開源資安防護搭配入侵偵測(SNORT)

北區資訊安全維運中心

資安工程師：劉家維

01
什麼是入侵偵測

網路威脅

社交工程

勒索軟體

網路蠕蟲

漏洞攻擊

網路釣魚

木馬程式

入侵偵測防護方式

特徵值偵測
Signature-based Detection

異常行為偵測
Anomaly-based Detection

狀態協定分析
Stateful Protocol Analysis

入侵指標防護
Intelligence-base Detection

Signature Detection

- 利用病毒特徵碼與攻擊手法制定入侵偵測規則及建立特徵值資料庫。
- 準確率較高，誤判機率較低。
- 須逐一檢測所有網路封包，與大量的特徵碼作比對，設備loading較重。
- 無法偵測未知型的攻擊，需要靠其他機制偕同運作。

Anomaly Detection

- 學習一段時間的網路連線數值後制定閥值。
  - 例如，登入失敗次數、主機DNS查詢次數等等
- 可偵測到未知的攻擊手法。
- 事件誤判機率較高
- 可搭配大數據或AI進階分析。

Stateful Protocol Analysis

- 利用系統預先定義好的通訊協定連線狀態資料庫，與實際網路通訊進行比對，例如於HTTP 連線進行時出現不正常的網頁存取行為，或是於使用者名稱欄位出現不正確的系統指令參數等。
- 能夠細緻的偵測到網路通訊時不符合該協定規範的異常行為。
- 非常消耗系統資源。

Intelligence Detection

- 透過各種IoC、檔案Hash、IP、Domain、URL黑名單阻擋異常行為。
- 效果取決於資安情資的數量、正確性、更新速度
- 消耗系統資源較小。

02
開源入侵偵測SNORT

SNORT 簡介

1. Snort是一套開放的(Open Source)、跨平台（Uinx, Windows…)的NIDS，可用來偵測網路上的異常封包， 1998年由Marty Roesch開發，全球下載超過四百萬 次。
2. 檢查所有經過的封包，並利用特徵比對的方式判斷 是否有可能的入侵行為
3. 規則是開放的方式來發展的，可以自行加入偵測規 則，以加強入侵行為的偵測
4. SNORT官方網站：http://www.snort.org/

SNORT 註冊

1. 至SNORT 官網進行註冊 ：http://www.snort.org/
2. 取得Oinkcode
3. 根據系統版本選取不同的安裝方式

SNORT 運行模式

Sniffer mode

讀取流經的網路封包並顯示封包的Header及Body，，不進行阻擋及儲存封包。

Packet Logger mode

與Sniffer mode 不同的點在於，將讀取的封包會儲存至指定的目錄，可下filter指令紀錄特定條件封包。

Network Intrusion Detection System mode

NIDS模式針對流經的網路流量進行檢測分析，可選擇不同的偵測規則，該模式下可設定Inline、Passive、Inline-Test等模式。

SNORT 行為模式差異

Rule Option	Inline Mode	Passive Mode	Inline-Test Mode
reject	Drop + Response	Alert + Response	Wdrop + Response
normalize	Normalizes packet	Doesn't normalize	Doesn't normalize
replace	replace content	Doesn't replace	Doesn't replace
respond	close session	close session	close session

SNORT IDS Component

Packet Capture Engine → Preprocessor Plug-ins → Detection Engine → Output Plug-ins

Packet capture engine

1. 透過WinPcap或Npcap 套件從網卡擷取網路封包
2. 將封包轉拋至Preprocessor 模組

Preprocessor Plug-ins

1. 接收封包並確認針對每個封包的處理方式(analysis、reject、alert)

2. TCP/IP流量狀態分析、偵測PortScan、Decoder

Detection Engine

1. 將解碼後的封包從L3 開始比對到L7的內容
2. 將封包內的特徵值與所有rule 依序比對。

Output Plug-ins

1. 將Preprocessor、Detection Engine 偵測的結果產生告警
   告警訊息並輸出。

SNORT 安装

Get Started

Step 1

Find the appropriate package for your operating system and install.

Source | Fedora | Centos | FreeBSD | Windows

```
wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

wget https://www.snort.org/downloads/snort/snort-2.9.19.tar.gz
```

```
tar xvzf daq-2.0.7.tar.gz

cd daq-2.0.7
./configure && make && sudo make install
```

```
tar xvzf snort-2.9.19.tar.gz

cd snort-2.9.19
./configure --enable-sourcefire && make && sudo make install
```

Downloads

Step 2

Sign up and get your Oinkcode. We recommend that everyone subscribe to get the latest detections. For those unable to subscribe, creating an account on Snort.org will still give you access to the registered user rule packages.

Sign up/Subscribe

Step 3

Stay current with the latest updates using PulledPork

Community rules | Registered rules | Subscriber rules

```
loads/community/community-rules.tar.gz -O community-rules.tar.gz
```

```
tar -xvzf community-rules.tar.gz -C /etc/snort/rules
```

Downloads

opensource.gz
snort3-community-rules.tar.gz
community-rules.tar.gz

Npcap 安装

安装Snort 套件前需先安装Npcap 套件。

Many more details about Npcap are available in the Npcap User/Developer Guide. We've also created a feature comparison between Npcap and WinPcap.

Downloading and Installing Npcap Free Edition

The free version of Npcap may be used (but not externally redistributed) on up to 5 systems (free license details). It may also be used on unlimited systems where it is only used with Nmap, Wireshark, and/or Microsoft Defender for Identity. Simply run the executable installer. The full source code for each release is available, and developers can build their apps against the SDK. The improvements for each release are documented in the Npcap Changelog.

- Npcap 1.60 installer for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019 (x86, x64, and ARM64).
- Npcap SDK 1.12 (ZIP).
- Npcap 1.60 debug symbols (ZIP).
- Npcap 1.60 source code (ZIP).

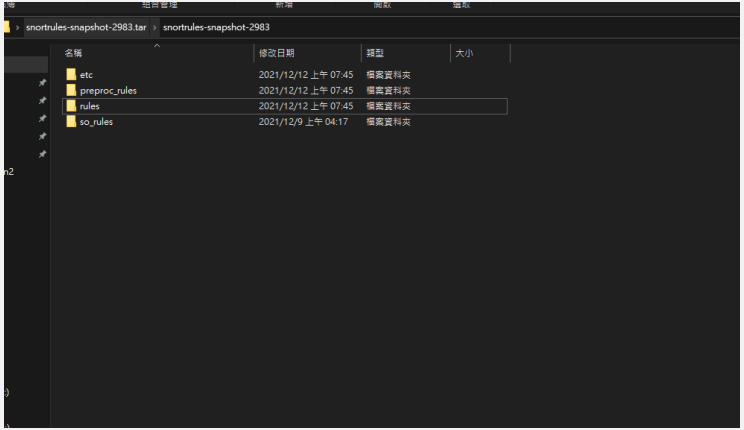
The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

Snort rule 下載

於Snort 官網登入後，下載Snort 2.9版規則壓縮檔，將四個資料夾覆蓋至Snort 跟目錄

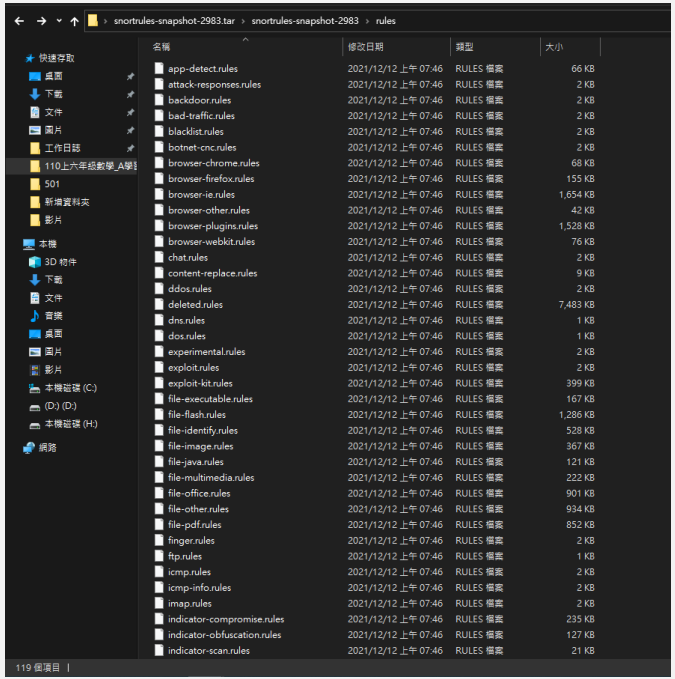
Snort v2.9

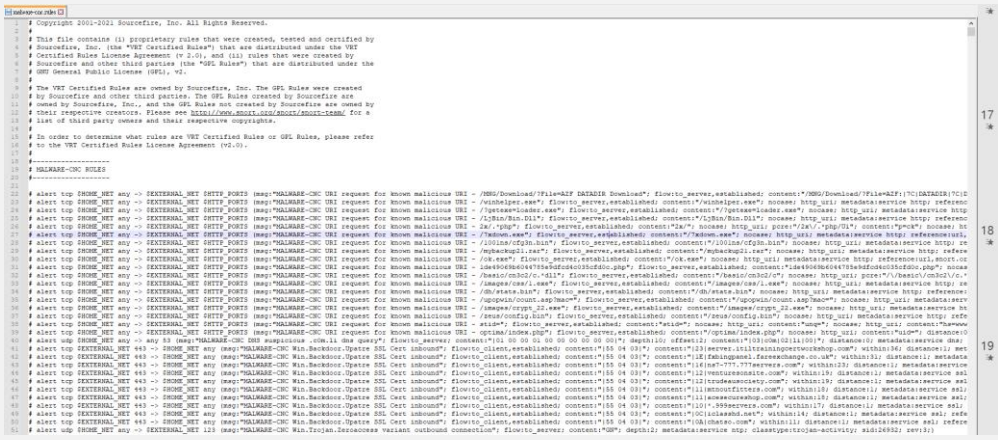
snortrules-snapshot-2983.tar.gz
snortrules-snapshot-29111.tar.gz
snortrules-snapshot-29130.tar.gz
snortrules-snapshot-29141.tar.gz
snortrules-snapshot-29151.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-29161.tar.gz
snortrules-snapshot-29170.tar.gz
snortrules-snapshot-29171.tar.gz
snortrules-snapshot-29181.tar.gz
snortrules-snapshot-29190.tar.gz



Snort rule 種類

現版本Snort Rule 包含118個分類，接近6萬條規則(58744)





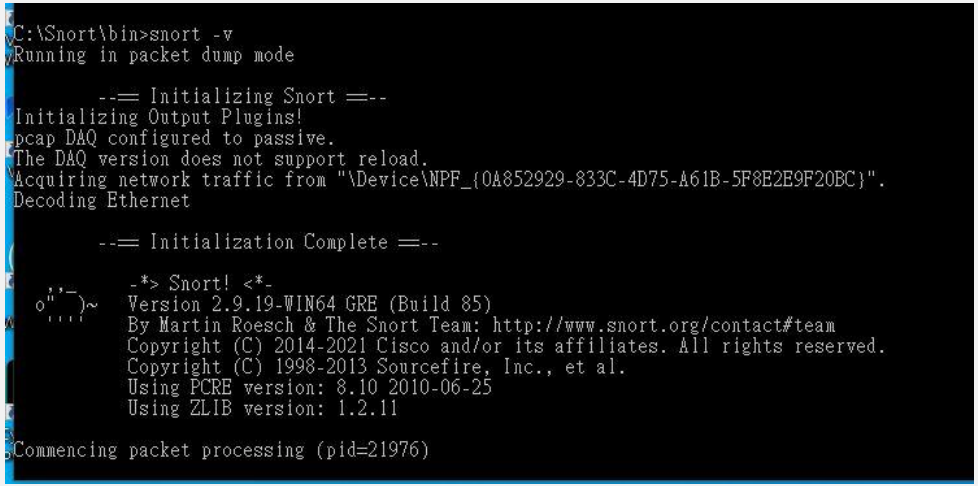
調整Snort config

1. 調整規則存取路徑變數
2. 註解尚未使用的動態函示庫
3. 修改Home_net 網段
4. 新增讀取規則種類

```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH C:\Snort\rules
var SO_RULE_PATH C:\Snort\so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

啟動Snort

指令: Snort –v　　確認Snort 版本及是否成功安裝



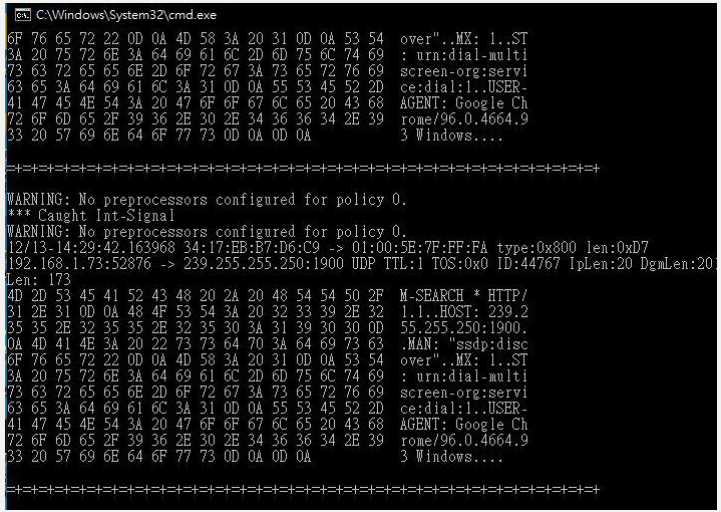
選擇偵測網卡

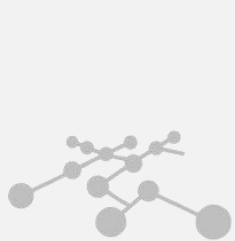
指令: Snort –W　選擇監聽的網卡介面

```
C:\Snort\bin>snort -W

           -*> Snort! <*-
  o"  )~   Version 2.9.19-WIN64 GRE (Build 85)
           By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{0A852929-833C-4D75-A61B-5F8E2E9F20BC}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{8141DB5F-369B-433E-90D1-27BBFC714B01}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{F187D9ED-B6BC-4C6F-94C6-BD16BCD0CC4B}      WAN Miniport (IP)
    4   7C:10:C9:6F:6D:DA       0000:0000:fe80:0000:0000:0000:a02f:5e45 \Device\NPF_{2A47872B-6504-49B7-84DE-C332F95963F9}      Bluetooth Device (Personal Area Network)
    5   00:50:56:C0:00:08       0000:0000:fe80:0000:0000:0000:c196:6a7d \Device\NPF_{0CB616EF-C598-4E7F-873A-753D06794703}      VMware Virtual Ethernet Adapter for VMnet8
    6   00:50:56:C0:00:01       0000:0000:fe80:0000:0000:0000:f807:33e7 \Device\NPF_{05A69261-9110-432E-9F83-39011D13279D}      VMware Virtual Ethernet Adapter for VMnet1
    7   48:4D:7E:D9:79:AB       0000:0000:fe80:0000:0000:0000:359f:5205 \Device\NPF_{1EDA4C27-A11D-4187-BACF-65C51CFE84F9}      Intel(R) Ethernet Connection I217-LM
    8   0A:00:27:00:00:15       0000:0000:fe80:0000:0000:0000:5589:c243 \Device\NPF_{BB738A84-C995-4164-B305-460E27614F3D}      VirtualBox Host-Only Ethernet Adapter
    9   00:00:00:00:00:00       disabled        \Device\NPF_Loopback    Adapter for loopback traffic capture
   10   00:09:0F:FE:00:01       0000:0000:fe80:0000:0000:0000:9d03:9961 \Device\NPF_{B1AF42E3-941D-4A4C-9068-B4DD3B8A0B9A}      Fortinet Virtual Ethernet Adapter (NDIS 6.30)
```

Sniffer mode

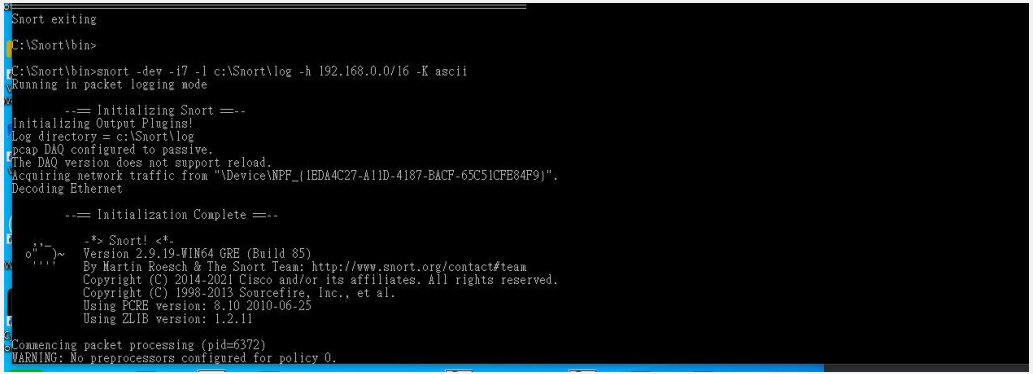
指令1: Snort –v –i1　監聽index 1網卡介面存取TCP/IP 檔頭資訊
指令2: Snort -v –d –i1監聽index 1網卡介面讀取至Layer 7資訊
指令3: Snort –v –d –e –i1監聽index 1網卡介面顯示完整封包及流向資訊





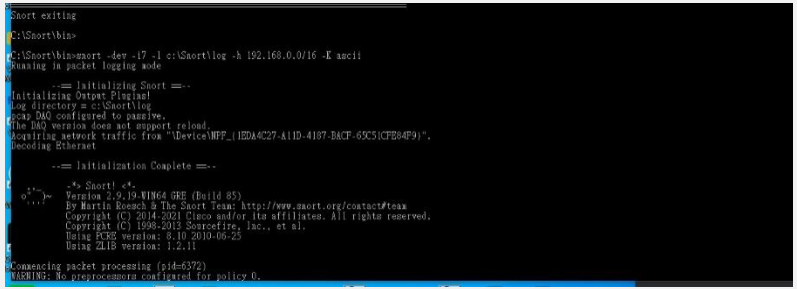
Packet Logger mode

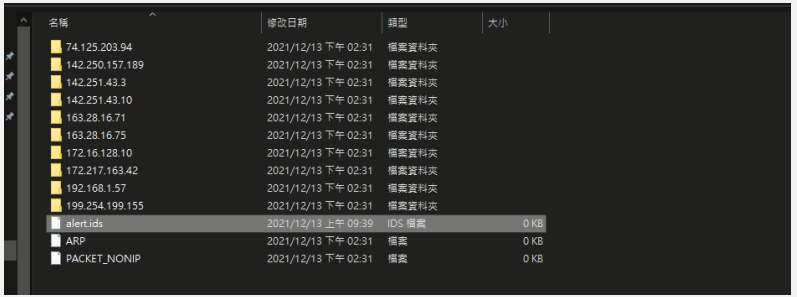
指令1: Snort –dev –i7 –l c:\Snort\log –h 192.168.0.0/16
監聽index 7網卡介面儲存完整封包及流向資訊 至c:\Snort\log 目錄下，預設檔案為tcpdump格式。
指令2: Snort –dev –i7 –l c:\Snort\log –h 192.168.0.0/16 –K ascii
監聽index 7網卡介面儲存完整封包及流向資訊 至c:\Snort\log 目錄下，儲存成ascii code格式。



Network Intrusion Detection System mode

指令: Snort –dev –i7 –l c:\Snort\log –h 192.168.0.0/16 –K ascii –c c:\Snort\etc\snort.conf
啟動NIDS模式，將網路流量與規則進行比對，並將異常告警紀錄至Snort\log 中內的alert.ids檔案。





SNORT 缺點

1. 純文字介面，操作不夠直覺
2. 規則更新需手動下載後覆蓋
3. 如需圖形化介面需安裝額外套件及sql串接

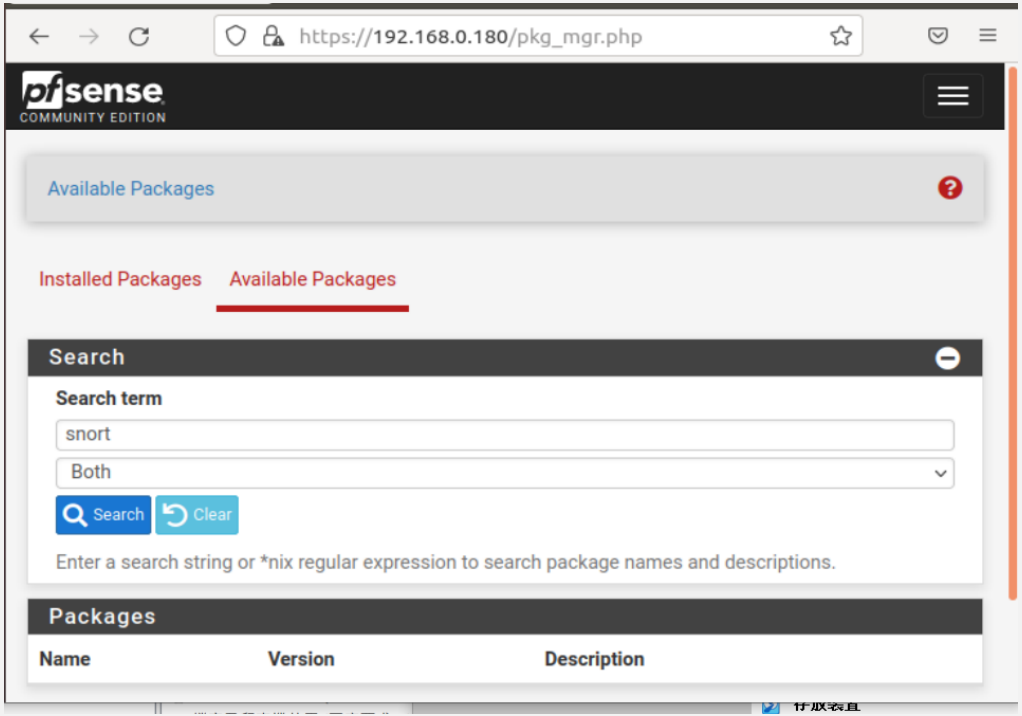
03
開源防火牆Pfsense

Pfsense 簡介

1. 以FreeBSD為基底的，免費開源定製發行版。
2. Web界面管理並包含防火牆、路由器、VPN等功能。
3. 可使用眾多套件

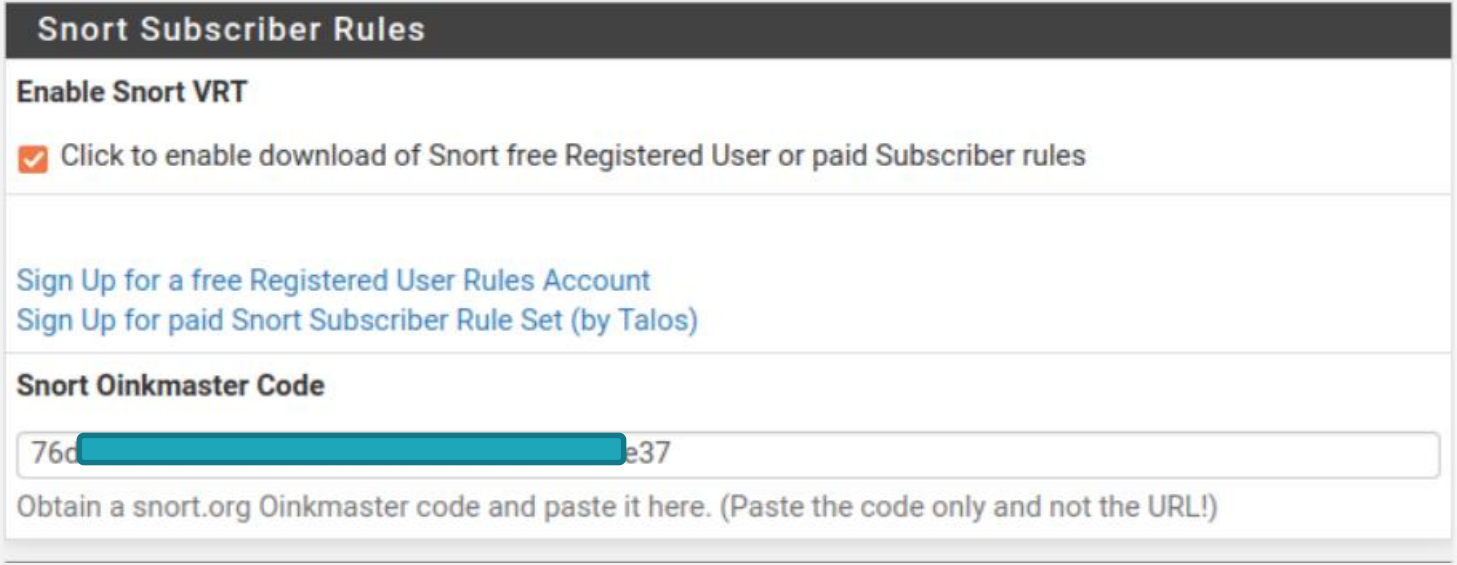
Pfsense 安裝Snort Packages

可直接透過Packages Manager 下載並安裝Snort套件



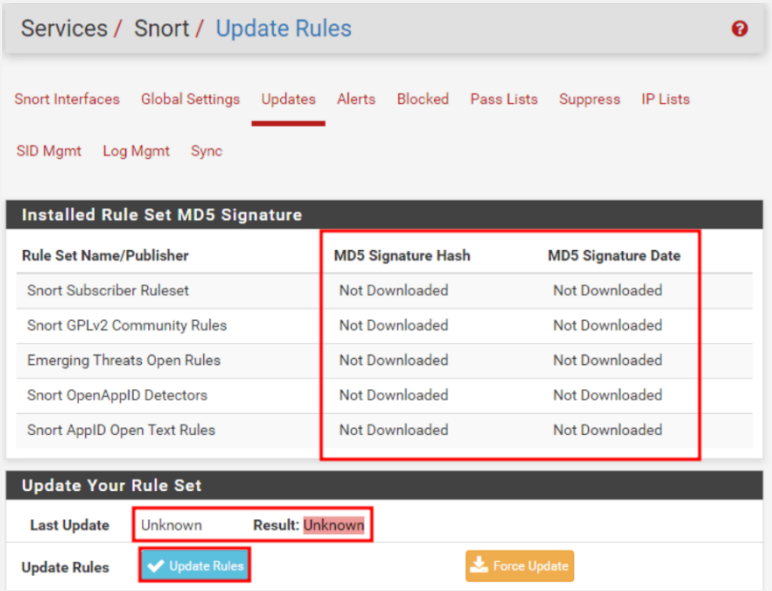
Snort Global Setting

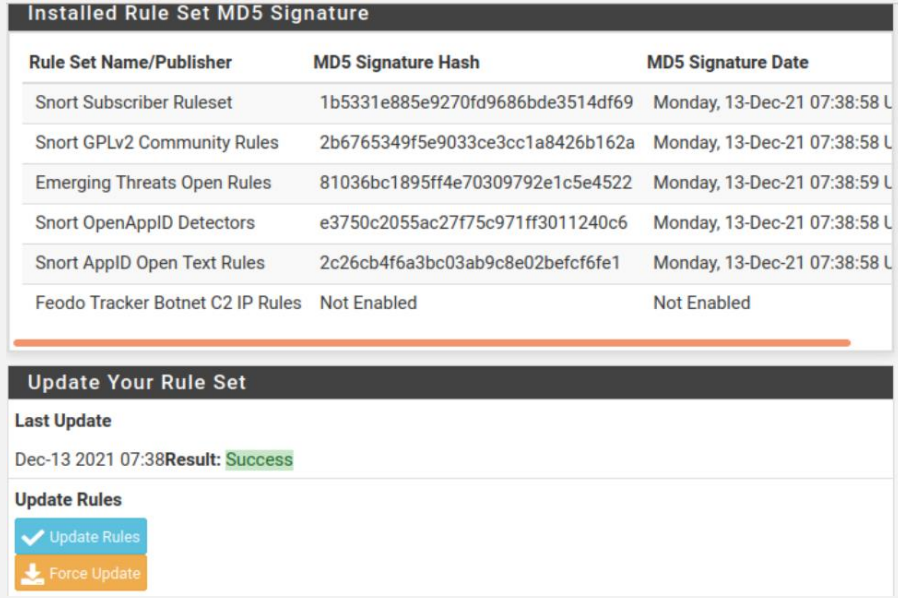
啟用 Snort VRT 透過OinkCode 存取Snort Rule，並啟用偵測規則。



更新Snort Rule

System>Snort>Update Rules 點擊更新規則





建立偵測介面

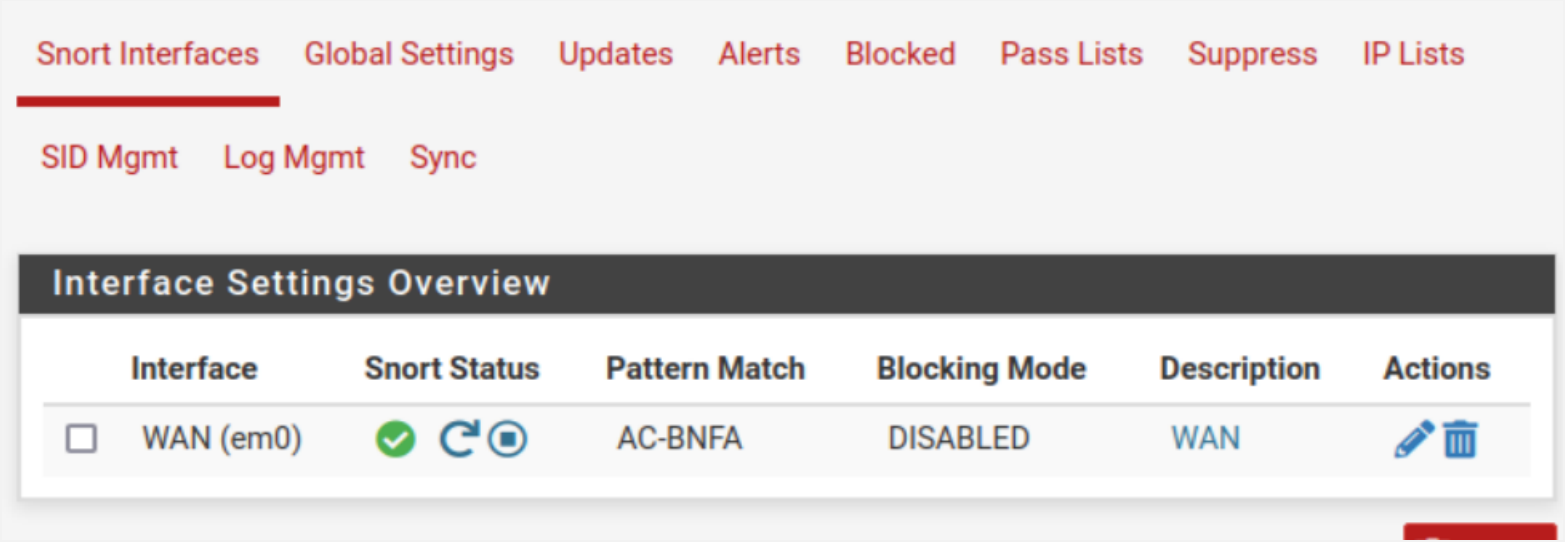
建立需使用入侵偵測的介面。

設定Preprocessor

設定需偵測的協定、porscan處理

啟用監控服務

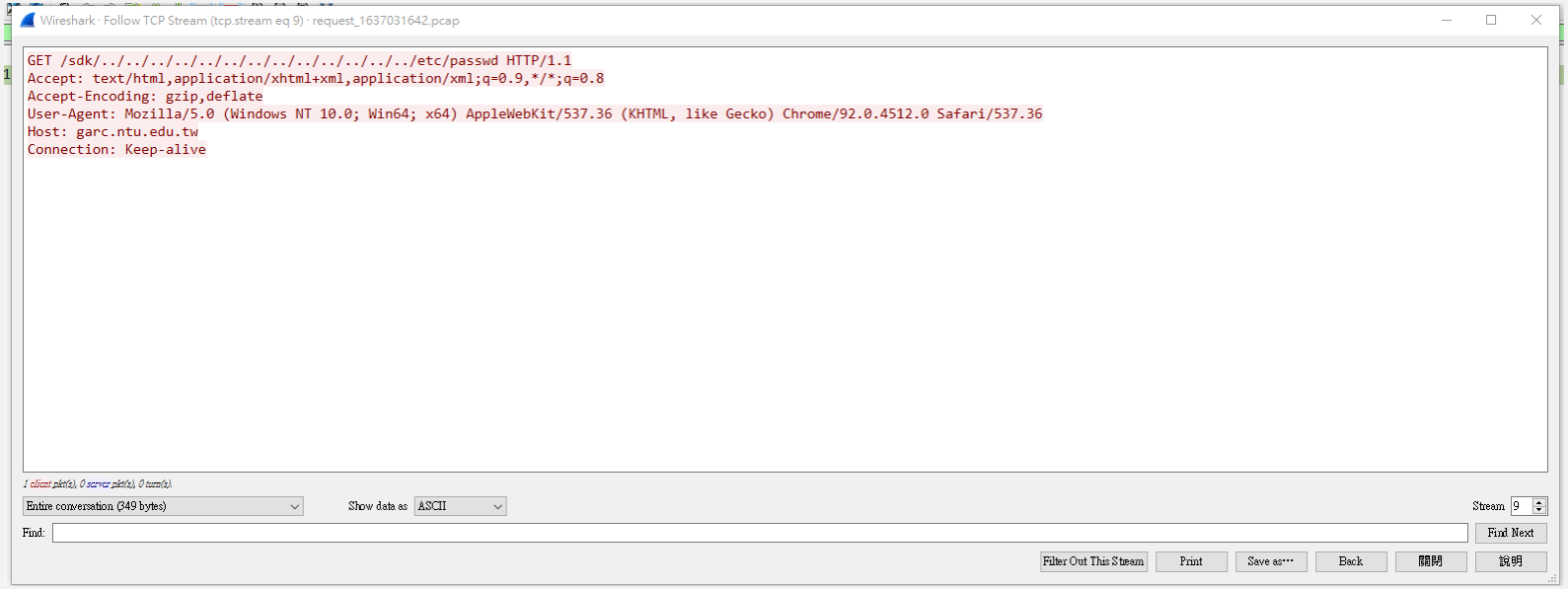
點擊播放按鈕啟用snort規則偵測。



03
Snort 案例判斷

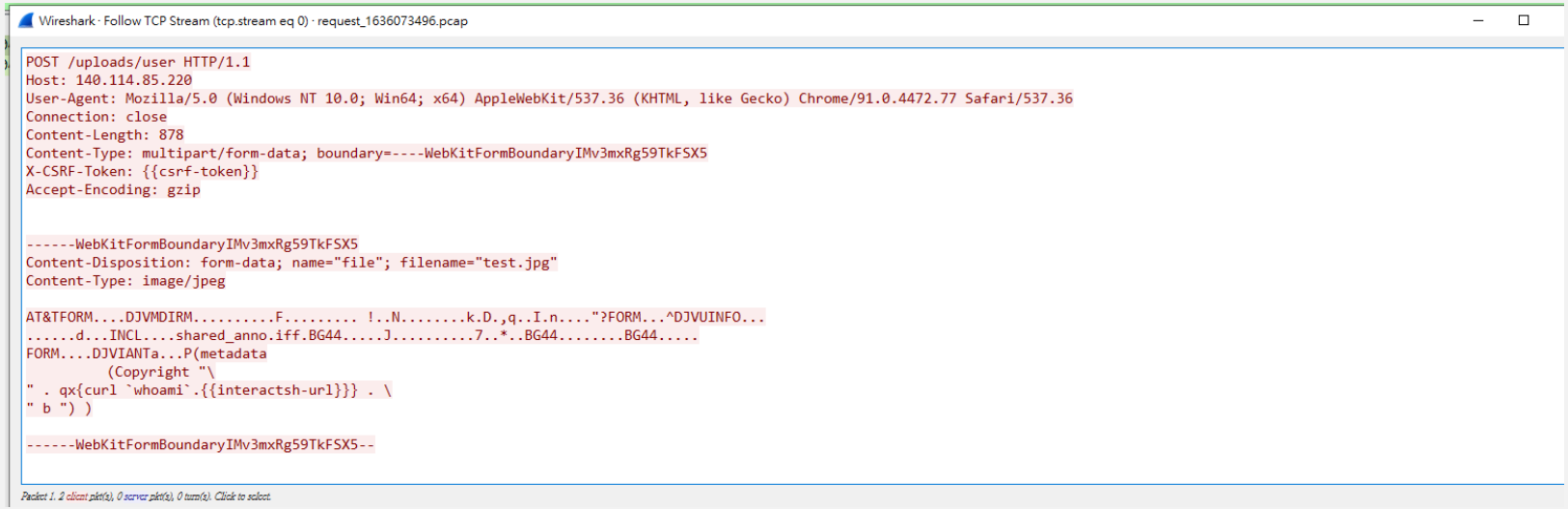
目錄遍歷案例

目錄遍歷漏洞測試。



圖片內嵌指令碼案例

試圖透過網頁上傳包含指令碼的webshell



簡報結束，感謝聆聽