1. IOT從架構生態系統到安全

IoT Attack Surface Areas 物聯網攻擊面向

物聯網的發展面向會更廣，尤其是當裝置感測器更多元，系統彼此間更開放互連，並能與各式應用服務相結合，攻擊面向也將更廣。 常見的攻擊像網路攻擊行為，通常就是電腦中毒、資料竊取、網站被入侵等，在物聯發展浪潮之下，現在攻擊重心開始擴散至各式連網系統與裝置，受到攻擊與濫用的比例已有明顯的增加趨勢。以往在電腦、智慧型手機上才有的隱私保護、資訊安全問題，也成為更多連網設備與系統同樣需要面對的事。

**Ecosystem Access Control 生態系統訪問控制**

* Implicit trust between components
* Enrollment security
* Decommissioning system
* Lost access procedures

**Device Memory 設備的記憶體**

* Cleartext usernames
* Cleartext passwords
* Third-party credentials
* Encryption keys

**Device Physical Interfaces 設備的實體存取介面**

* Firmware extraction
* User CLI
* Admin CLI
* Privilege escalation
* Reset to insecure state
* Removal of storage media

**Device Web Interface 設備的網頁介面**

* SQL injection
* Cross-site scripting
* Cross-site Request Forgery
* Username enumeration
* Weak passwords
* Account lockout
* Known default credentials

**Device Firmware 設備的韌體**

* Hardcoded credentials
* Sensitive information disclosure
* Sensitive URL disclosure
* Encryption keys
* Firmware version display and/or last update date

**Device Network Services 設備的網路服務**

* Information disclosure
* User CLI
* Administrative CLI
* Injection
* Denial of Service
* Unencrypted Services
* Poorly implemented encryption
* Test/Development Services
* Buffer Overflow
* UPnP
* Vulnerable UDP Services
* DoS

**Administrative Interface 管理介面**

* SQL injection
* Cross-site scripting
* Cross-site Request Forgery
* Username enumeration
* Weak passwords
* Account lockout
* Known default credentials
* Security/encryption options
* Logging options
* Two-factor authentication
* Inability to wipe device

**Local Data Storage 本地資料儲存**

* Unencrypted data
* Data encrypted with discovered keys
* Lack of data integrity checks

**Cloud Web Interface 雲端網頁介面**

* SQL injection
* Cross-site scripting
* Cross-site Request Forgery
* Username enumeration
* Weak passwords
* Account lockout
* Known default credentials
* Transport encryption
* Insecure password recovery mechanism
* Two-factor authentication

**Third-party Backend APIs 第三方的後端API**

* Unencrypted PII sent
* Encrypted PII sent
* Device information leaked
* Location leaked

**Update Mechanism 更新機制**

* Update sent without encryption
* Updates not signed
* Update location writable
* Update verification
* Malicious update
* Missing update mechanism
* No manual update mechanism

**Mobile Application 行動裝置的應用程式**

* Implicitly trusted by device or cloud
* Username enumeration
* Account lockout
* Known default credentials
* Weak passwords
* Insecure data storage
* Transport encryption
* Insecure password recovery mechanism
* Two-factor authentication

**Vendor Backend APIs 供應商後端API**

* Inherent trust of cloud or mobile application
* Weak authentication
* Weak access controls
* Injection attacks

**Ecosystem Communication 生物系統的通訊**

* Health checks
* Heartbeats
* Ecosystem commands
* Deprovisioning
* Pushing updates

**Network Traffic 網路流量**

* LAN
* LAN to Internet
* Short range
* Non-standard

1. IOT機制安全的挑戰話題

**IoT Security TOP 10 物聯網十大安全測試**

物聯網十大安全測試目標是幫助測試人員評估物聯網空間中的物聯網設備和應用程序。下面列出10項基本測試。但這不是全部的事項，但確保涵蓋這些基本原則將大大提高任何物聯網產品的安全性

**I1. Insecure Web Interface 不安全的網頁介面**

其實也就是一般最常見的Web安全，任何網站在實作上可能產生的漏洞(SQLi, XSS, CSRF…)都在這個範疇，可參考OWASP Top 10。

* Assess any web interface to determine if weak passwords are allowed
* Assess the account lockout mechanism
* Assess the web interface for XSS, SQLi and CSRF vulnerabilities and other web application vulnerabilities
* Assess the use of HTTPS to protect transmitted information
* Assess the ability to change the username and password
* Determine if web application firewalls are used to protect web interfaces

**I2. Insufficient Authentication/Authorization 認證/授權不足**

任何需要存取的動作，都需要去確認認證與授權是否合法。那麼在IoT中要去哪裡檢查認證與授權呢？答案是找出整個IoT架構中所有的介面(Interface)，無論是雲端提供介面給設備傳遞資料過去，或者是使用者透過行動裝置連至雲端提供的行動介面存取資料。建議做法如啟用雙因子認證、當使用到一些比較敏感的功能可以進行重新認證、確保發給client的認證token/session key保持不一樣等。

* Assess the solution for the use of strong passwords where authentication is needed
* Assess the solution for multi-user environments and ensure it includes functionality for role separation
* Assess the solution for Implementation two-factor authentication where possible
* Assess password recovery mechanisms
* Assess the solution for the option to require strong passwords
* Assess the solution for the option to force password expiration after a specific period
* Assess the solution for the option to change the default username and password

**I3. Insecure Network Services 不安全的網路服務**

若物聯網裝置有不安全的網路服務公開在Local或Global Network，可能會導致Buffer Overflow或DoS的問題，可以利用自動化工具如Port Scanner或Fuzzer。

* Assess the solution to ensure network services don't respond poorly to buffer overflow, fuzzing or denial of service attacks
* Assess the solution to ensure test ports are are not present

**I4. Lack of Transport Encryption 缺少傳輸加密**

物聯網資料間的傳輸，無論是有線或無線的都可能使用各式各樣的協定或技術(BLE, TLS, RFID, NFC…)。這些協定或技術在傳輸時是否會進行加密其實也不一定，需要去了解這些協定的實作。

* Assess the solution to determine the use of encrypted communication between devices and between devices and the internet
* Assess the solution to determine if accepted encryption practices are used and if proprietary protocols are avoided
* Assess the solution to determine if a firewall option available is available

**I5. Privacy Concerns 隱私問題**

這個部分舉例來說，當使用者在設定或啟用物聯網裝置時，可以去檢查看看裝置所蒐集的資料。裝置是建議最好不要蒐集敏感性資料，要儲存的話可將資料去識別化或匿名後再儲存。

* Assess the solution to determine the amount of personal information collected
* Assess the solution to determine if collected personal data is properly protected using encryption at rest and in transit
* Assess the solution to determine if Ensuring data is de-identified or anonymized
* Assess the solution to ensure end-users are given a choice for data collected beyond what is needed for proper operation of the device

**I6. Insecure Cloud Interface 不安全的雲端介面**

關於雲端介面的安全性，OWASP也有Cloud Top 10，不過這Top 10會包含整個雲的安全性問題，但這邊主要著重在提供給使用者/管理者的雲端介面安全。

* Assess the cloud interfaces for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces)
* Assess the cloud-based web interface to ensure it disallows weak passwords
* Assess the cloud-based web interface to ensure it includes an account lockout mechanism
* Assess the cloud-based web interface to determine if two-factor authentication is used
* Assess any cloud interfaces for XSS, SQLi and CSRF vulnerabilities and other vulnerabilities
* Assess all cloud interfaces to ensure transport encryption is used
* Assess the cloud interfaces to determine if the option to require strong passwords is available
* Assess the cloud interfaces to determine if the option to force password expiration after a specific period is available
* Assess the cloud interfaces to determine if the option to change the default username and password is available

**I7: Insecure Mobile Interface 不安全的行動介面**

關於行動介面的安全性，OWASP也提出了Mobile Top 10可以參考。基本上不外乎提供給使用者操作的行動介面證機制是否安全完善、資料傳輸時是否安全、連續登入失敗帳號是否鎖定、密碼復原機制是否有漏洞、APP是否有進行混淆或防竄改機制等。

* Assess the mobile interface to ensure it disallows weak passwords
* Assess the mobile interface to ensure it includes an account lockout mechanism
* Assess the mobile interface to determine if it Implements two-factor authentication (e.g Apple's Touch ID)
* Assess the mobile interface to determine if it uses transport encryption
* Assess the mobile interface to determine if the option to require strong passwords is available
* Assess the mobile interface to determine if the option to force password expiration after a specific period is available
* Assess the mobile interface to determine if the option to change the default username and password is available
* Assess the mobile interface to determine the amount of personal information collected

**I8. Insufficient Security Configurability 安全配置性不足**

主要講得是物聯網裝置的安全設定，例如有些設備可能提供可以設定密碼的功能，但卻沒強制一定要輸入”強”密碼，這是一種安全性設定的不足；又或者傳輸中的或儲存在設備上的敏感資料未加密也是一種。另外也建議IoT設備可以對於安全事件做紀錄或通知使用者。

* Assess the solution to determine if password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication) are available
* Assess the solution to determine if encryption options (e.g. Enabling AES-256 where AES-128 is the default setting) are available
* Assess the solution to determine if logging for security events is available
* Assess the solution to determine if alerts and notifications to the user for security events are available

**I9. Insecure Software/Firmware 不安全的軟體與韌體**

此部分主要鎖定在IoT設備軟體/韌體更新的安全性。若設備具有自動更新功能時，除了更新伺服器的安全外，更新檔傳輸時(是否使用加密通道)以及更新檔本身的安全性(檔案是否加密、是否簽章並在傳遞/安裝前驗證過)都很重要。

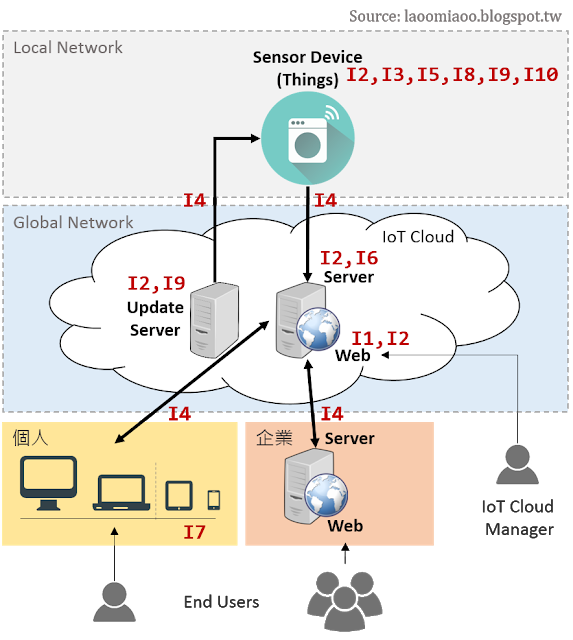
* Assess the device to ensure it includes update capability and can be updated quickly when vulnerabilities are discovered
* Assess the device to ensure it uses encrypted update files and that the files are transmitted using encryption
* Assess the device to ensure is uses signed files and then validates that file before installation

**I10. Poor Physical Security 實體安全考量不足**

考量到物聯網裝置的實體安全，例如裝置是否有可卸除式儲存設備如SD Card能輕易移除，若裡面的資料又未加密則可能遭到竊取或竄改；又或者有些物聯網設備可能會透過USB Port進行軟體更新，此USB Port若未受控制，也可能被利用於修改設備軟體或拿來複製資料。

* Assess the device to ensure it utilizes a minimal number of physical external ports (e.g. USB ports) on the device
* Assess the device to determine if it can be accessed via unintended methods such as through an unnecessary USB port
* Assess the device to determine if it allows for disabling of unused physical ports such as USB
* Assess the device to determine if it includes the ability to limit administrative capabilities to a local interface only

OWASP IoT Top 10架構圖



**案例【微軟修補Outlook系列Security Feature Bypass資訊產品漏洞】**

概述：

Microsoft Outlook系列產品存在共同弱點，駭客可迂迴執行任意程式碼，截獲信件內文，Microsoft就相關版本軟體提供對應之安全更新。

編註：

(1) Security Feature Bypass漏洞：係因Outlook對記憶體內物件處理不當，駭客採行一套”檔案共享攻擊”劇本，設計特製文件提供給使用者，並說服其開檔互動，得手後利用該漏洞能以受害者權限執行任意程式。

(2) Information Disclosure漏洞：Outlook建立安全連線失敗，駭客藉此監視網路，取得受害者郵件內文。

受影響之版本

Microsoft Outlook 2010 SP2、2013 RT SP1、2016

解決辦法：

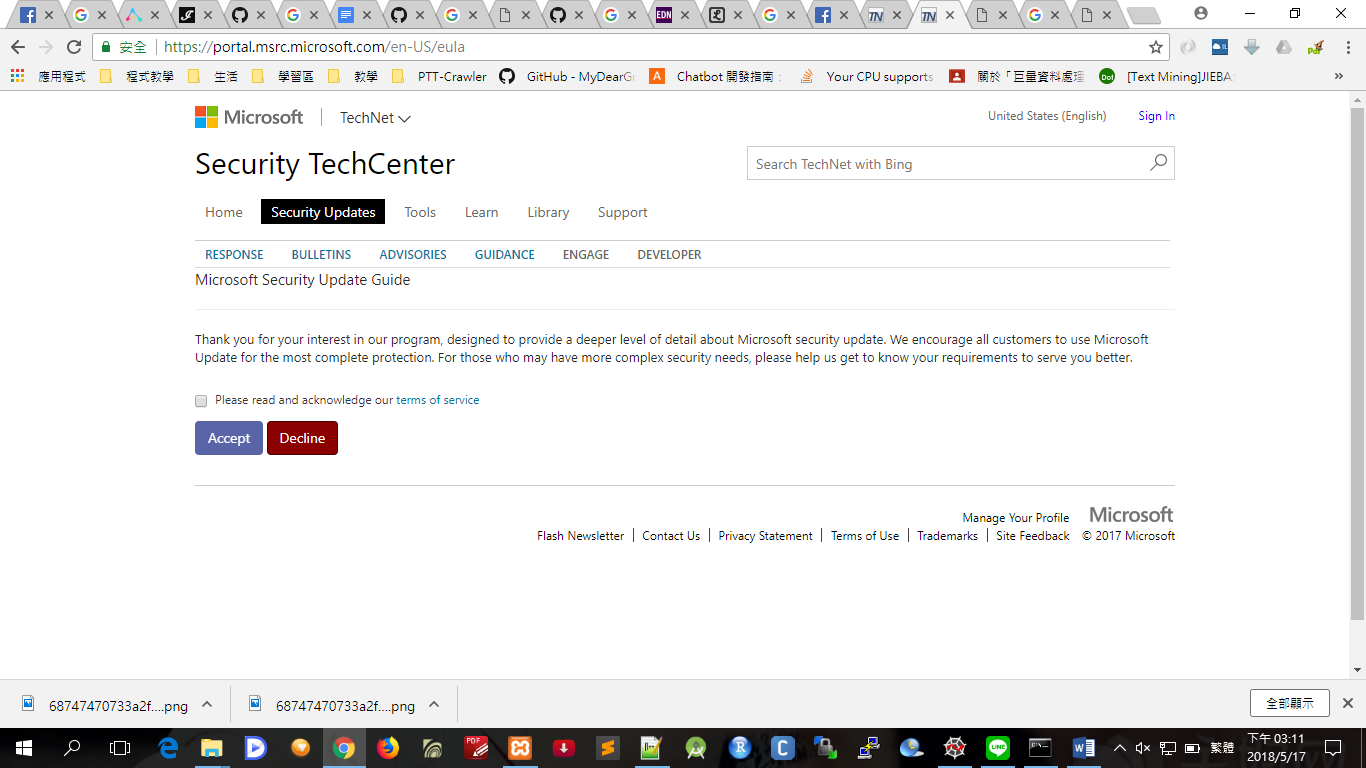
(1)閱覽以下連結，下載所需更新檔。

https://portal.msrc.microsoft.com/en-US/eula

(2)避免以管理者權限進行一般性文書處理。

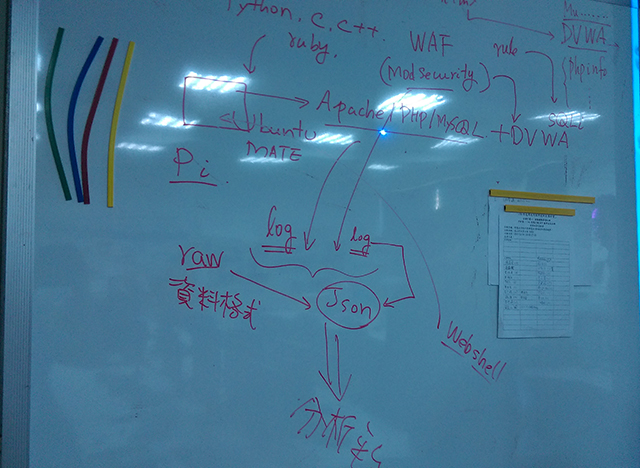
更多【資訊產品漏洞】請參考

https://www.twcert.org.tw/twcert/advistory



1. IOT安全演練

DVWA漏洞測試架構



**檢視apache web server的log檔**

/var/log/apache2

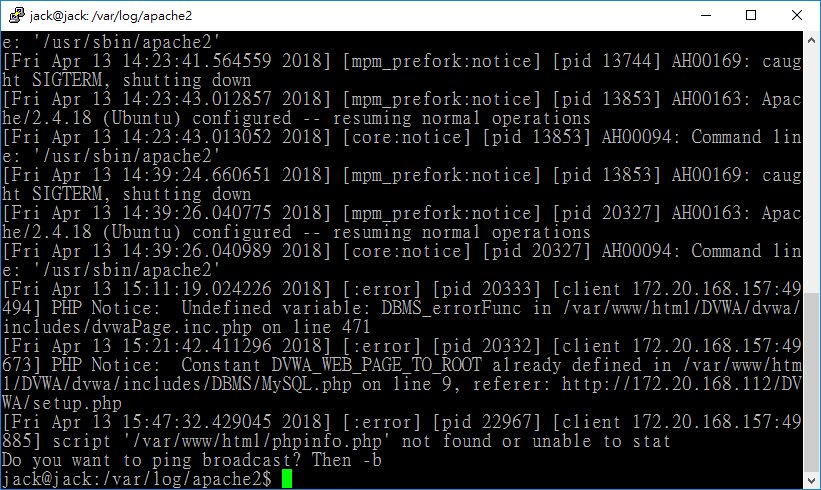
access.log

error.log

modsec\_audit.log

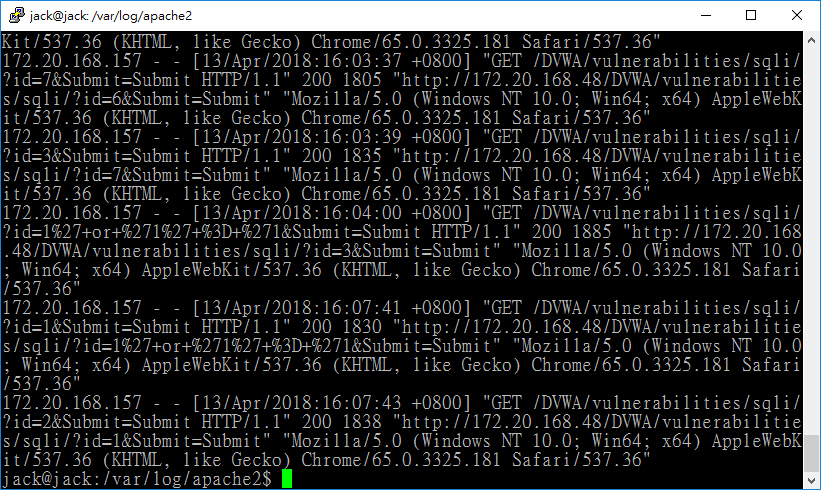
**cat error.log**

DVWA網頁下過的指令有錯誤的，會記錄在error.log中， 讓使用者知道有那些錯誤的內容



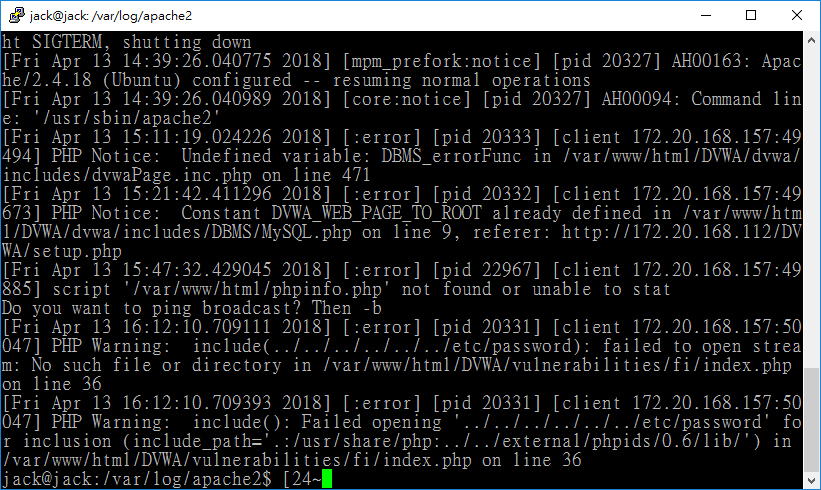
**cat access.log**

DVWA網頁下過的指令都會記錄在access.log中， 讓使用者了解下過那些指令



在網址打 <http://172.20.168.157/DVWA/vulnerabilities/fi/?page=../../../../../../etc/password>

cat error.log 會出現剛才打網址的error message

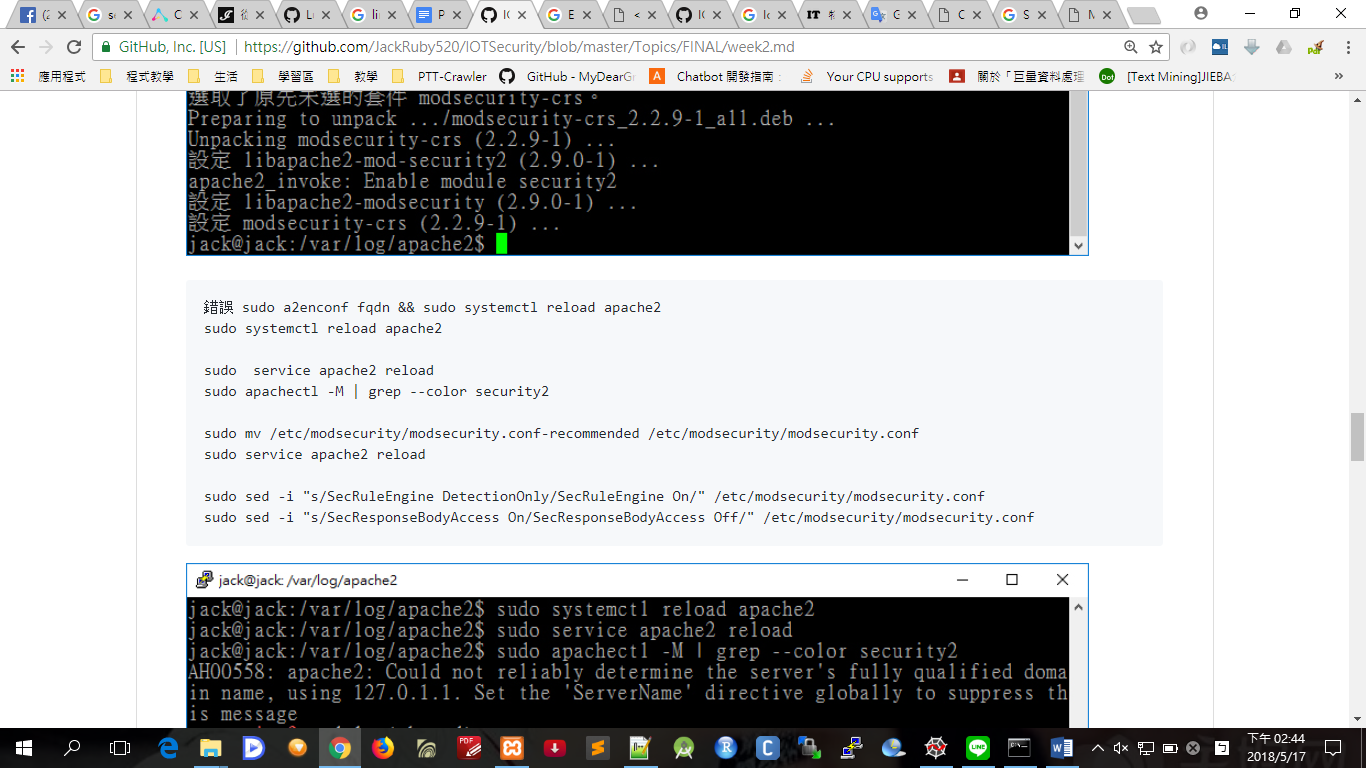


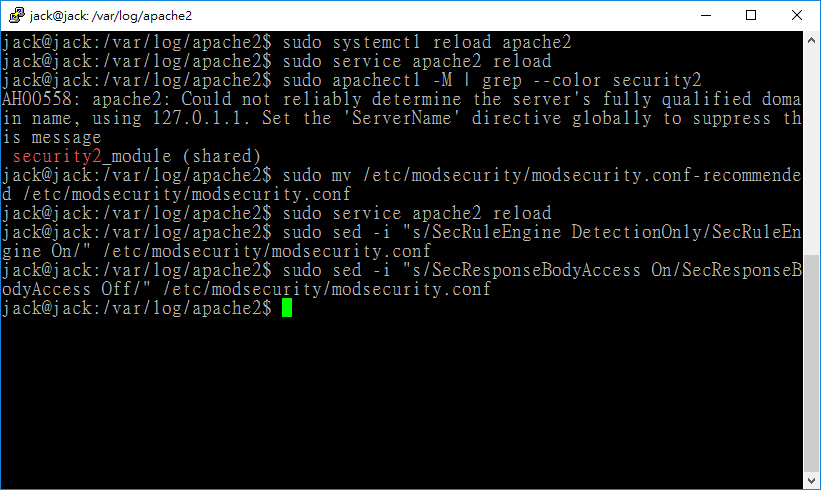
### 安裝modsecurity

sudo apt-get update

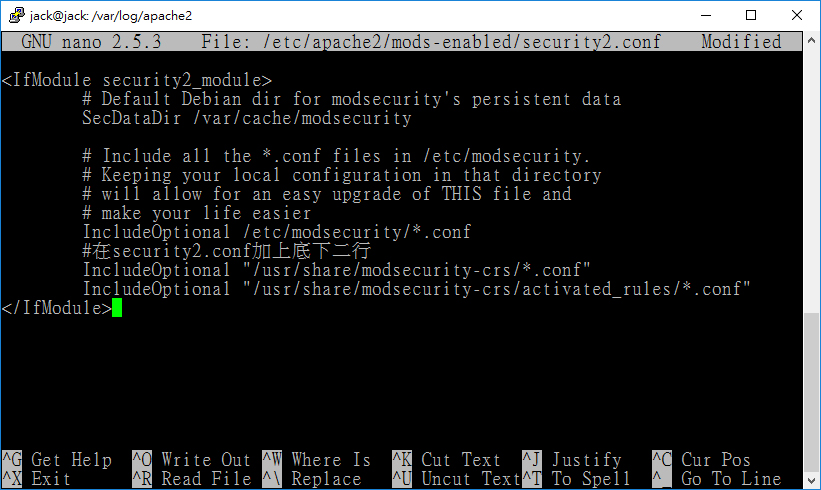
sudo apt-get install libapache2-modsecurity -y







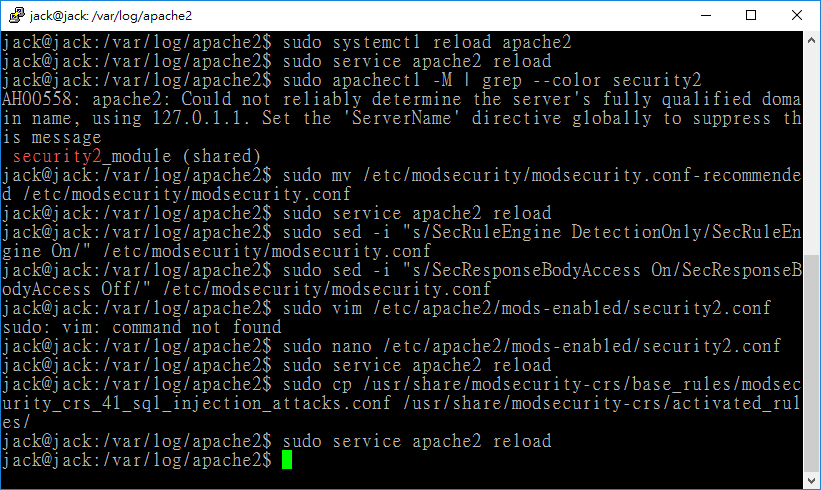




sudo service apache2 reload

sudo cp /usr/share/modsecurity-crs/base\_rules/modsecurity\_crs\_41\_sql\_injection\_attacks.conf /usr/share/modsecurity-crs/activated\_rules/

sudo service apache2 reload







安裝伺服器系統

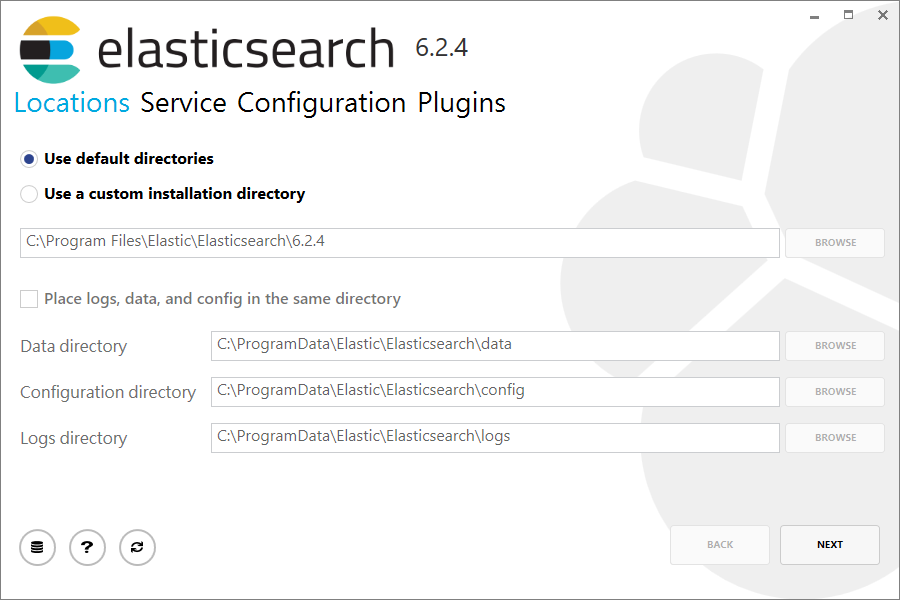
Elasticsearch + Kibana

**安裝 Elasticsearch**

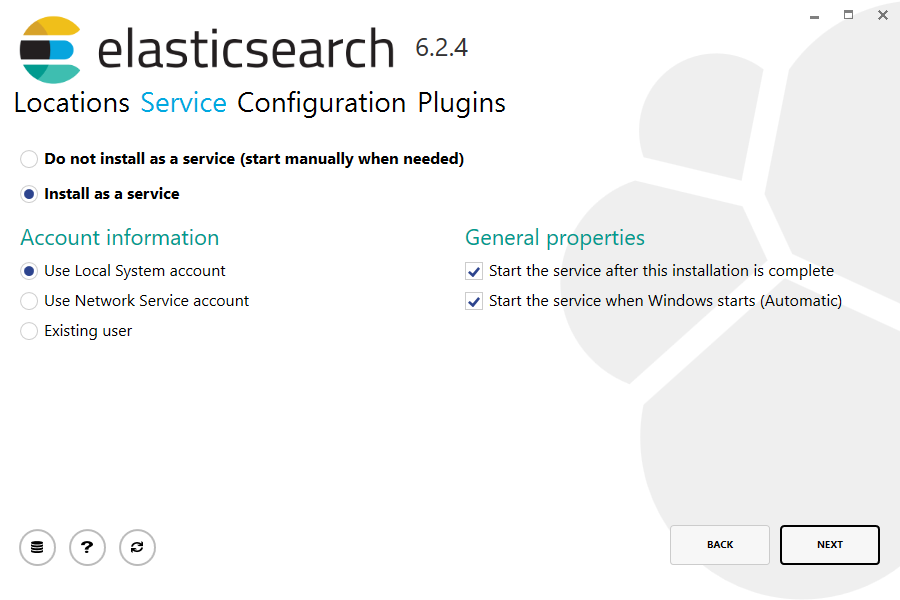
下載網址: https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.2.4.msi

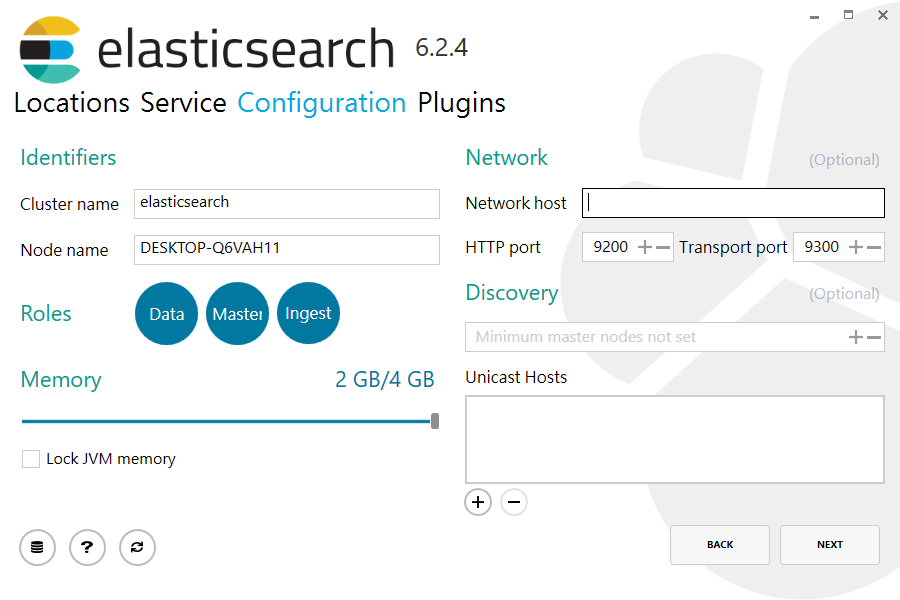
開始安裝

Step1.



Step2.



Step3.  
[](https://github.com/MtFeather/IOTSecurity/blob/master/images/elastic_3.PNG)

**啟動服務**

使用系統管理員身分執行cmd移動到"C:\Program Files\Elastic\Elasticsearch\6.2.4\bin"

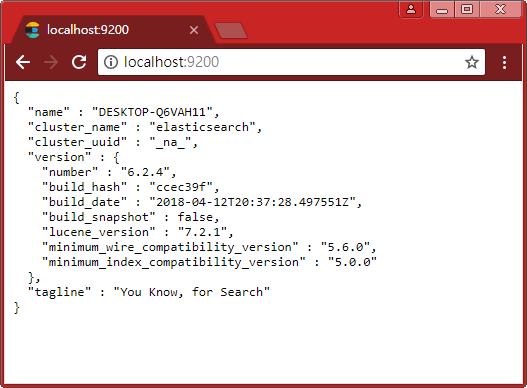
cd C:\Program Files\Elastic\Elasticsearch\6.2.4\bin

**執行啟動**

./elasticsearch.exe

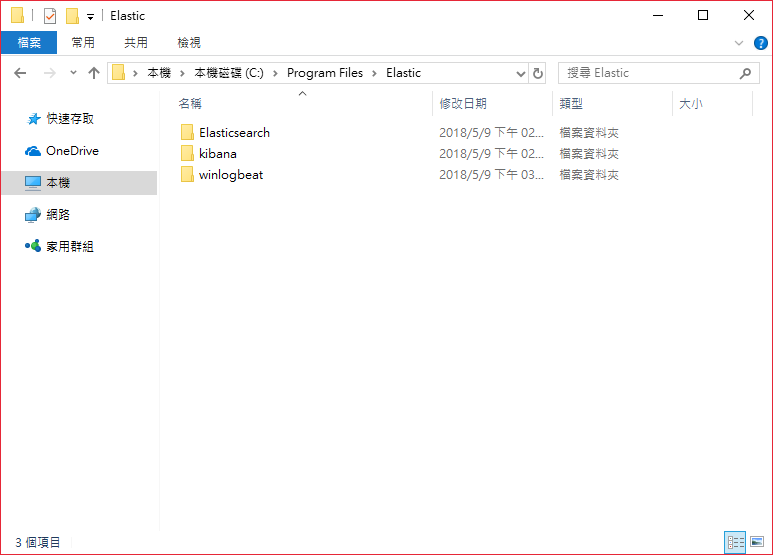
**檢查測試**

在網站URL: http://localhost:9200/



**安裝 Kibana**

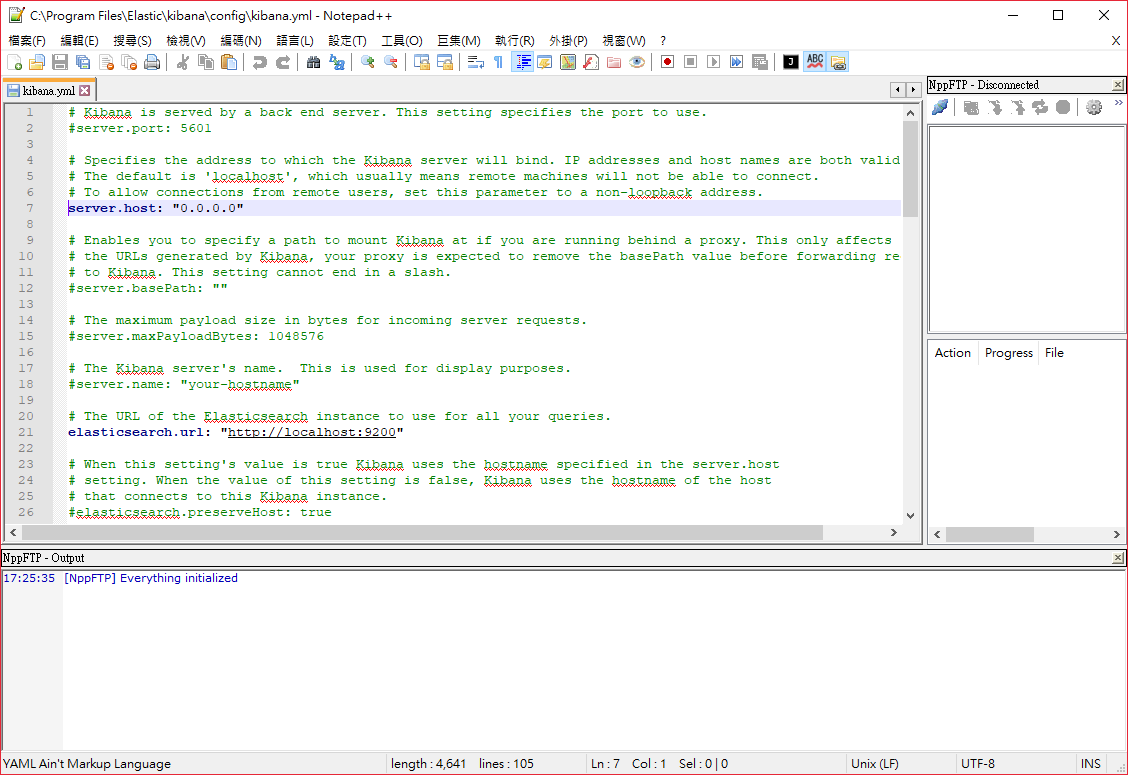
* 下載網址: https://artifacts.elastic.co/downloads/kibana/kibana-6.2.4-windows-x86\_64.zip
* 解壓縮後，我是將目錄與Elasticsearch放在同一層的目錄(C:\Program Files\Elastic)，並且將目錄去除後面的版本名稱



### 修改設定值

* 修改kibana目錄的config/kibana.yml，將server.host的註解拿掉，並把裡面的"localhost"換成"0.0.0.0"

server.host: "0.0.0.0" # 0.0.0.0 表示綁定所有 IP



**啟動服務**

使用系統管理員身分執行cmd移動到"C:\Program Files\Elastic\kibana\bin"

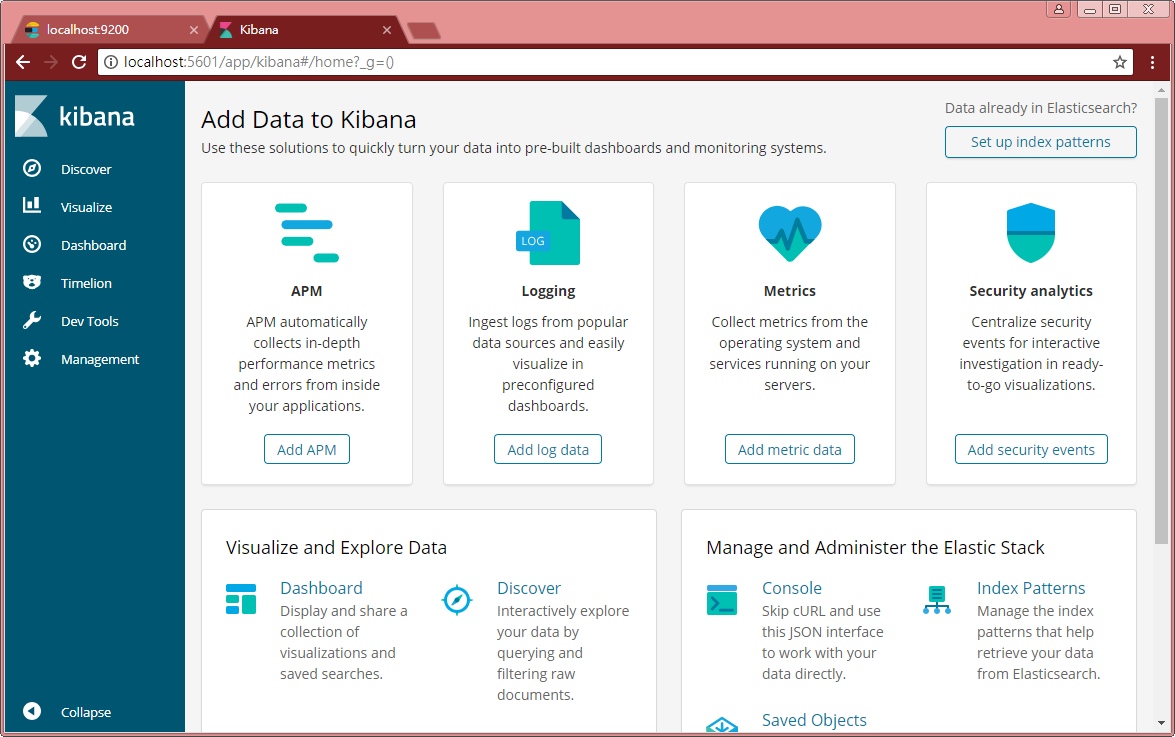
cd C:\Program Files\Elastic\kibana\bin

**執行啟動**

./kibana.bat

**檢查測試**

在網站URL: http://localhost:5601/

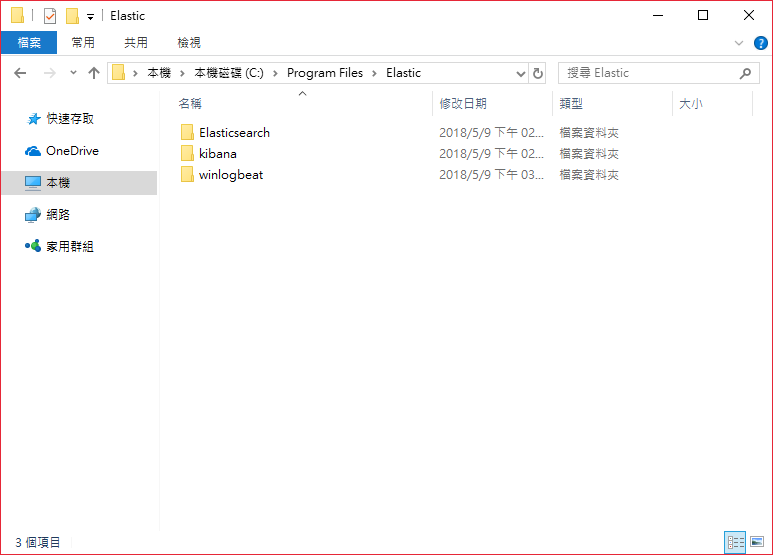


**安裝客戶端資料傳送軟體**

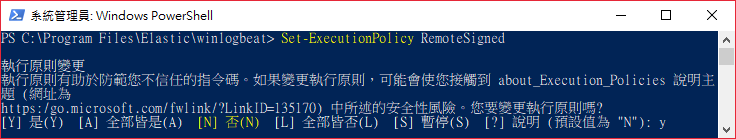
Windows是winlogbeat，Linux是logstash

**安裝 winlogbeat@Windows**

* 下載網址: https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-6.2.4-windows-x86\_64.zip
* 解壓縮後，我是將目錄與Elasticsearch放在同一層的目錄(C:\Program Files\Elastic)，並且將目錄去除後面的版本名稱



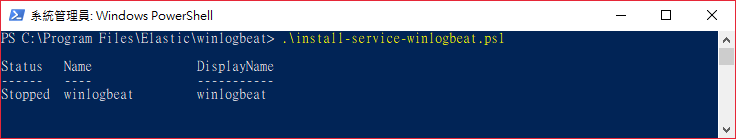
Set-ExecutionPolicy RemoteSigned



**安裝**

cd 'C:\Program Files\Elastic\winlogbeat'

.\install-service-winlogbeat.ps1



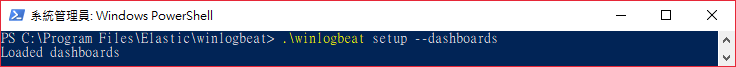
**測試**

cd 'C:\Program Files\Elastic\winlogbeat'

.\winlogbeat.exe test config -c .\winlogbeat.yml -e

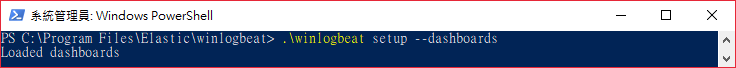


.\winlogbeat setup –dashboards

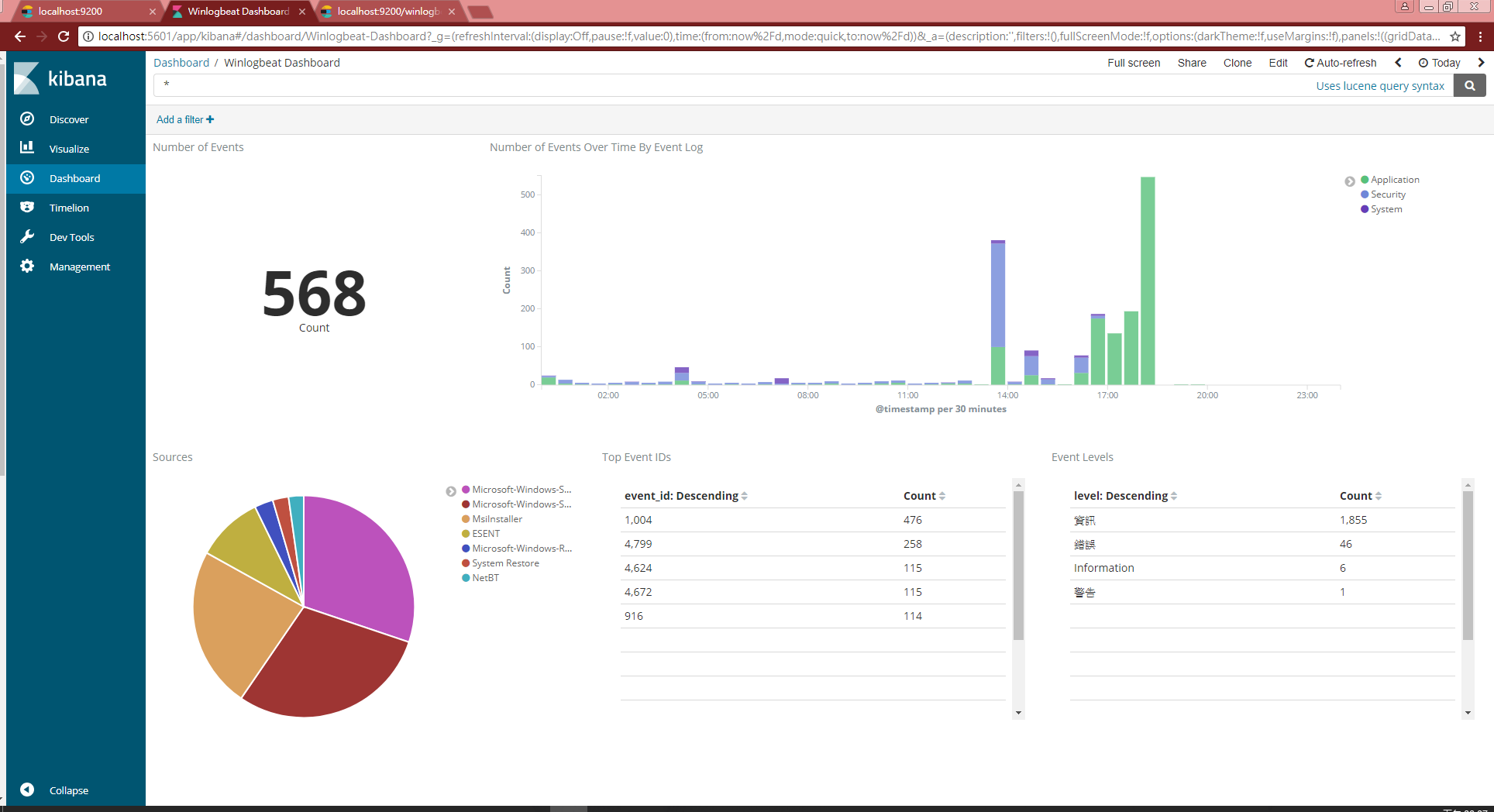


**啟動winlogbeat服務**

Start-Service winlogbeat



在kibana看到的結果



1. 未來研究方向

我的論文研究是**AI 自然語言處理(NLP)的語料訓練**，將Python Scrapy爬取的語料去掉網頁標籤，之後將語料轉成向量做訓練，將訓練好的語料庫運用在AI 機器人seq2seq的語音對話。機器人本身就是Server，未來會研究IOT**安全資訊系統開發(SSDLC)**，來防備Server不受安全漏洞的攻擊，讓AI機器人語音系統更機密性、完整性、可用性，使本系統在資訊安全減少漏洞的攻擊。