|  |
| --- |
|  |
| GCB 檢測程式說明文件 |
|  |
|  |
| **Peter Hsieh** |
|  |

# 修改紀錄

* 2020/3/3
  1. 新增arg.txt用法
  2. 附錄-2 py檔案轉換執行檔(exe)步驟

1. 前言

政府組態基準(Government Configuration Baseline, 以下簡稱GCB)目的在於規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。而相關設備之組態設定檔案(configuration)內容龐雜，如果以人工檢查方式進行比對勢必發生檢查錯誤或漏查之情事，且效率低落，為了改善以上情形，本公司著手開發GCB parser程式，可讀入設備組態設定檔案後自動輸出對每條GCB規範的檢測結果，例如「正確設定」，「錯誤設定」或「尚未設定」，快速提供檢查人員參考。

1. 執行環境

GCB parser程式由Python3語言開發，請至官方網站下載安裝Python3環境

<https://www.python.org/downloads/>

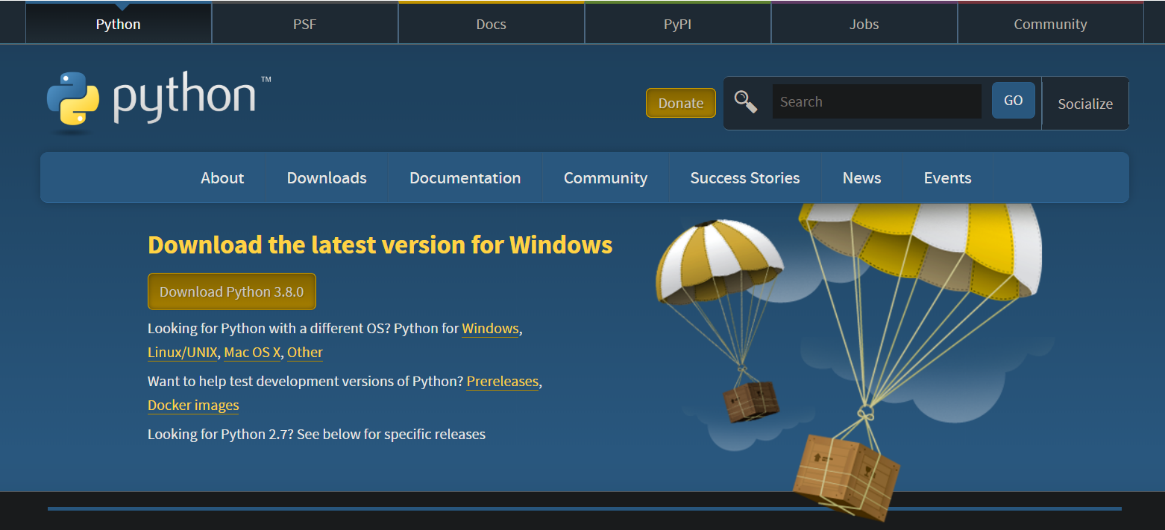
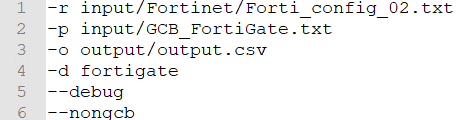


Figure ：Python3下載網站

1. 程式運作流程

檢測程式GCB\_parser.py讀取檔案「arg.txt」內的參數，程式依照參數內容運作。arg.txt範例如下：

參數說明如下：

|  |  |
| --- | --- |
| **參數** | **說明** |
| -r | 設備組態檔案路徑 |
| -p | GCB規則檔案路徑 |
| -o | 輸出檔案路徑 |
| -d | 設備類型 |
| --debug | 進入debug模式，產生更多輔助訊息 |
| --nongcb | 依照自訂語法進行檢測(開發中) |

運作流程如Figure 2：程式接收1個輸入檔：arg.txt參數檔，並產生輸出結果

Figure ：程式運作流程

參數檔

(arg.txt)

輸出結果

(-o指定)

**檢測程式**

**GCB\_parser.py**

以下詳細說明檢測程式所需要之檔案

1. **設備組態檔(-r)**

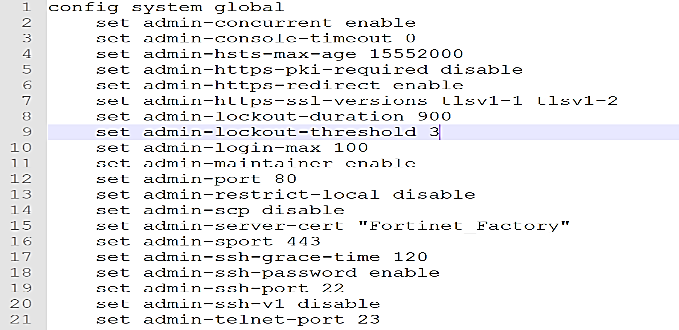
設備組態檔乃由設備內直接取出之configuration檔案，檔案第一行應為組態設定之第一行，其餘無關內容請刪除後再輸入檢測程式。

Figure ：設備組態檔範例

1. **GCB規則檔案(-p)**

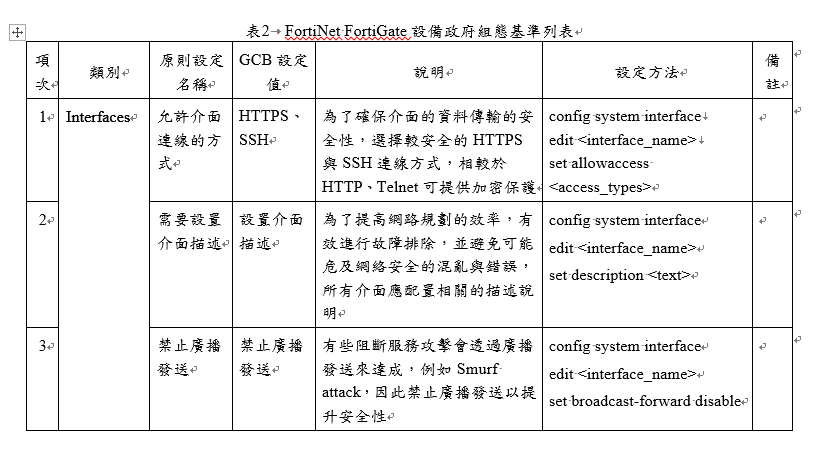
此檔案將GCB規範轉化為程式可讀規則格式，GCB規範可參考技服中心所頒佈文件，範例為Figure 4

Figure : GCB規範範例

第一條規範為

*config system interface，edit <interface\_name>，set allowaccess <access\_types>*，

箭頭括號(<>)內可為任意文字，但不可空白，此規範轉化以下規則

*config system interface，edit <interface\_name>，set allowaccess <access\_types>****，***

檢測程式方可讀取規則後進行檢測。

再以第三條規範為例：

*config system interface，edit <interface\_name>，set broadcast-forward disable*

，此規範重點為必須設定disable，若為其他設定(例如enable)均視為錯誤設定，所以在規則內需以引號(“)設定，故第三條規則應為：

*config system interface，edit <interface\_name>，set broadcast-forward “disable”*

若遇到對設定值有上下限要求的GCB規範(例如GCB12)，則其規則應該以箭頭括號表示，例如GCB12「set min-number 1」的1應該是最低值，非固定值，也就是只要是大於1的值均為正確設定，所以規則應設為「set min-number <number>」，代表number非固定值，至於該值是否大於1，程式會自行判斷，檢測人員無需設定。

下表為規範與規則之對照表節錄：

|  |  |  |
| --- | --- | --- |
| **項次** | **規範** | **規則** |
| GCB 1 | config system interface  edit <interface\_name>  set allowaccess <access\_types> | config system interface  edit <interface\_name>  set allowaccess <access\_types> |
| GCB 3 | config system interface  edit <interface\_name>  set broadcast-forward disable | config system interface  edit <interface\_name>  set broadcast-forward “disable” |
| GCB12 | config system password-policy  set min-number 1 | config system password-policy  set min-number <number> |

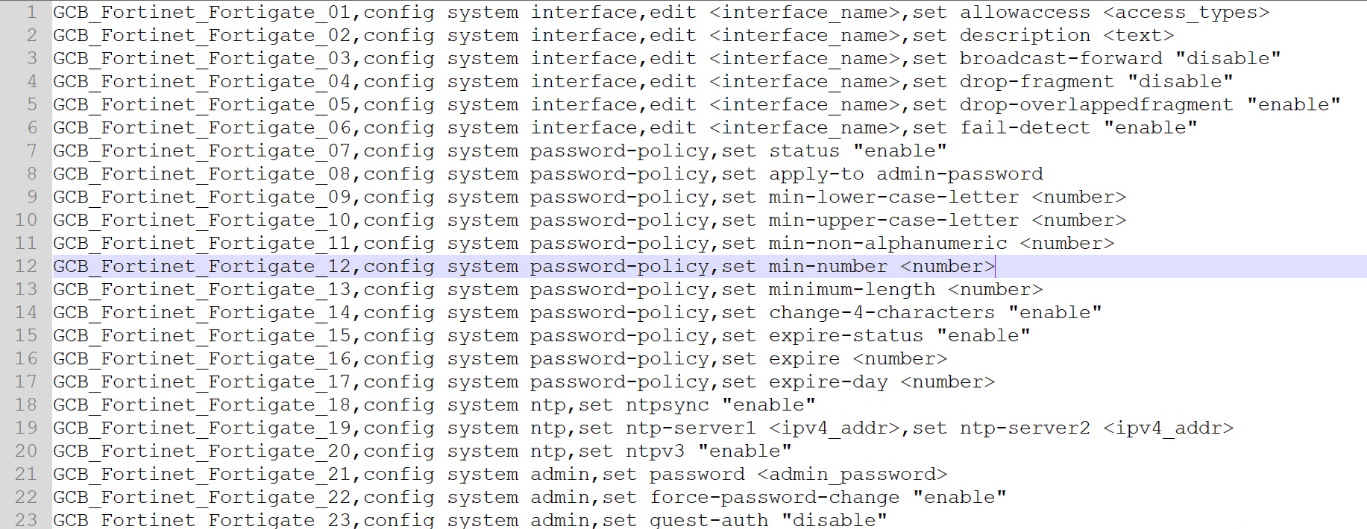
GCB規則檔案內記錄由GCB規範所轉化的規則，每一行分為2部分，前半部為GCB編號，後半部為該規範之轉化規則

Figure ：GCB規則檔案

|  |  |  |
| --- | --- | --- |
|  | **規則前半** | **規則後半部** |
| **說明** | GCB之編號，格式為  GCB\_[廠牌]\_[型號]\_[編號] | 對組態之要求 |
| **範例** | GCB\_Fortinet\_Fortigate\_18 | config system ntp,set ntpsync "enable" |

1. **輸出結果(-o)**

輸出結果檔案記錄檢測結果，每行記錄規則之編號，組態內設定與檢測結果。以GCB 1規則為例，若set allowaccess之協定出現http或telnet等明碼協定則為錯誤設定，因此Figure 6第2行的檢測結果為錯誤設定。另外GCB 2要求set description之後不可為空字串，所以第10行為錯誤設定。

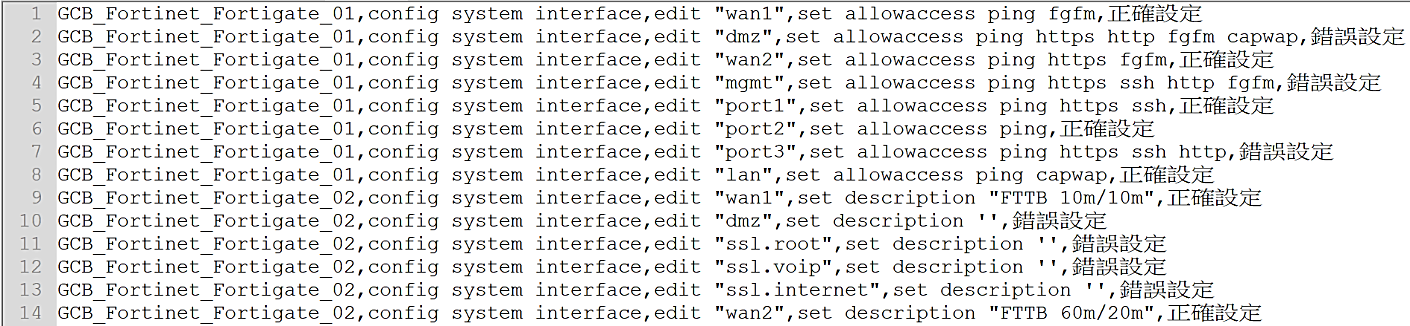
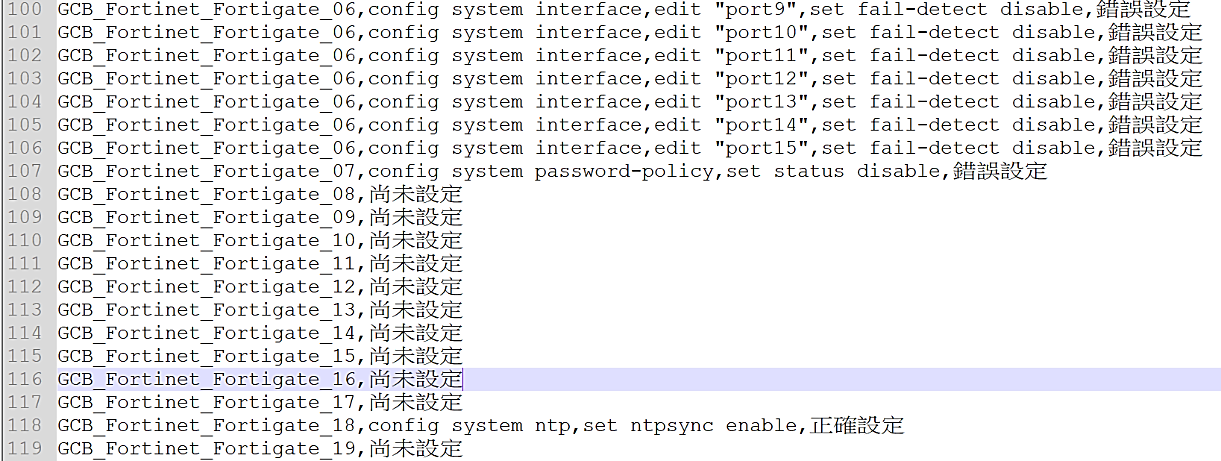
另外，需額外考慮GCB規範要求設定，但組態檔案中卻未出現之情形，例如Figure 7第108行為例，組態檔案內沒有符合GCB 8(config system password-policy,set apply-to admin-password)的設定，因此顯示結果為尚未設定。設備管理員可據此進行正確設定。

Figure 輸出結果

Figure : 輸出結果-含尚未設定

附錄-1 GCB規範規則對照表

|  |  |  |
| --- | --- | --- |
| **項次** | **規範** | **規則** |
| **GCB 1** | config system interface  edit <interface\_name>  set allowaccess <access\_types> | config system interface  edit <interface\_name>  set allowaccess <access\_types> |
| **GCB 2** | config system interface  edit <interface\_name>  set description <text> | config system interface  edit <interface\_name>  set description <text> |
| **GCB 3** | config system interface  edit <interface\_name>  set broadcast-forward disable | config system interface  edit <interface\_name>  set broadcast-forward “disable” |
| **GCB 4** | config system interface  edit <interface\_name>  set drop-fragment enable | config system interface  edit <interface\_name>  set drop-fragment "disable" |
| **GCB 5** | config system interface  edit <interface\_name>  set drop-overlappedfragment enable | config system interface  edit <interface\_name>  set drop-overlappedfragment "enable" |
| **GCB 6** | config system interface  edit <interface\_name>  set fail-detect enable | config system interface  edit <interface\_name>  set fail-detect "enable" |
| **GCB 7** | config system password-policy  set status enable | config system password-policy  set status "enable" |
| **GCB 8** | config system password-policy  set apply-to admin-password | config system password-policy  set apply-to admin-password |
| **GCB 9** | config system password-policy  set min-lower-case-letter 1 | config system password-policy  set min-lower-case-letter <number> |
| **GCB 10** | config system password-policy  set min-upper-case-letter 1 | config system password-policy  set min-upper-case-letter <number> |
| **GCB 11** | config system password-policy  set min-non-alphanumeric 1 | config system password-policy  set min-non-alphanumeric <number> |
| **GCB 12** | config system password-policy  set min-number 1 | config system password-policy  set min-number <number> |
| **GCB 13** | config system password-policy  set minimum-length 12 | config system password-policy  set minimum-length <number> |
| **GCB 14** | config system password-policy  set change-4-characters enable | config system password-policy  set change-4-characters "enable" |
| **GCB 15** | config system password-policy  set expire-status enable | config system password-policy  set expire-status "enable" |
| **GCB 16** | config system password-policy  set expire 90 | config system password-policy  set expire <number> |
| **GCB 17** | config system password-policy  set expire-day 14 | config system password-policy  set expire-day <number> |
| **GCB 18** | config system ntp  set ntpsync enable | config system ntp  set ntpsync "enable" |
| **GCB 19** | config system ntp  set ntp-server1 <ipv4\_addr>  set ntp-server2 <ipv4\_addr> | config system ntp  set ntp-server1 <ipv4\_addr>  set ntp-server2 <ipv4\_addr> |
| **GCB 20** | config system ntp  set ntpv3 enable | config system ntp  set ntpv3 "enable" |
| **GCB 21** | config system admin  set password <admin\_password> | config system admin  set password <admin\_password> |
| **GCB 22** | config system admin  set force-password-change enable | config system admin  set force-password-change "enable" |
| **GCB 23** | config system admin  set guest-auth disable | config system admin  set guest-auth "disable" |
| **GCB 24** | config system admin  set allow-remove-adminsession disable | config system admin  set allow-remove-adminsession "disable" |
| **GCB 25** | config system auto-install  set auto-install-config disable | config system auto-install  set auto-install-config "disable" |
| **GCB 26** | config system auto-install  set auto-install-image enable disable | config system auto-install  set auto-install-image "disable" |
| **GCB 27** | config system global  set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2 | config system global  set admin-https-ssl-versions <tlsv1-0 tlsv1-1 tlsv1-2> |
| **GCB 28** | config system global  set admin-https-redirect enable | config system global  set admin-https-redirect "enable" |
| **GCB 29** | config system global  set admin-lockout-threshold 3 | config system global  set admin-lockout-threshold <number> |
| **GCB 30** | config system global  set admin-lockout-duration 900 | config system global  set admin-lockout-duration <number> |
| **GCB 31** | config system global  set hostname <unithostname> | config system global  set hostname <unithostname> |
| **GCB 32** | config system global  set fds-statistics disable | config system global  set fds-statistics "disable" |
| **GCB 33** | config system global  set admin-ssh-grace-time 900 | config system global  set admin-ssh-grace-time <number> |
| **GCB 34** | config system global  set admin-login-max 1 | config system global  set admin-login-max <number> |
| **GCB 35** | config system global  set admin-reset-button disable | config system global  set admin-reset-button "disable" |
| **GCB 36** | config system global  set cfg-save manual | config system global  set cfg-save manual |
| **GCB 37** | config system snmp user  edit <username>  set set security-level auth-priv | config system snmp user  edit <username>  set set security-level auth-priv |
| **GCB 38** | config system snmp user  edit <username>  set priv-proto aes256 | config system snmp user  edit <username>  set priv-proto aes256 |
| **GCB 39** | config system snmp user  edit <username>  set auth-proto sha | config system snmp user  edit <username>  set auth-proto sha |
| **GCB 40** | config system snmp user  edit <username>  set query-port <port\_int> | config system snmp user  edit <username>  set query-port <port\_int> |
| **GCB 41** | config system snmp community  edit <index Num>  set name <community\_name> | config system snmp community  edit <index Num>  set name <community\_name> |
| **GCB 42** | config system snmp community  set query-v1-status disable | config system snmp community  set query-v1-status "disable" |
| **GCB 43** | config system snmp community  edit <index Num>  set query-v1-prot <port num> | config system snmp community  edit <index Num>  set query-v1-prot <port num> |
| **GCB 44** | config system snmp community  set query-v2c-status disable | config system snmp community  set query-v2c-status "disable" |
| **GCB 45** | config system snmp community  edit <index Num>  set query-v2c-prot <port num> | config system snmp community  edit <index Num>  set query-v2c-prot <port num> |
| **GCB 46** | config log setting  set log-invalid-packet enable | config log setting  set log-invalid-packet "enable" |
| **GCB 47** | config log setting  set user-anonymize disable | config log setting  set user-anonymize "disable" |

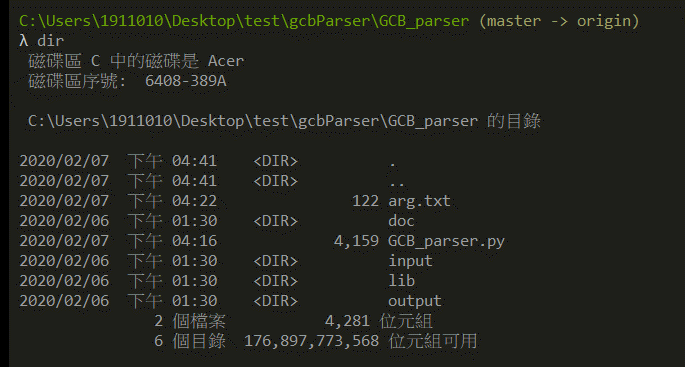
附錄-2 py檔案轉換執行檔(exe)步驟

當檢測程式缺乏Python原始碼(\*.py)執行環境且檢測環境作業系統為Windows時，需要以下步驟將Python原始碼轉換為執行檔(.exe)，轉換完畢後直接執行該執行檔便可執行檢測作業。

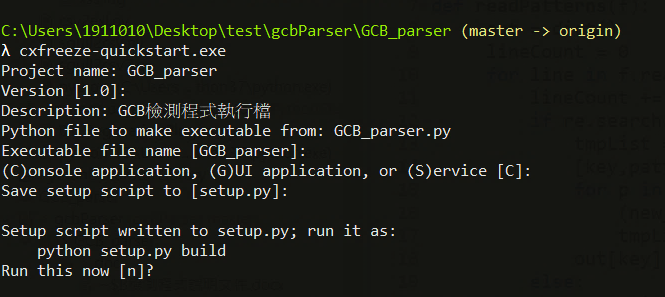
* 安裝[cx\_freeze](https://anthony-tuininga.github.io/cx_Freeze/)工具

python -m pip install cx\_Freeze --upgrade

* 命令列視窗切換至python程式所在資料夾，資料夾中至少應包含欲轉換的python程式與相關函式庫，例如以下的「**GCB\_parser.py**」程式與「**lib**」資料夾



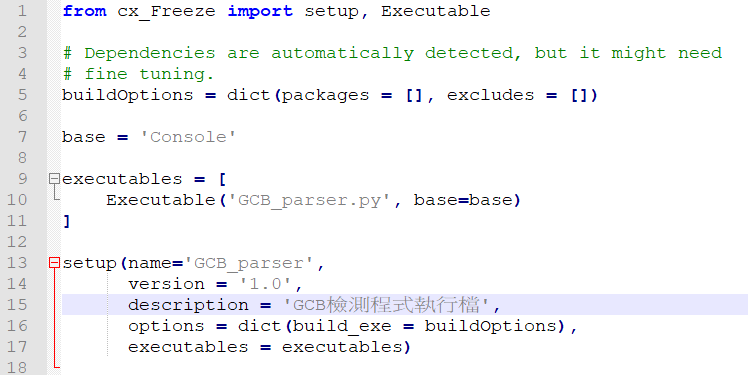
* 建立setup.py

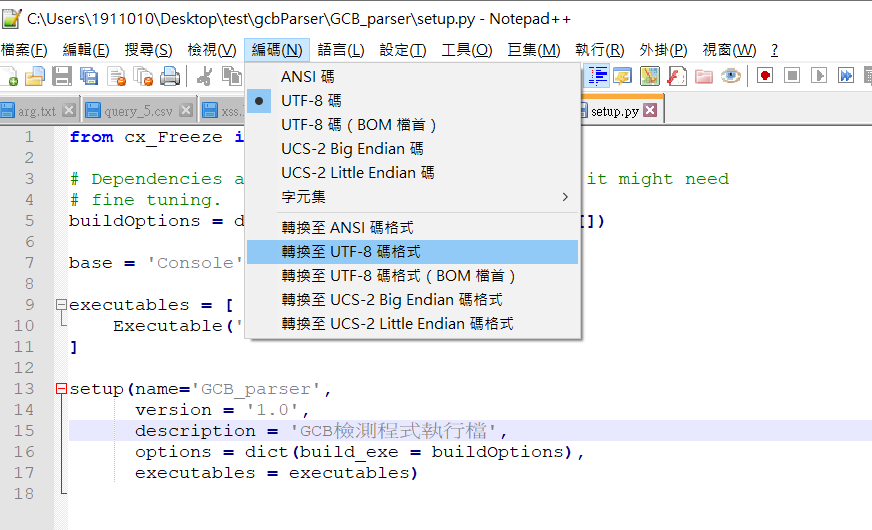


執行cxfreeze-quickstart後依序填入相關資訊或採用預設值(出現方括號[\*]之欄位)

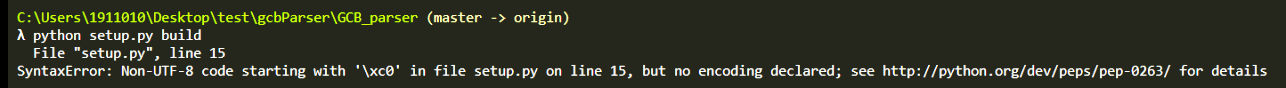
檢視前一步驟將自動產生setup.py後再執行，先選n

* 檢視setup.py

setup.py內容應如下圖所示，前一步驟所填入資訊應該也會出現於setup.py內。

另外，應使用編輯器將setup.py轉換為UTF-8編碼，如未轉換UTF-8編碼，執行時將發生錯誤。

* 執行setup.py

執行指令「python setup.py build」，若前一步驟未執行UTF-8編碼轉換，可能將出現「*SyntaxError: Non-UTF-8 code starting with*」錯誤訊息。

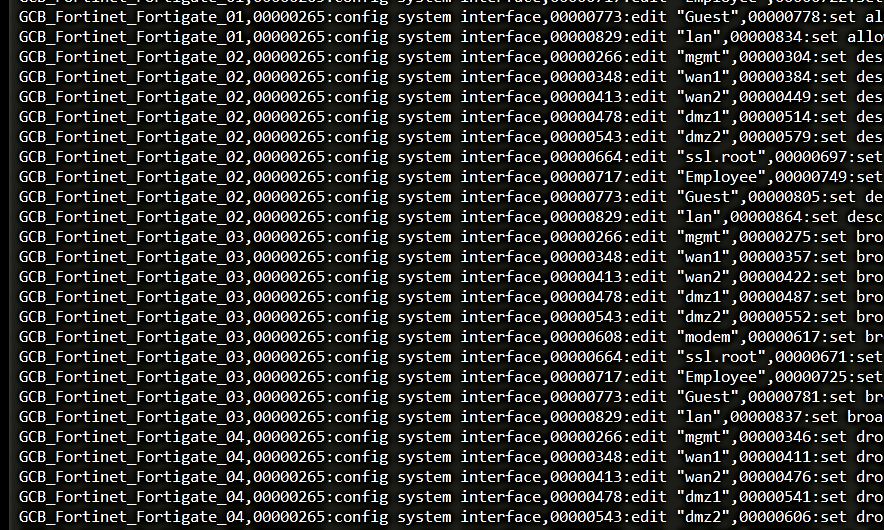
執行成功後，將產生build資料夾，內部包含了相關檔案

Build底下子資料夾「exe.win-amd64-3.7」包含了最終的執行檔(exe)及其他檔案



* 執行執行檔

於arg.txt將參數設定完畢並置於與執行檔(GCB\_parser.exe)同一資料夾內，直接於命令列模式或點擊執行(建議採用命令列模式，方可檢視訊息)



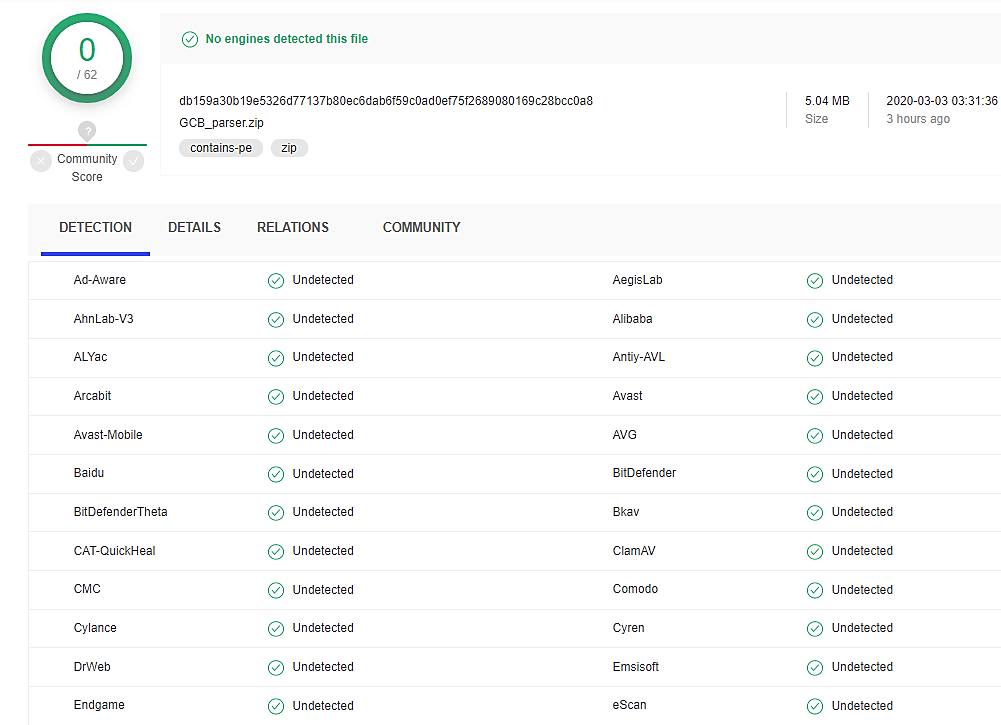
**執行檔**

**執行結果**

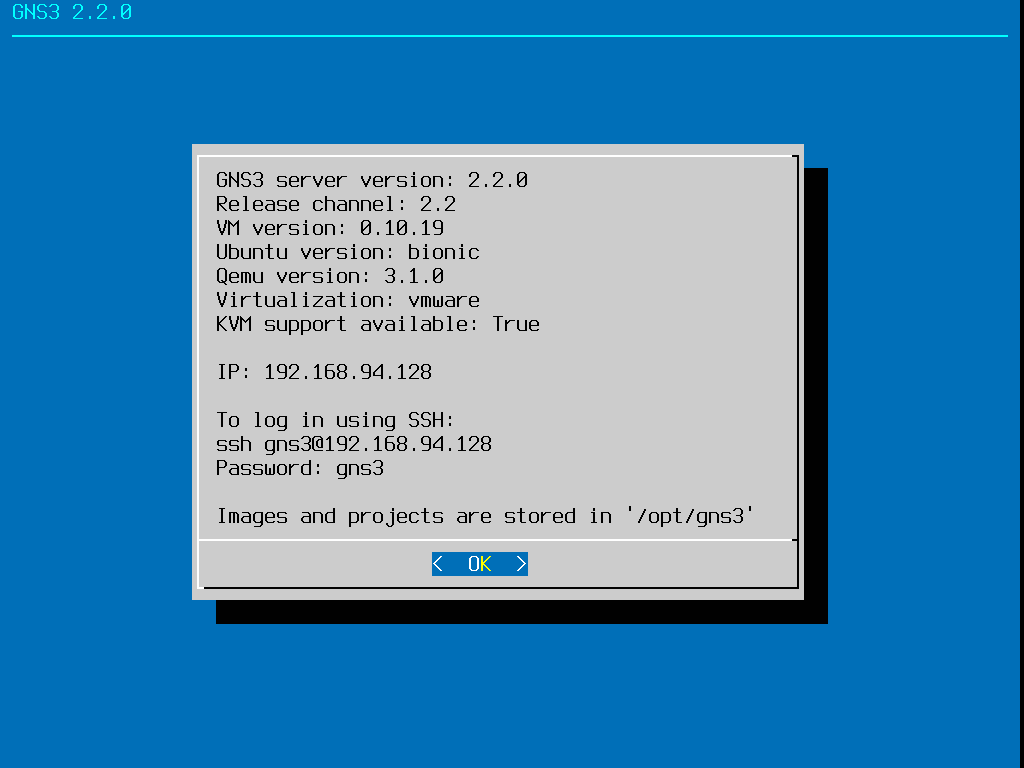
* 打包檔案

Build資料夾底下子資料夾「exe.win-amd64-3.7」包含了最終的執行檔(exe)及其他檔案，有時將該資料夾打包壓縮為一個壓縮檔對後續作業較為方便。可使用「run.bat」檔案將資料夾壓縮。run.bat可將GCB parser的python程式碼(py)轉為可執行檔(exe)並打包為單一壓縮檔，run.bat的程式碼如下：

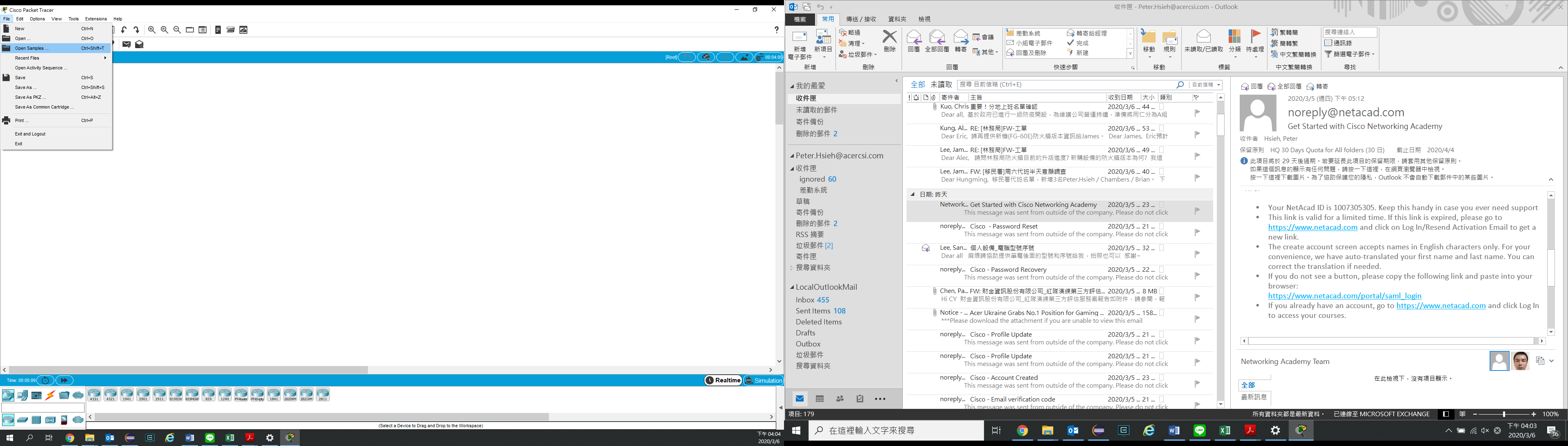
完成之壓縮檔可上傳[VirusTotal](https://www.virustotal.com/gui/home)網站進行掃毒，以便通過受測方相關規定。

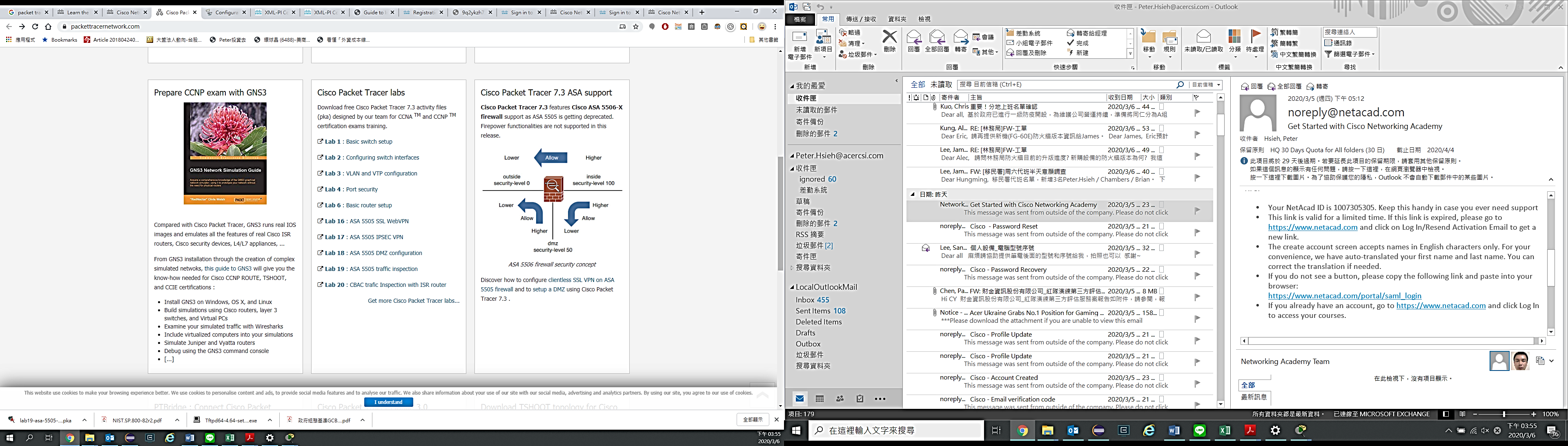


附錄3-建立Cisco ASA模擬器(GNS3)

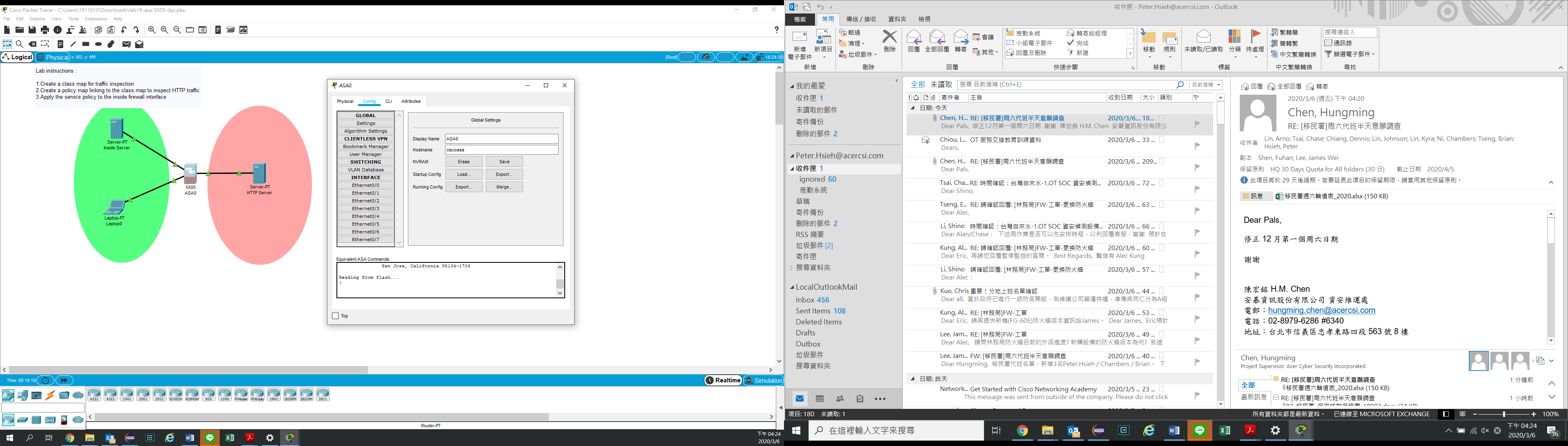
1. 安裝[VMware Workstation Pro](https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html)
2. 下載[GNS3 VM](https://docs.gns3.com/1Bn-s1Izkjp13HxcPF4b8QSGfkWJYG_dpMt9U1DQjvZ4/index.html)(VMware workstation版本)
3. [導入GNS3 VM](https://docs.gns3.com/1wdfvS-OlFfOf7HWZoSXMbG58C4pMSy7vKJFiKKVResc/index.html#h.7bpr0ifw7uh1)
4. [連結本機GNS3與GNS3 VM](https://docs.gns3.com/1wdfvS-OlFfOf7HWZoSXMbG58C4pMSy7vKJFiKKVResc/index.html#h.wu16cddrm37o)，連結成功後，GNS3 VM將會開機，並呈現以下畫面
5. (暫緩)

附錄3-建立Cisco ASA模擬器(packet tracer)

1. 下載並安裝[packet tracer](https://www.netacad.com/zh-hant/courses/packet-tracer)
2. 申請[Cisco帳號](https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui)
3. 開啟packet tracer並使用帳號登入
4. 至 <https://www.packettracernetwork.com/>下載ASA lab檔案(\*.pka)，例如lab16、17、18、19



1. 開啟pka檔案，File🡪Open Samples
2. ASA lab開啟，點擊ASA 圖示，開啟視窗



**ASA圖示**

1. 點擊Export按鈕，導出config檔案

