「您安全嗎?」

預防加密垃圾軟件快速自我檢查表

Speedy Group Corporation Limited

自我評估

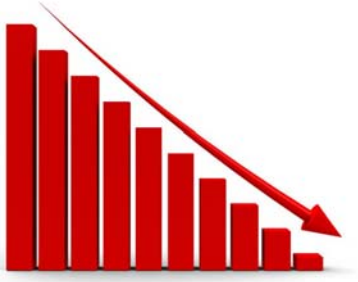
- 快速自我評估分為兩部份：

1. 預訪Ransomware的基本保安設定
2. 不幸中了Ransomware，備份設定能還原完整的資料嗎？

Ransomware 的攻擊途徑

- 主動型
  - 與一般 Hacking 程序無異
  1. 搜尋目標系統上的漏洞(Port Scan)
  2. 取得控制權後，直接執行 Ransomware 惡意程式碼

- 被動型
  - 鈎魚電郵
  - 藏於網頁內的惡意程式碼



保安設定快速檢查

- 使用者電腦及伺服器有没有防毒軟件?
- 使用者電腦及伺服器上的防火牆有沒有開啓?
- Windows Server 2003 或更早期的版本會存在嗎？
- MS Windows 的網域使用者密碼強度有沒有設置?
- 是否清楚有多少 MS Windows 的網域使用者擁有網域管理員權限?
- 是否清楚其他服務供應商有否在 MS Windows 的網域內建立使用者帳號及其權限?
- 已離職的同事帳號有沒有停用?
- 提供網頁服務、電郵服務或 FTP 服務的伺服器是否存在於 DMZ 內?
- 電郵伺服器有沒有過濾功能?
- 開啓了遠端連線功能的伺服器有沒有設定訪問 IP 限制?

自我檢查 (網絡安全設定)

- 實體防火牆上的預設規則
  - 一般的實體防火牆會在公用網絡進入內聯網(WAN -> LAN)的設定上，在最後的規則預設了拒絕所有的訪問，但不會顯示出來

自我檢查(網絡安全設定)

- NMAP port scan
- nmap.exe -Pn --top-port 20 <x.x.x.start>-<end>
  - Example: nmap.exe -Pn --top-port 20 192.168.0.1-254

```
Nmap scan report for 192.168.0.65
Host is up (0.054s latency).
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   open     domain
80/tcp   filtered http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  open     msrpc
```

```
139/tcp  open     netbios-ssn
143/tcp  filtered imap
443/tcp  open     https
445/tcp  open     microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp open     ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy
```

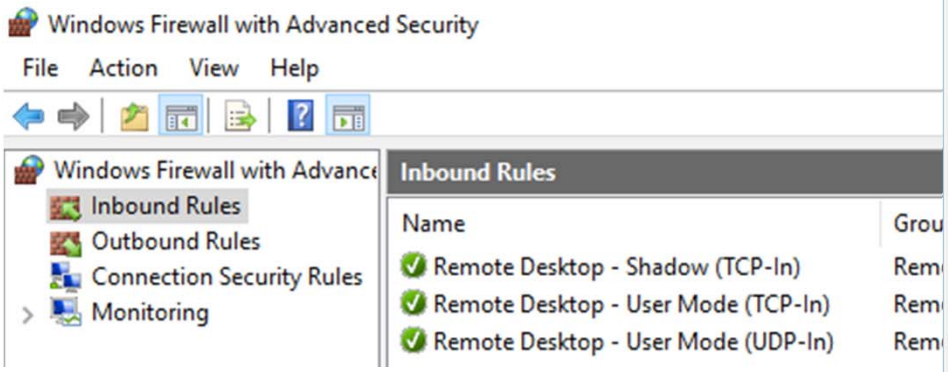
自我檢查(網絡安全設定)

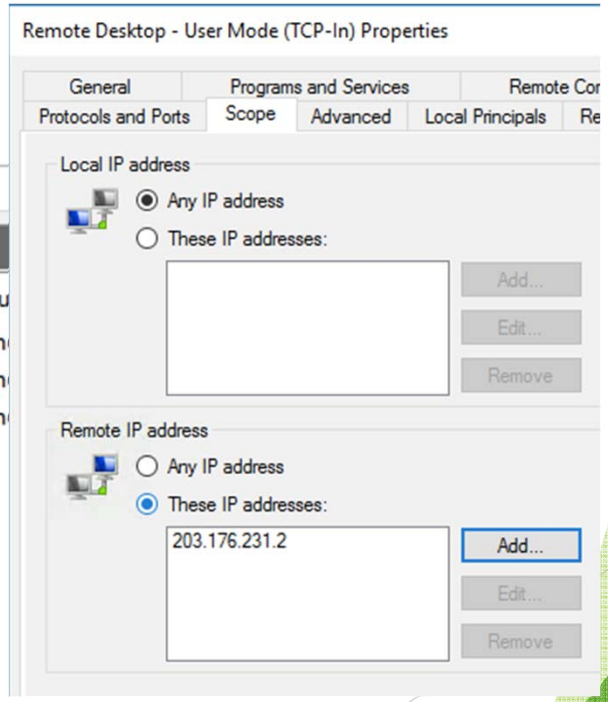
- 檢查一
  - 用任一真 IP 地址掃描屬於學校的真 IP 範圍
- 檢查二
  - 用校內任一使用者電腦掃描校內 IP 範圍
- 檢查三
  - 如有DMZ，把手提電腦連至DMZ，掃描校內 IP 範圍
  - 如顯示遠端連線或檔案共用連線能夠連接校內電腦，即防火牆設定有問題

- 如WiFi900的設定有把老師的無線網路與 ITED 打通，也應該用學生及來賓的無線網路來掃描 ITED 的網絡

自我檢查(網絡安全設定)

- Windows 伺服器上的遠端桌面連線防火牆設定
  - 要設定訪問IP地址

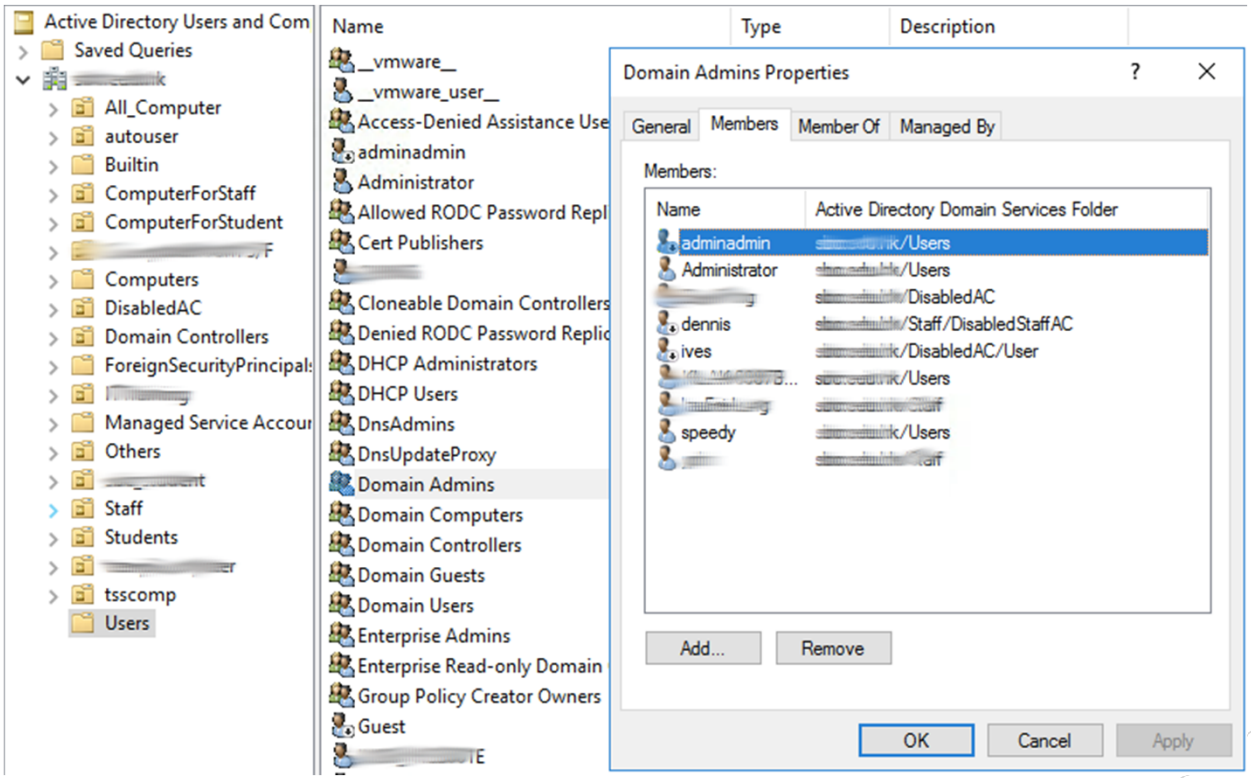




其他 OS 平台的遠端管理
如 ssh
也要有類似的設定

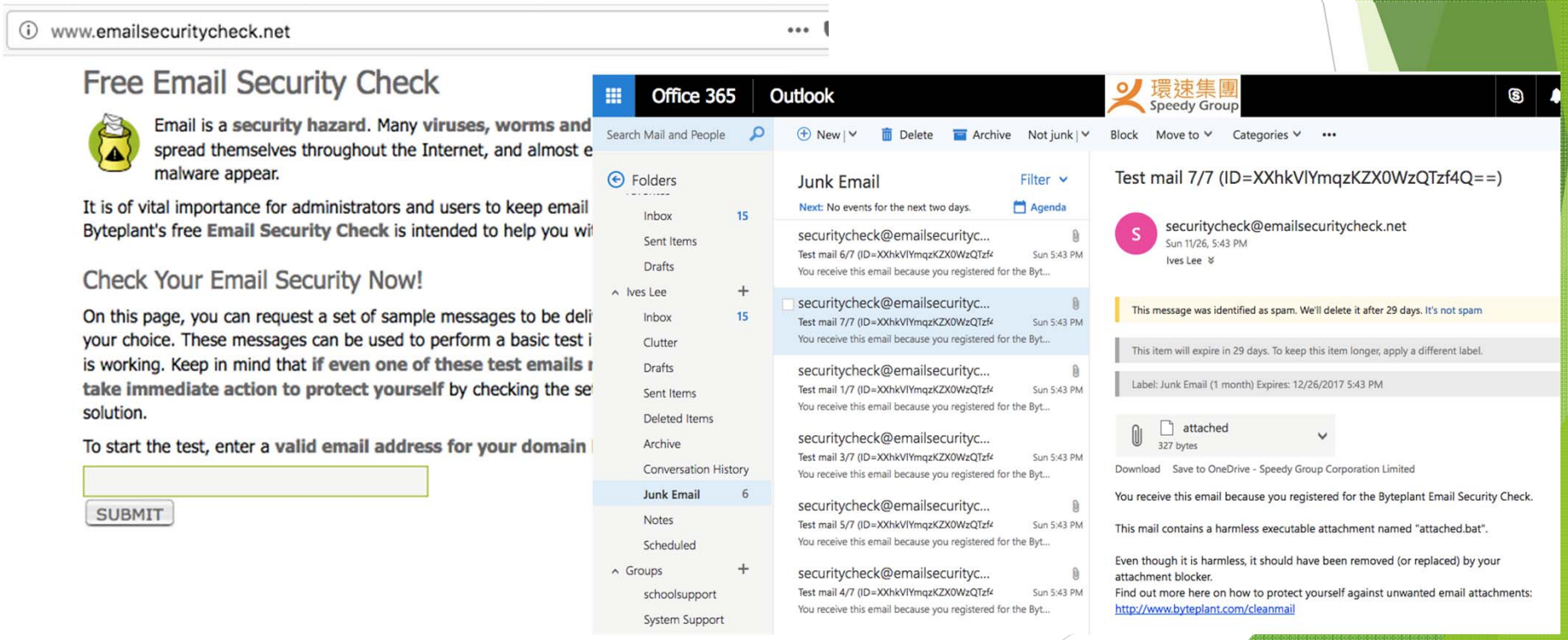
自我檢查(網絡安全設定)

- 要清楚知道有多少人擁有網域管理員權限



自我檢查(網絡安全設定)

- 檢查電郵保安能力 (http://www.emailsecuritycheck.net)

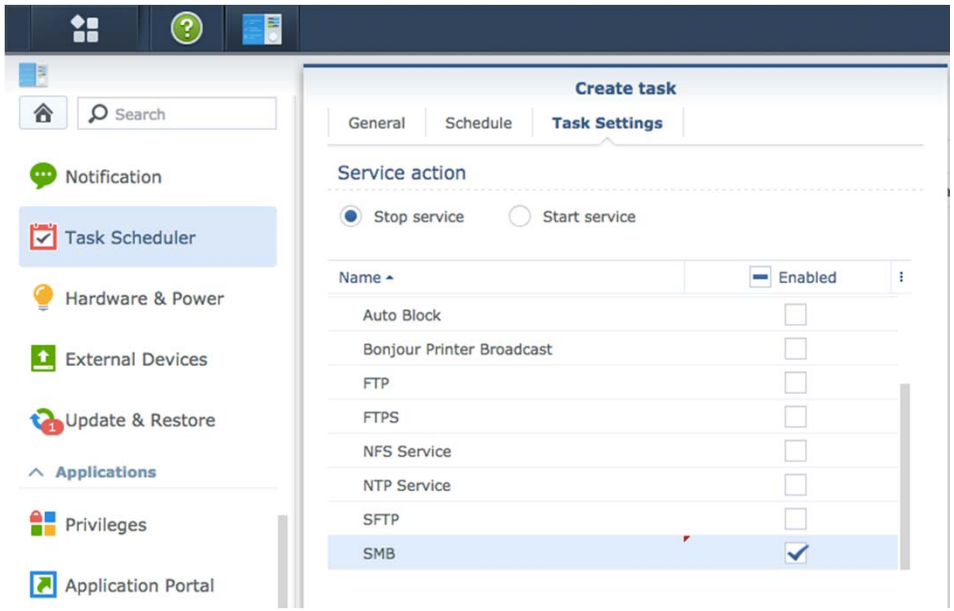


備份設定快速檢查

- 有沒有多過一份以星期為基數的備份 (Weekly Backup)
- 有沒有映象備份(Image Backup)
- 有沒有檔案備份(File Backup)
- 有沒有離線備份 (Offline Backup)
- 有沒有遠端備份 (Offsite Backup)
- 有沒有多過一個的本地儲存備份裝置
- 有沒有檢查最近一次備份是否成功

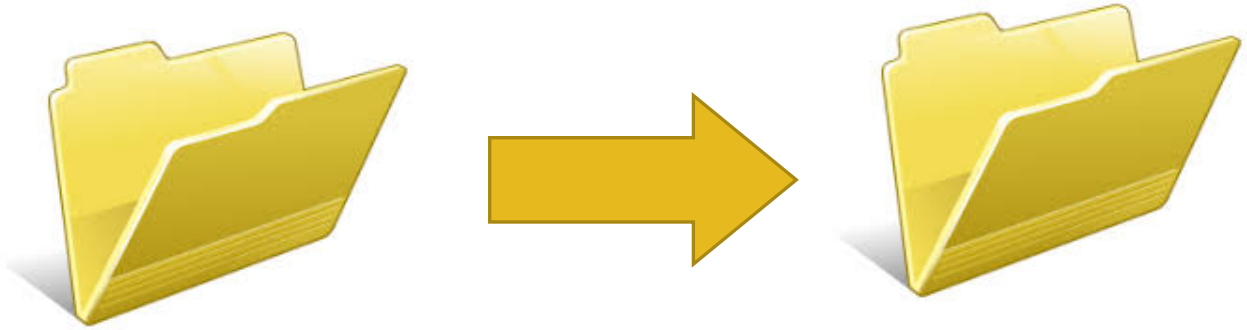
備份設定的建議

- 最少要有兩份 Weekly Backup
- 這兩份 Weekly Backup 各自儲存在不同的備份裝置
- 備份裝置最好能夠設定排程，能加入定時開啓/停用檔案共用服務，達到離線備份的效果



有了映像備份，為何需要檔案備份？

- 檔案備份的定義就像 Copy & Paste，不作任何壓縮處理或打包成一個映像檔
- 映像備份還原須要多少時間取決於有多少資料要還原
- 進行映像備份還原中途，可提供暫時的投產環境
- 如有映像備份，建議使用檔案備份去保存近一個月有更改的資料



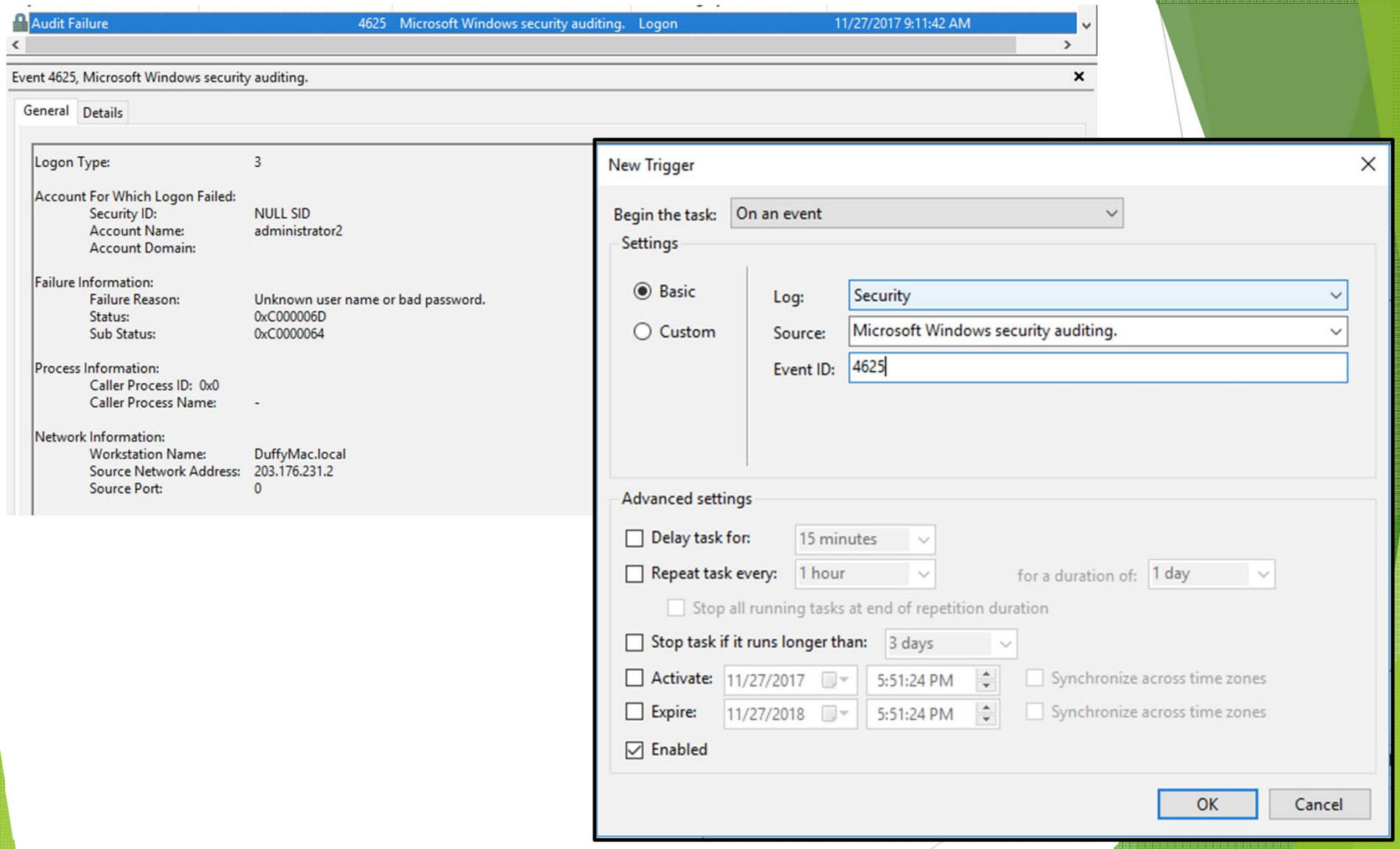
遠端存取的進階保安設定

- 使用VPN: PPTP, L2TP over IPSEC, SSLVPN
- PPTP
  - 不建議使用，不安全
  - 上YouTube 找找便知道
- L2TP over IPSEC
  - 安全
  - 設置比SSLVPN難小小
- SSLVPN
  - 安全，容易設置
  - 普遍要買SSLVPN授權

不論那種VPN，
如你的使用者帳號及
密碼過於簡單，
比駭客撞中了或截取到，
就等如駭客可在
學校的網絡內橫行

遠端存取的進階保安設定

- Password Failure Detection
- 嘗試登入系統數次失敗後，封鎖其IP
- 有免費軟件在 Linux/Unix 系統上提供這服務
- Windows Server 有 password lockout policy，不過這是鎖帳號
- 如要在 Windows Server 有封鎖IP的效果，要自行寫Power Shell Coding，流程大概如下:
  1. 監察 Security log event id 4625 (每一分鐘監察一次)
  2. 當event id 4625 出現，從紀錄檔的內容抽取IP地址，把IP地址寫進文字檔
  3. 每五分鍾分析一次文字檔內的IP地址，出現多過特定數目便把它加進防火牆
  4. 每15分鍾清除一次文字檔


Audit Failure 4625 Microsoft Windows security auditing. Logon 11/27/2017 9:11:42 AM
Event 4625, Microsoft Windows security auditing.
General Details
Logon Type: 3
Account For Which Logon Failed:
Security ID: NULL SID
Account Name: administrator2
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC0000064
Process Information:
Caller Process ID: 0x0
Caller Process Name: -
Network Information:
Workstation Name: DuffyMac.local
Source Network Address: 203.176.231.2
Source Port: 0
New Trigger
Begin the task: On an event
Settings
Basic
Custom
Log: Security
Source: Microsoft Windows security auditing.
Event ID: 4625
Advanced settings
Delay task for: 15 minutes
Repeat task every: 1 hour
for a duration of: 1 day
Stop all running tasks at end of repetition duration
Stop task if it runs longer than: 3 days
Activate: 11/27/2017 5:51:24 PM
Synchronize across time zones
Expire: 11/27/2018 5:51:24 PM
Synchronize across time zones
Enabled
OK
Cancel