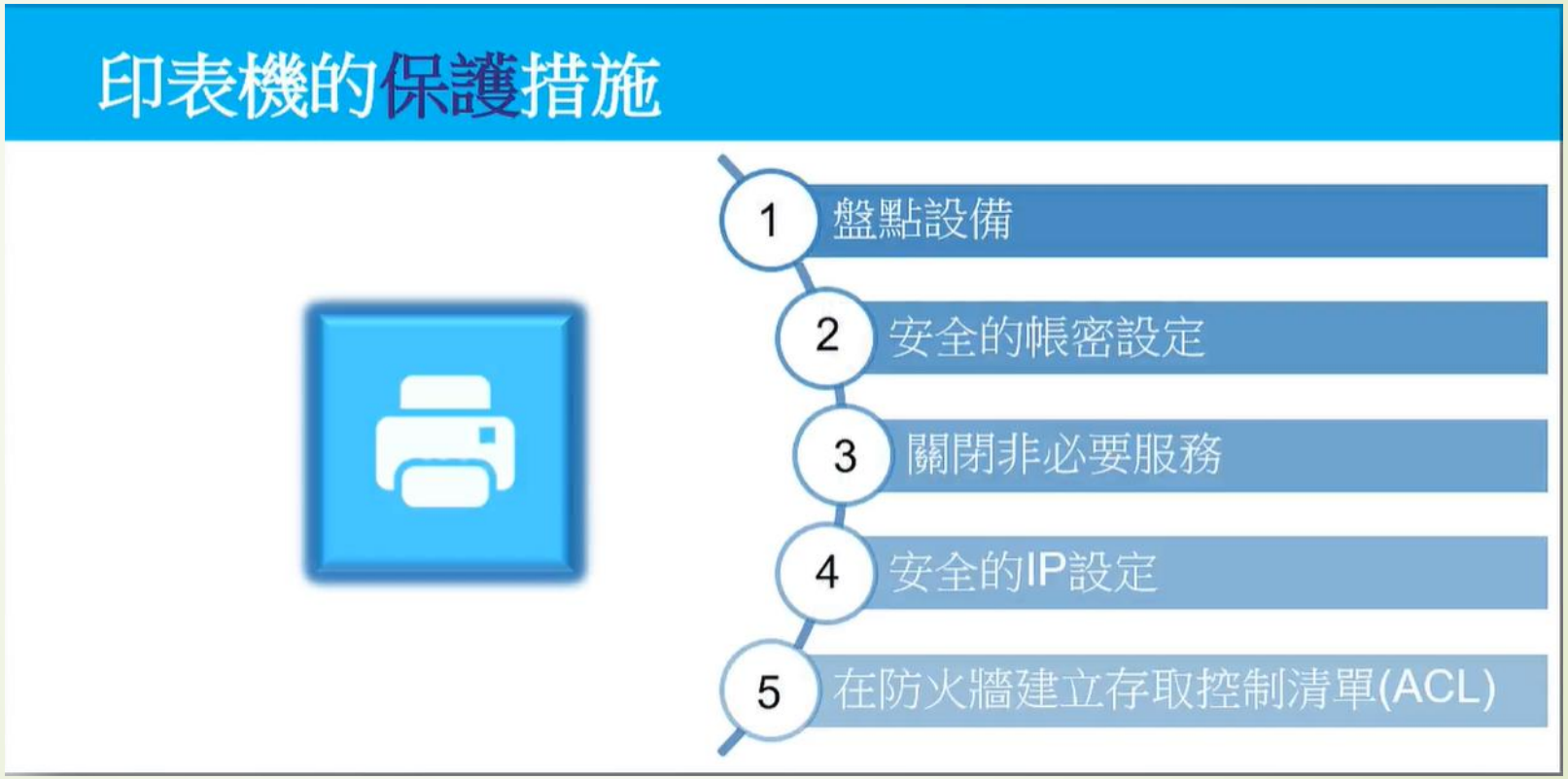
1.弱點掃描簡介

1. 以C:主機本身，較能完整掃描所有的漏洞
2. 實務上，以B:網內，較符合現況。

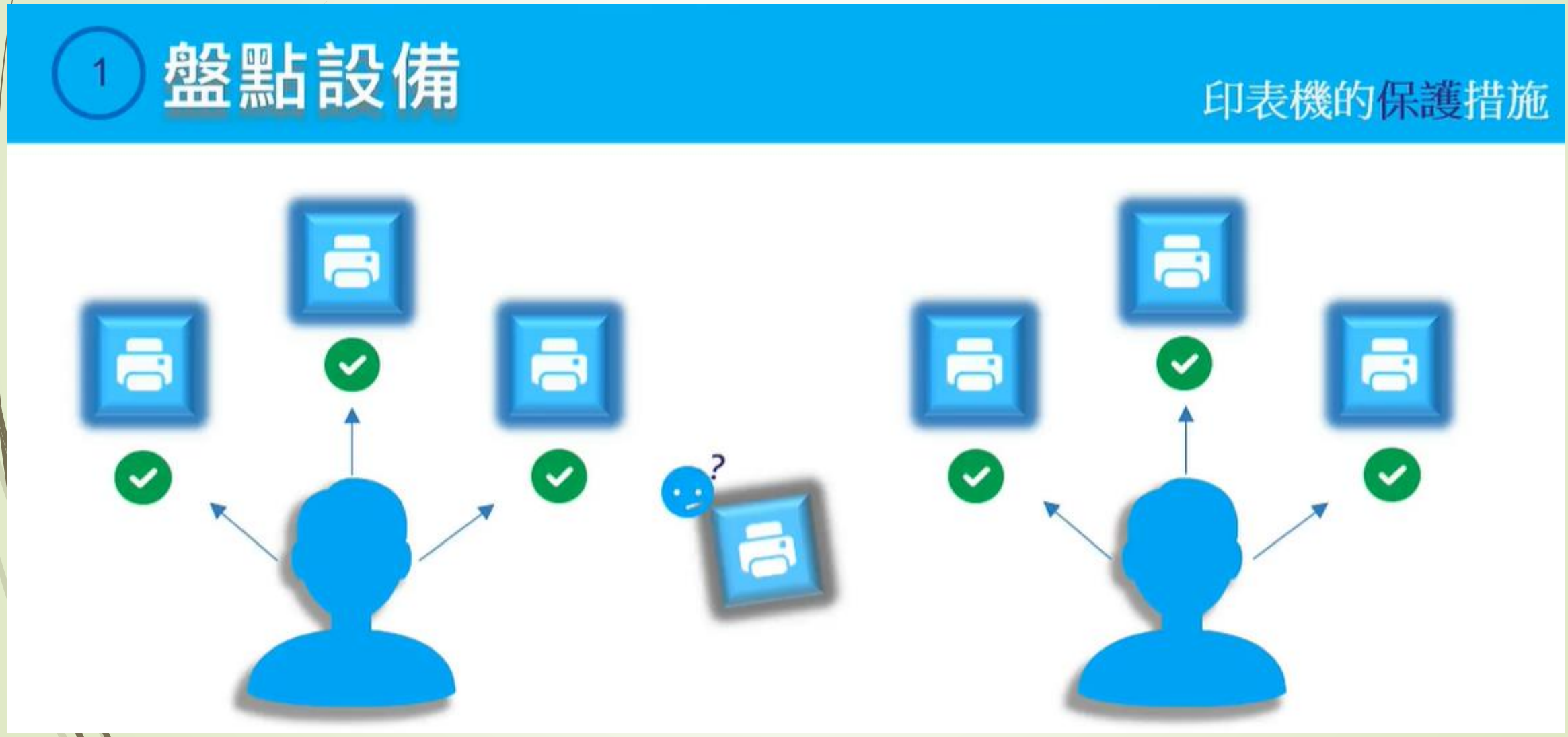
2.物聯網安全

- 網路印表機
- 網路攝影機

2.物聯網安全-網路印表機



2.物聯網安全-網路印表機



2.物聯網安全-網路印表機

2 安全的帳密設定

印表機的保護措施

避免使用預設密碼

並設定**8位數**以上

英文、數字、符號結合的密碼

您的印表機會安全許多！

2.物聯網安全-網路印表機

2 安全的帳密設定

印表機的保護措施

密碼設定範例

帳號：ntrc

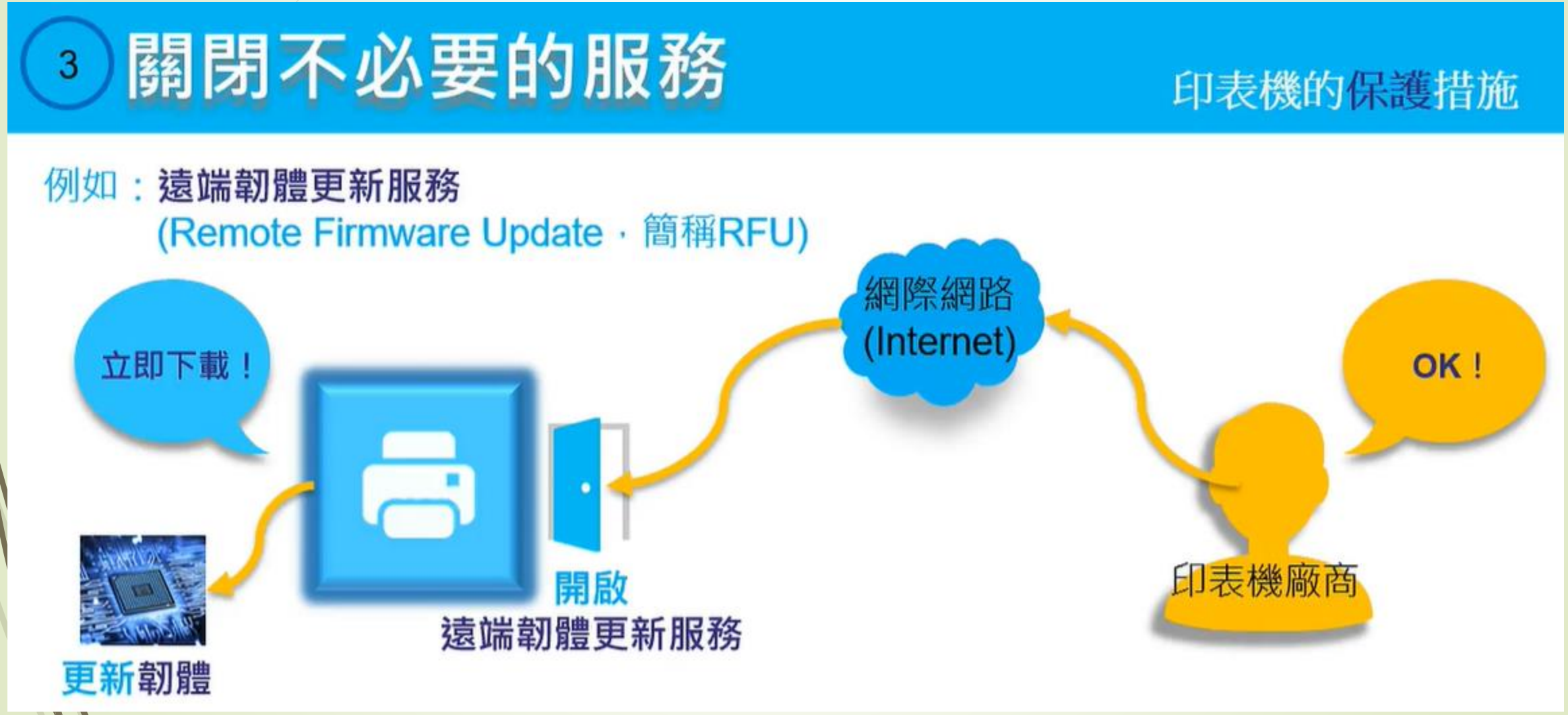
密碼：1060407a

1060407a

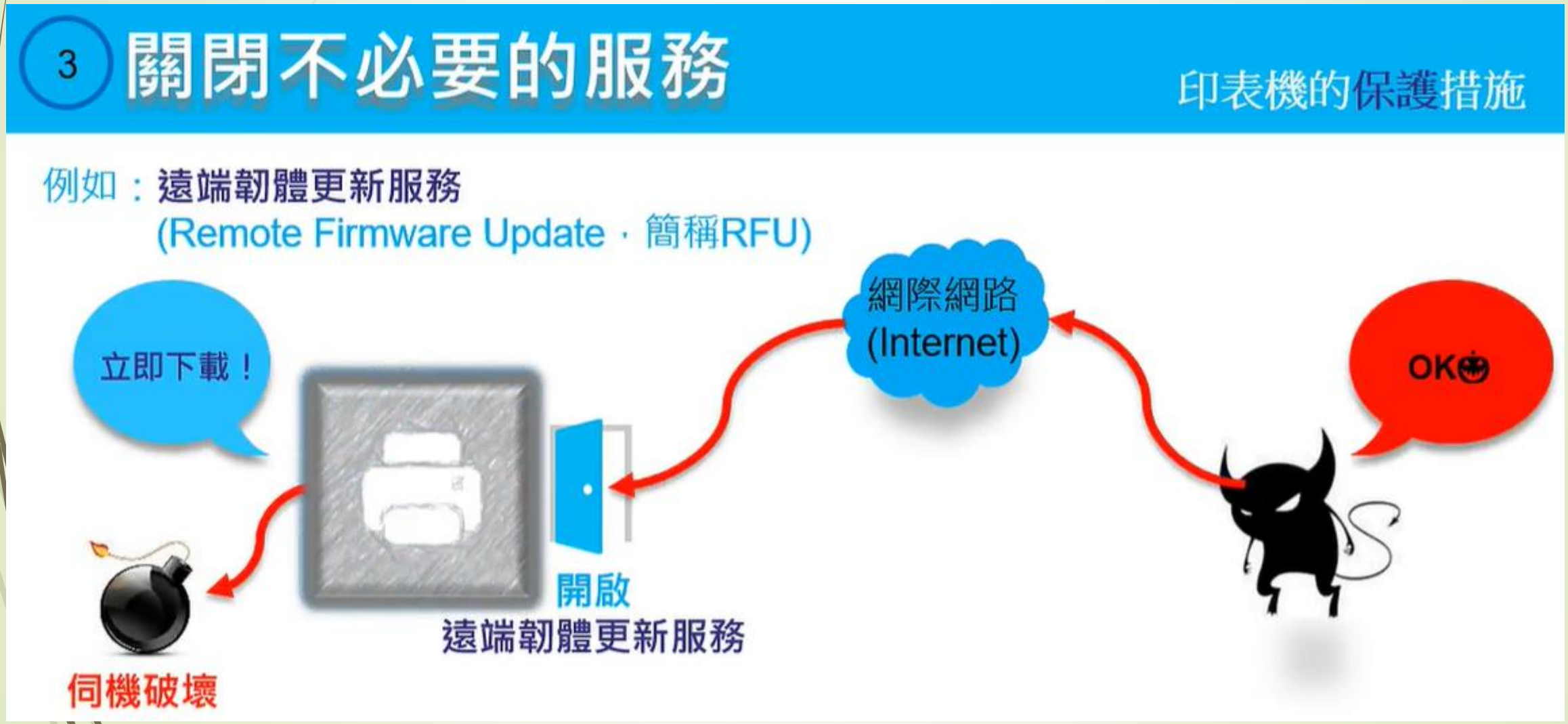
Shift

106)$)&a

2.物聯網安全-網路印表機



2.物聯網安全-網路印表機



2.物聯網安全-網路印表機

3 關閉不必要的服務

印表機的保護措施

- 關閉印表機的**遠端韌體更新服務**
  (Remote Firmware Update，簡稱RFU)
- 關閉其他不必要的預設服務

2.物聯網安全-網路印表機

2.物聯網安全-網路印表機

2.物聯網安全-網路攝影機

網路攝影機(監視器)介紹

1. 每臺網路攝影機皆可視為一臺小型電腦
2. 它們都有自己的IP位址
3. 它們都可以連接到網路中

- 但是安裝網路攝影機時，時常缺乏資訊安全防護處理。

2.物聯網安全-網路攝影機

常見網路攝影機的兩種威脅

1. 遭駭客入侵
   - 隱私權遭受威脅

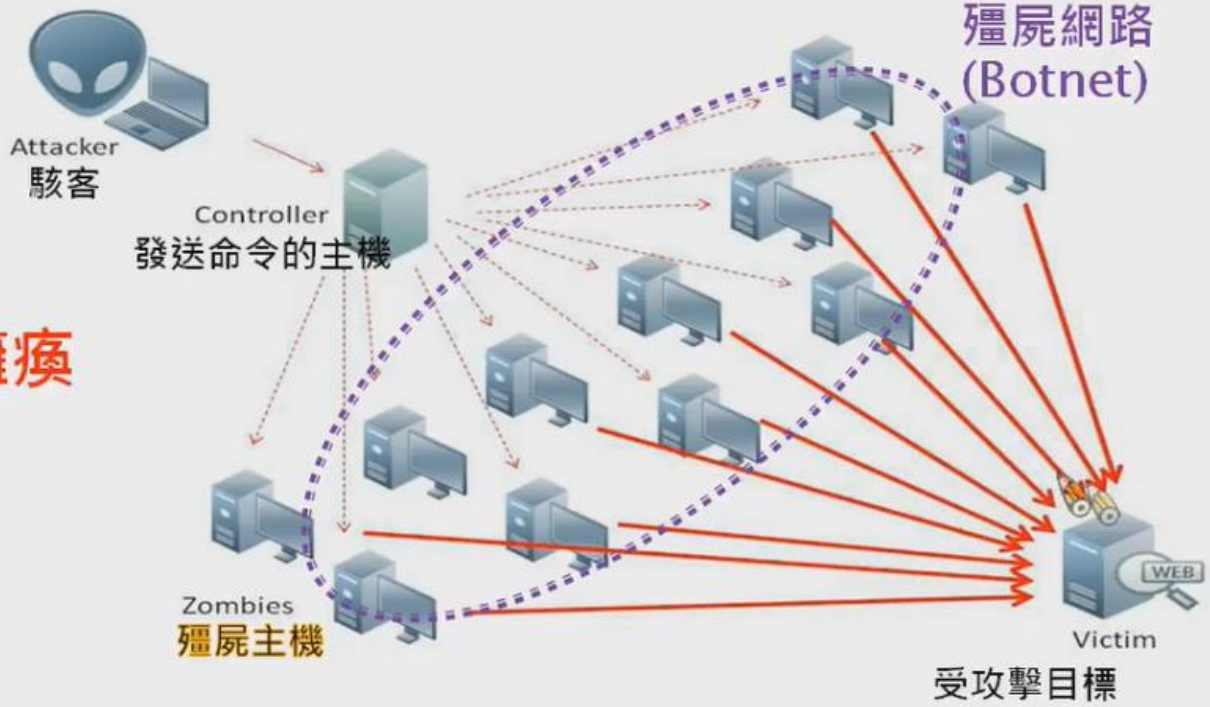
2. 被植入病毒
   - 成為駭客發動攻擊的跳板

2.物聯網安全-網路攝影機

2.被植入病毒

- 成為殭屍主機(Zombies)
- 感染其他網路攝影機
- 形成殭屍網路(Botnet)
- 殭屍網路(Botnet)
  是駭客發動攻擊的跳板

使受攻擊目標網路癱瘓



2.物聯網安全-網路攝影機

參與駭客攻擊的殭屍主機，佔用學校對外所有頻寬

- 導致學校網路無法正常使用

資安監控中心會追查攻擊來源，並作「資安通報」

- 殭屍主機所屬單位會收到資安通報單
- 資安中心很可能會依照資安通報程序，阻斷殭屍主機的IP位址。

2.物聯網安全-網路攝影機

網路攝影機 資訊安全防護建議

1. 關閉不必要之連線服務
2. 限定特定IP位址才能存取攝影機
3. 修改預設帳號密碼
4. 請維護網路攝影機的廠商進行設備軟體、韌體更新，修補漏洞。

3.EVS平台使用說明

- 帳號使用說明
- 網站弱掃申請
- 平台管理

3.EVS平台使用說明

帳號使用說明

初次登入

- 以帳號及密碼登入
- 修改帳戶資料
- 收信驗證後啟用帳號

忘記密碼

- 輸入帳號及初登入所填信箱
- 收信確認還原預設密碼
- 接續「初登入」流程

人員交接

- 現任者登入後，觸發還原預設密碼
- 現任者收信確認還原預設密碼
- 告知接任者帳號及預設密碼
- 接任者操作「初登入」流程

3.EVS平台使用說明

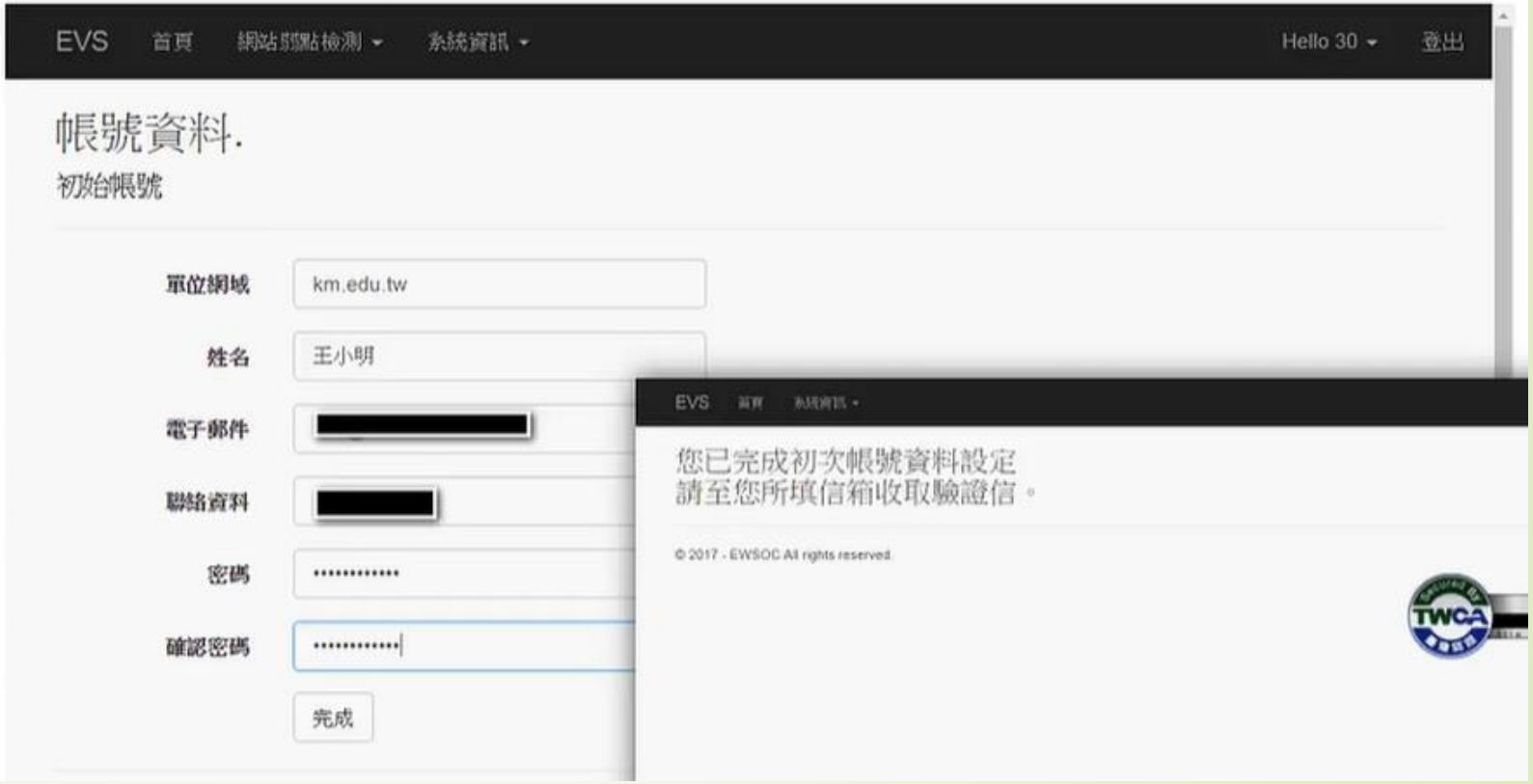
網站弱點掃描流程

3.EVS平台使用說明

網站弱點掃描流程

1.登入
2.新增網站
3.申請掃描
4.查看掃描結果

- 初次登入
- **填寫帳號資料**

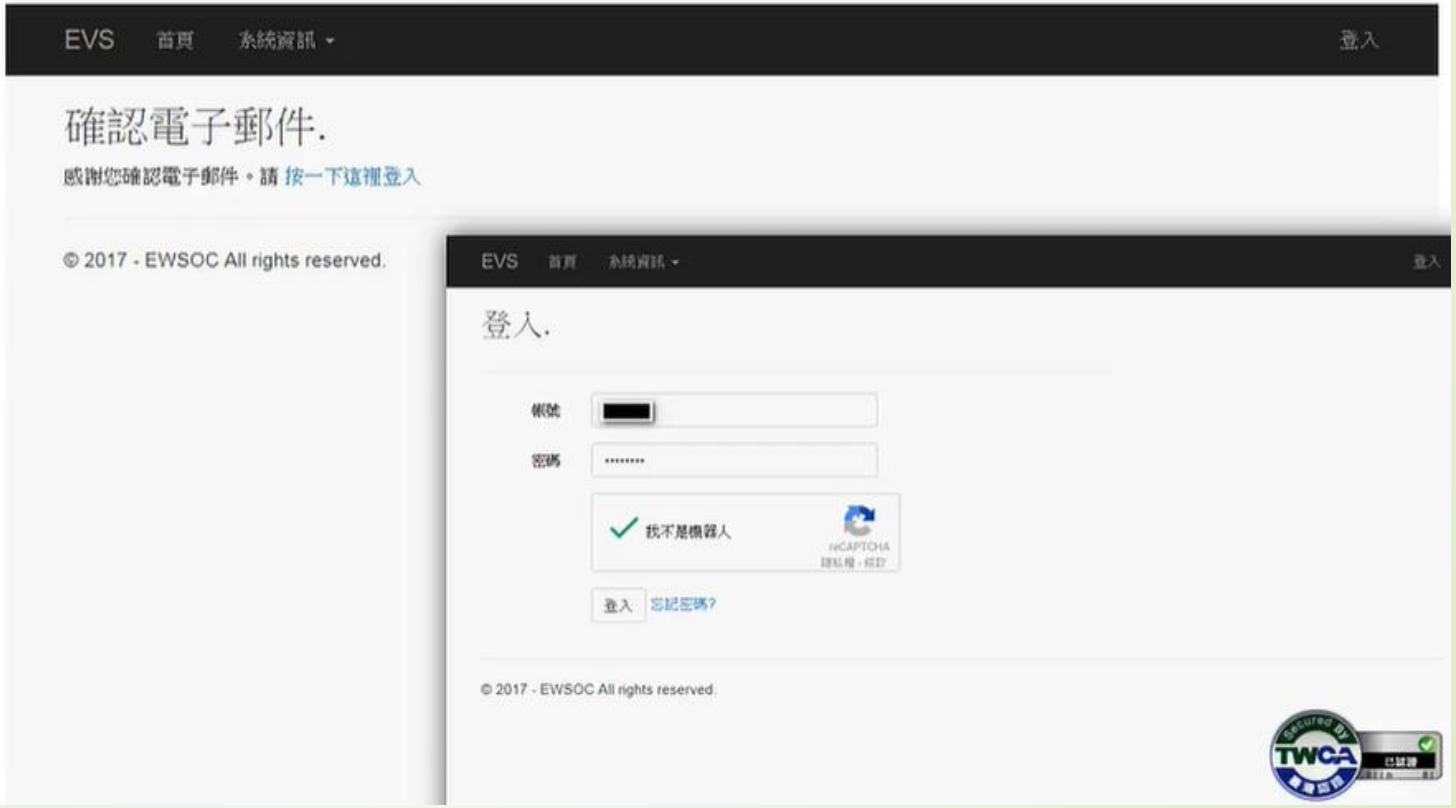


3.EVS平台使用說明

網站弱點掃描流程

1.登入
2.新增網站
3.申請掃描
4.查看掃描結果

- 初次登入
- 填寫帳號資料
- 收驗證信
- **信箱驗證完成，用新密碼登入**



3.EVS平台使用說明

網站弱點掃描流程

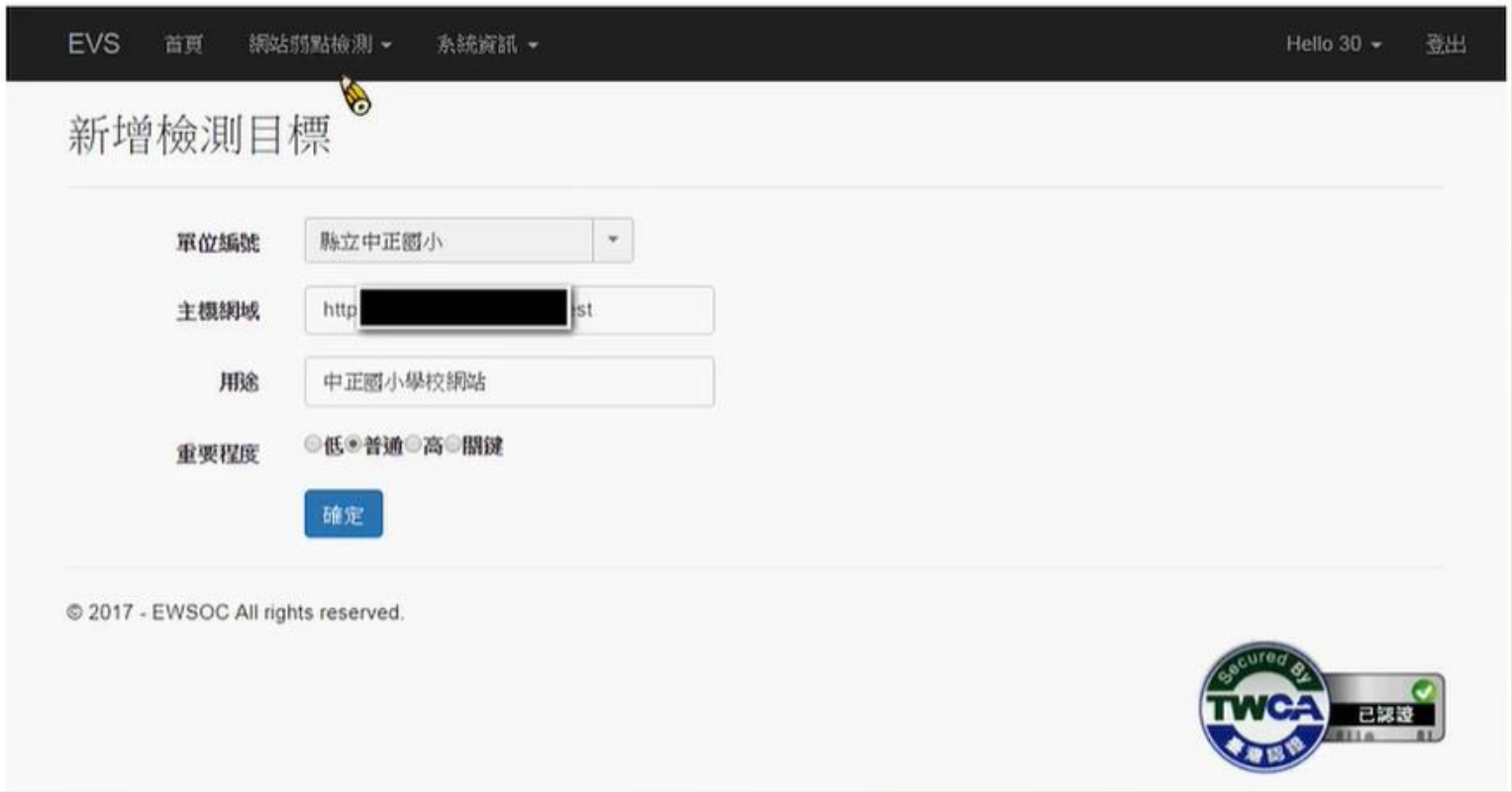
新增/匯入欲執行弱點掃描之網站

3.EVS平台使用說明

網站弱點掃描流程

1.登入
2.新增網站
3.申請掃描
4.查看掃描結果

- **新增單一網站**



3.EVS平台使用說明

網站弱點掃描流程

1.登入
2.新增網站
3.申請掃描
4.查看掃描結果

- 新增單一網站
- **匯入多個網站：**

  網域限制說明

  - 使用網域:
    - 中心單位：依初登入所填網域來新增網站
    - 轄下單位：依轄下單位初登入所填網域；若轄下單位未填網域(如:尚未完成初登入帳號)則依管理者網域驗證
  - 使用IP:僅限區網中心及縣市網中心
    - 若轄下單位欲使用IP需由中心協助以「匯入」方式處理
  - 匯入格式請由系統下載範本填寫後上傳
    - 欄位：單位代碼、主機網域、用途
    - 工作表名稱：檢測目標

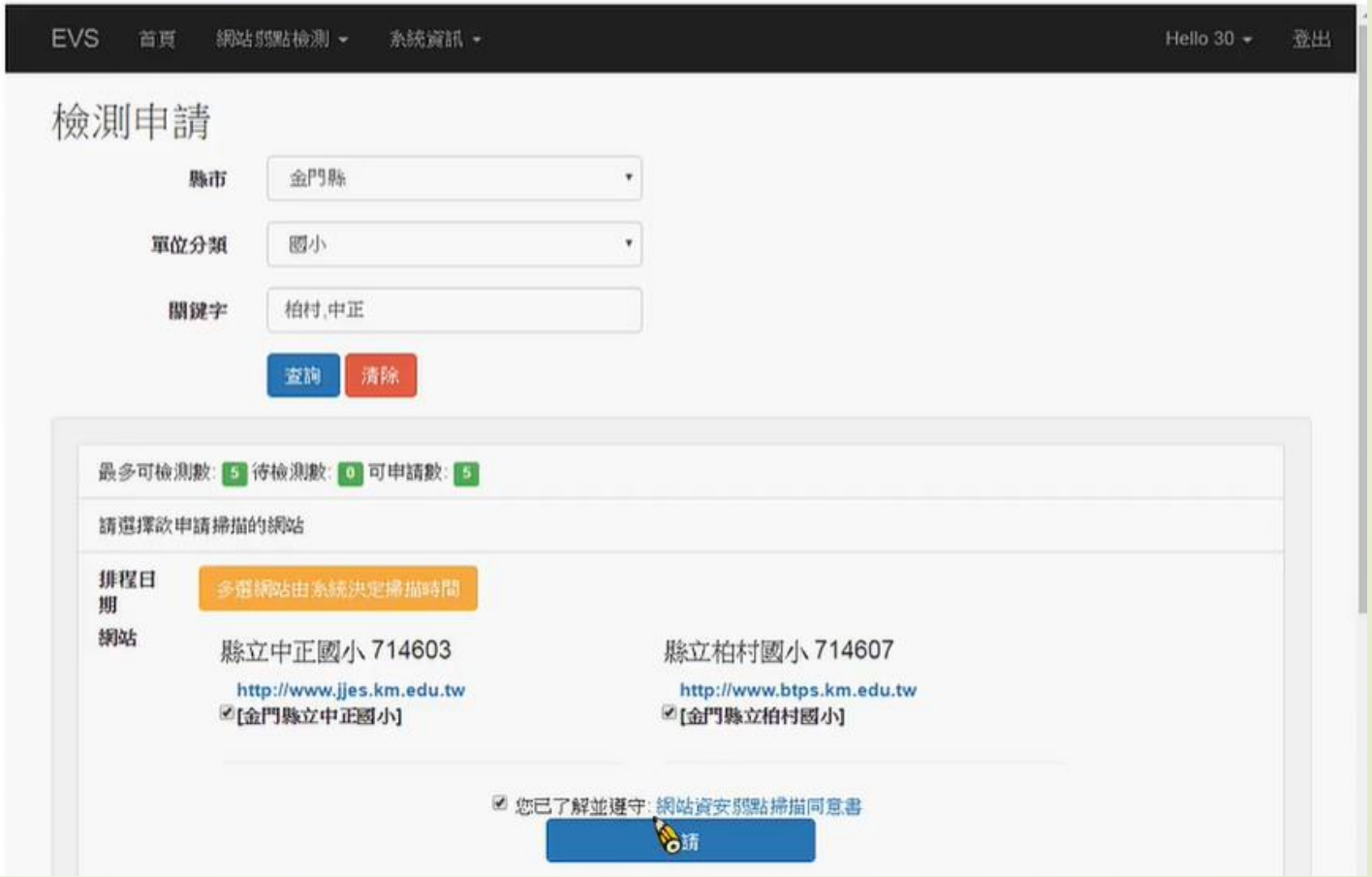
3.EVS平台使用說明

網站弱點掃描流程

網站弱點掃描流程

1. 登入
2. 新增網站
3. **申請掃描**
4. 查看掃描結果

- 申請限制
- 單站申請
- **多站申請**

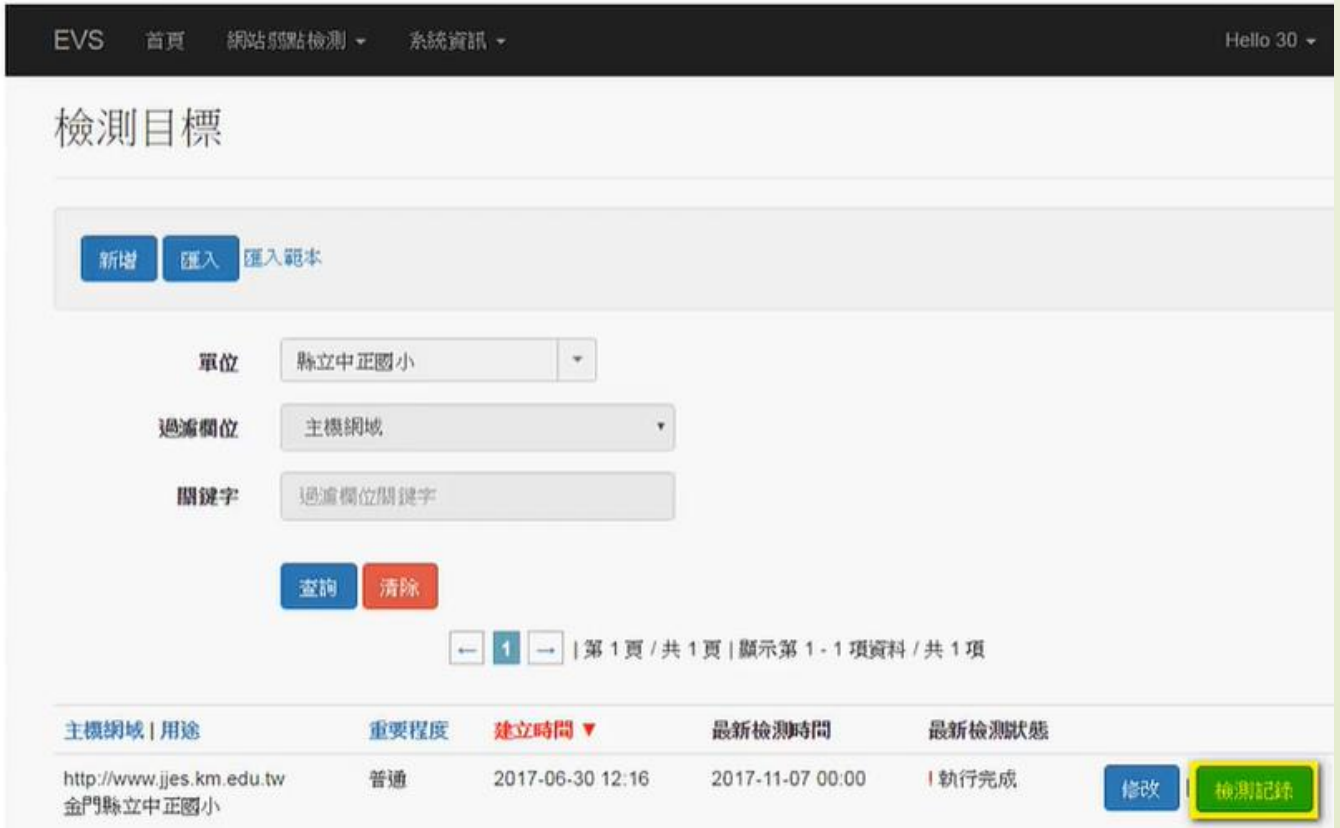


網站弱點掃描流程

網站弱點掃描流程

1.登入
2.新增網站
3.申請掃描
4.查看掃描結果

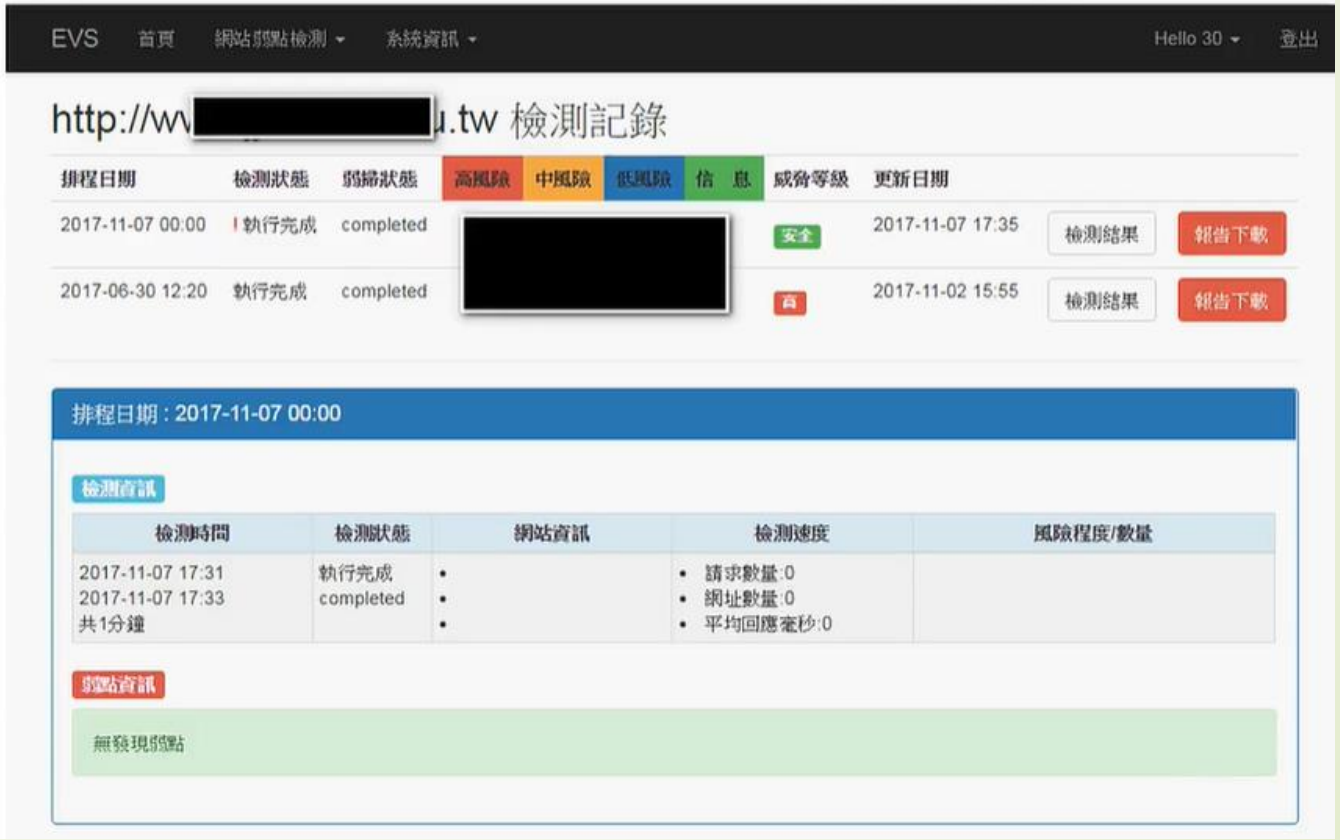
- **查看檢測結果**



網站弱點掃描流程

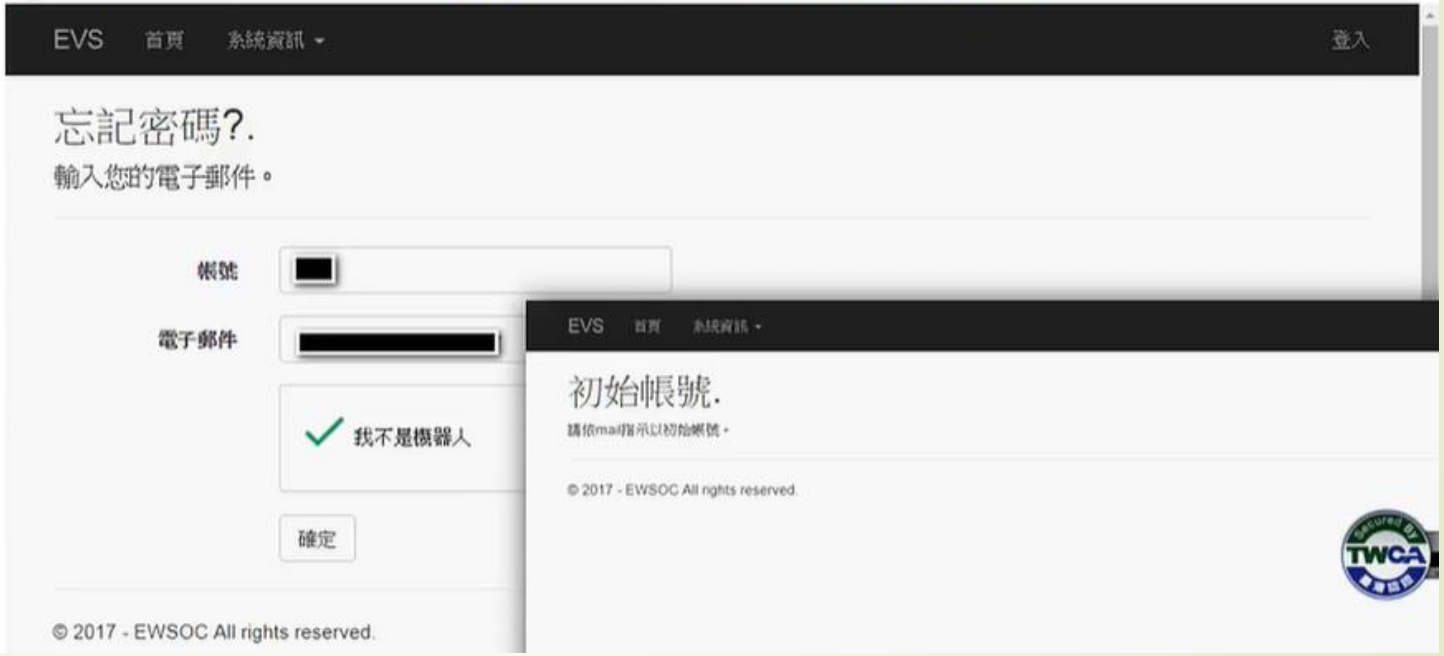
1. 登入
2. 新增網站
3. 申請掃描
4. 查看掃描結果

- 查看檢測結果
- **下載檢測結果**



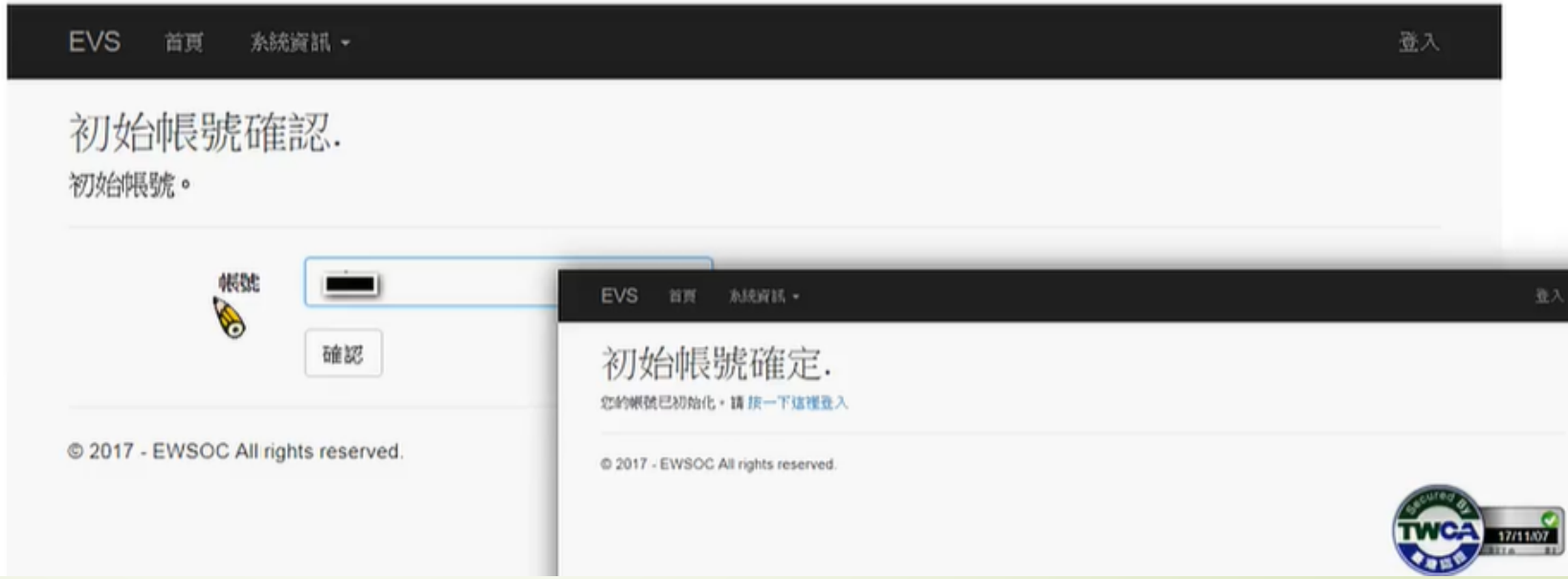
- 忘記密碼
- 人員交接
- 管理帳號
- 轄下單位帳號

1. 點選忘記密碼
2. 輸入帳號及初登入設定的電子郵件
3. 依收到的電子郵件指示，還原帳號預設密碼



- **忘記密碼**
- 人員交接
- 管理帳號
- 轄下單位帳號

1. 點選忘記密碼
2. 輸入帳號及初登入設定的電子郵件
3. 依收到的電子郵件指示，還原帳號預設密碼
4. 收信確認，將密碼還原成預設密碼
5. **輸入帳號，確認還原預設密碼，即可使用預設密碼登入**



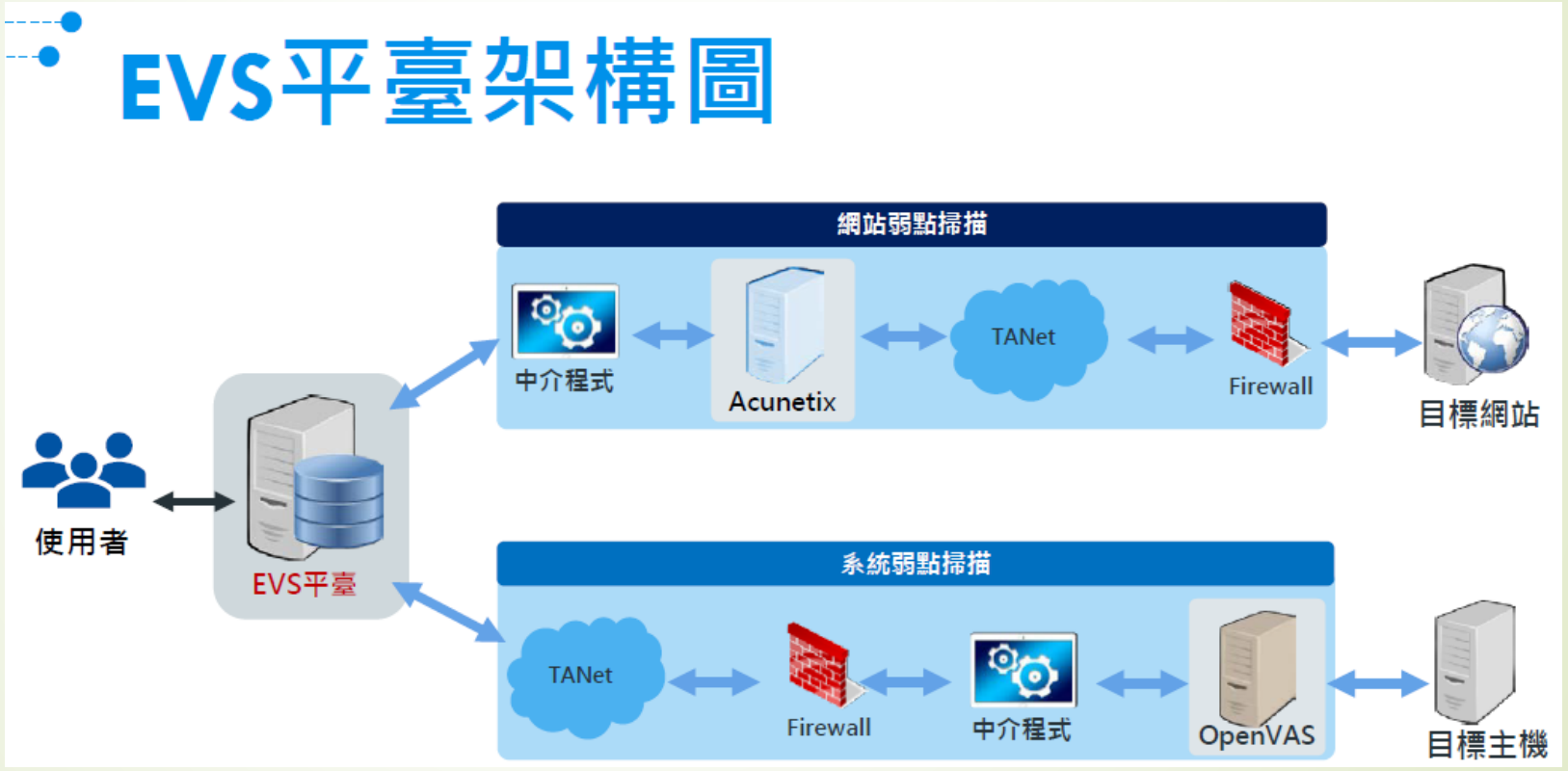
- 忘記密碼
- **人員交接**
- 管理帳號
- 轄下單位帳號

1. 由現任者登入後，點選「初始帳號」
2. 現任者收信確認，將密碼還原成預設密碼
3. **輸入帳號，確認還原預設密碼**
4. **現任者告知接任者帳號及預設密碼**
5. **接任者即可使用預設密碼登入**

- 忘記密碼
- 人員交接
- **管理帳號**
- 轄下單位帳號

若人員未交接時
由**各區網、教網中心協助還原預設密碼**
初始帳號確認信將寄給**中心管理者**
由中心管理者收信確認，將密碼還原成預設密碼
中心管理者告知接任者帳號及預設密碼
接任者即可使用預設密碼登入

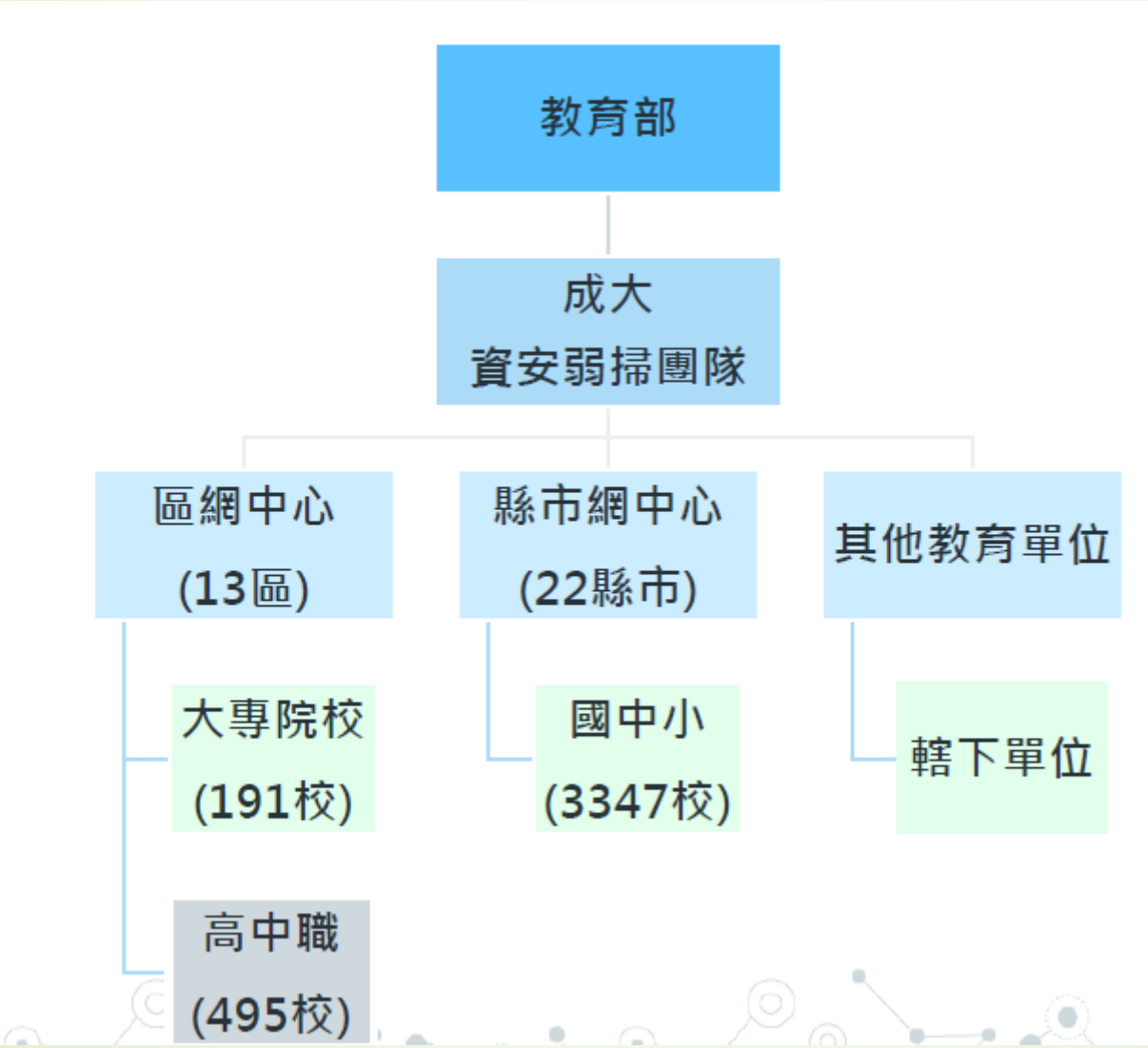
4.教育單位資安弱掃服務說明



EVS平臺弱掃引擎分布及IP

網站弱掃引擎IP白名單

- 163.28.114.9
- 140.116.221.36~39
- 163.28.52.142
- 163.28.84.125


教育部
成大
資安弱掃團隊
區網中心
(13區)
縣市網中心
(22縣市)
其他教育單位
大專院校
(191校)
國中小
(3347校)
轄下單位
高中職
(495校)

110年教育單位Top 10網站弱點

無中高風險網站徽章

- **無中高風險網站**可得到一顆徽章
- 預計於7月份更新
- 登入EVS平臺就可查看得到幾個徽章！
- 可查看各單位獲得了幾個徽章
- 根據最新一筆弱掃資料定期審核

單位	網站	最新檢測						
	網站網址 | 網站名稱 | 建立時間 | 重要程度	排程日期 ▼	狀態	風險				
				高風險	中風險	低風險	信　息	
國立暨南國際大學	網路組網站 2018-01-31 13:47 普通	2021-09-28 00:00	執行完成	0	0	1	5	修改 | 檢測記錄

弱掃時機

- 網站公開上線前
- 開發程式過程中
  可檢視使用的套件是否有弱點
- 職務異動
- 被開立DEF事件單者
- B級單位網站每年執行一次
- C級單位網站每兩年執行一次

弱掃前注意事項

1. **備份**
   弱掃前，請備份網站，因弱掃可能造成資料遺失毀損等狀況。
2. **公告弱掃時間**
   請提前公告弱掃時間，提醒使用者該時段網站服務有可能會中斷。
3. **設定白名單**
   請注意是否有其他資安設備，各資安設備、防火牆皆須開弱掃引擎白名單。
4. 弱掃期間**關閉防毒軟體**。
5. **整理網站目錄**
   弱掃時間最長為7小時，若超過7小時系統會自動中斷掃描，因此建議先整理網站目錄，將不必要的檔案移除(例如備份檔)。

弱掃前注意事項

因弱掃時會快速發送**大量的請求(requests)**
有可能造成網站服務中斷，或資安設備的異常狀況
建議**避免同單位多個網站都集中在同一時段弱掃**

掃描平均費時	51分鐘
網站平均網址數	362個
網站平均回應時間	19毫秒
平均請求數量	**82203個** → 平均每秒發送**31個請求**

申請弱掃注意事項

1. **可同時排程數量**

區縣市網中心：20個

區縣市網中心轄下單位：5個

例：國立彰化高商，需弱掃6個網站

1. 先匯入這6個需弱掃的網站資料
2. 申請排程5個網站
   - http://x1.chsc.chc.edu.tw
   - http://x2.chsc.chc.edu.tw
   - http://x3.chsc.chc.edu.tw
   - http://x4.chsc.chc.edu.tw
   - http://x5.chsc.chc.edu.tw
3. 等第1個網站弱掃完，第6個網站即可申請排程
   - http://x6.chsc.chc.edu.tw

申請弱掃注意事項

2. **可排程日期**

週末、例假日不提供排程

下拉選單未顯示之日期，即表示該時段排程已額滿

3. **暫時取消新授權網站每日申請額度限制**

110年6月起，將暫時取消新授權網站額度限制

各單位可依需求申請網站弱掃

預計於弱掃授權使用過半之後再開始管制

弱掃後常見異常狀況

1. 掃描超過七小時

掃描時間過長，系統自動中斷掃描

弱掃報告仍然有效，建議依報告修補弱點後，再進行複測

弱掃後常見異常狀況

不論執行完成/失敗，只要掃描少於1分鐘，不會產生弱掃報告

1. 掃描時間太短有可能是掃描異常，因此建議排查之可能原因：資安設備阻擋、該網址/IP未開啟Web服務、網路異常...
2. 建議排除上述原因後，來信詢問是否有其他異常，再重新申請掃描

常見Q & A

1. 如何取消排程
   - EVS平臺暫不提供取消排程功能
   - 請2天前來信通知，說明取消原因，由專案人員手動取消。
   - 取消後會email通知

結論

1. 弱點掃描為網站安全最基礎防護
2. 安全只能控制，不能保證
   - 弱點持續被發現
   - 駭客攻擊從不間斷
   - 目前的安全無法保證未來安全
   - 持續不斷進行弱點修正
3. 人員的資訊安全教育不可或缺

資料來源:成大資安弱掃團隊