整合
OpenVAS 與 shodan

ASOC

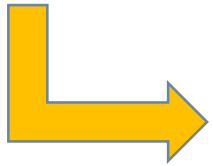
史賀文　童鵬哲

OpenVAS Brief

- 全名 (Open Vulnerability Assessment Syetem)
- Nessus 轉為商業版本後出現的分支。
- 以Nessus為基礎開發。
- OpenVAS 為一套漏洞掃描及管理解決方案的一個框架。
- OpenVAS 基於NVTs Feed 資料庫，進行弱點掃描。
- NVTs 是基於 NASL scripts 所撰寫之弱點測試資料庫。
- 目前提供了約7萬個弱點掃描。

OpenVAS 版本

- 商業版 Greenbone Security Manager (GSM)
- 免費版 Greenbone Community Edition (GCE)
- 免費版約只有商業版 70% 的部分 Feed

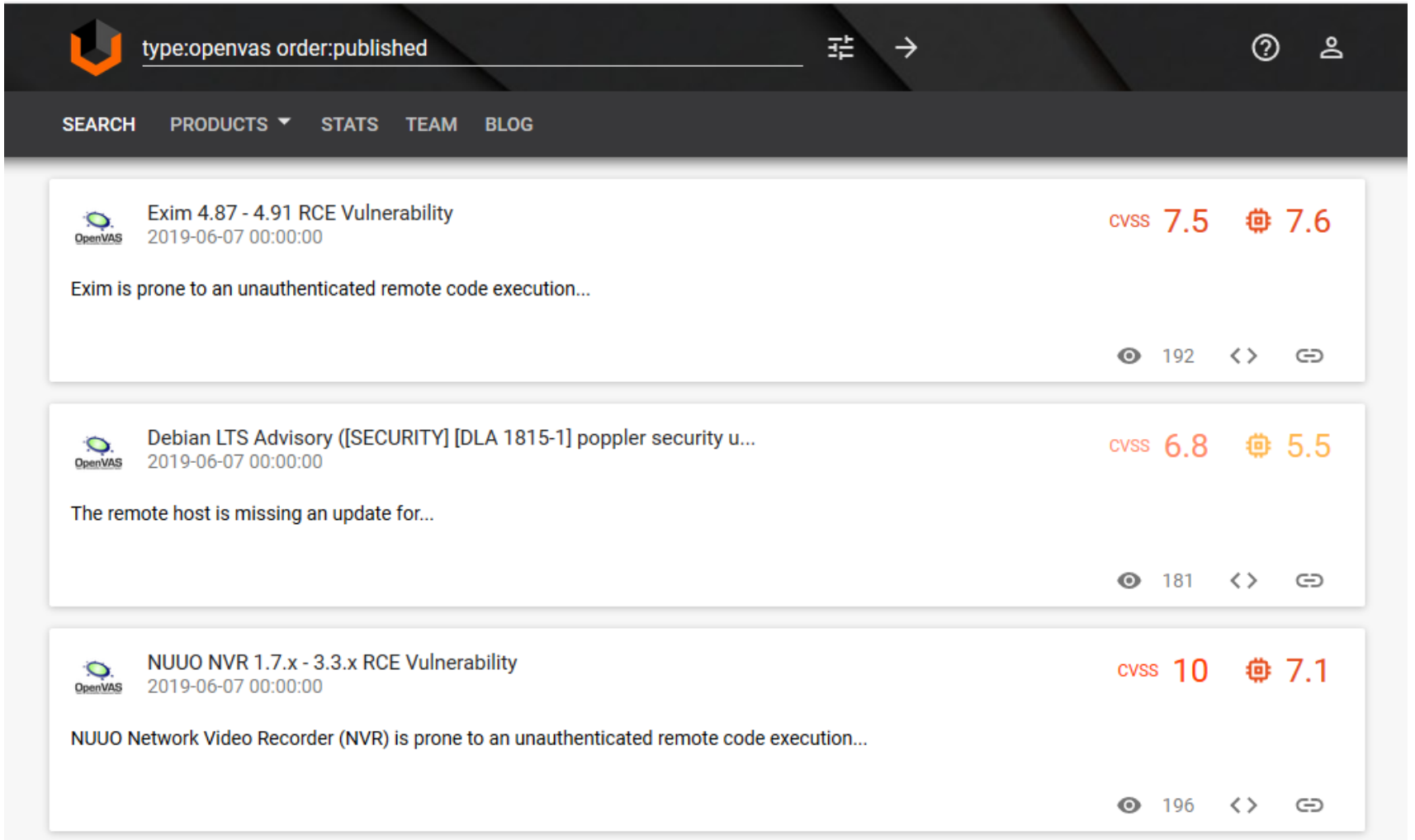


- Generally, all Enterprise-grade products and all OT (i.e. ICS/SCADA) products
- MS Windows Server and back office solutions (e.g. SharePoint, SQL Server, etc.)
- Products from Palo Alto Networks, Cisco, Juniper Networks and Fortinet
- Oracle Solaris IBM WebSphere products (i.e. IBM WebSphere Application Server)
- Lotus Notes or SAP products
- VMWare paid products

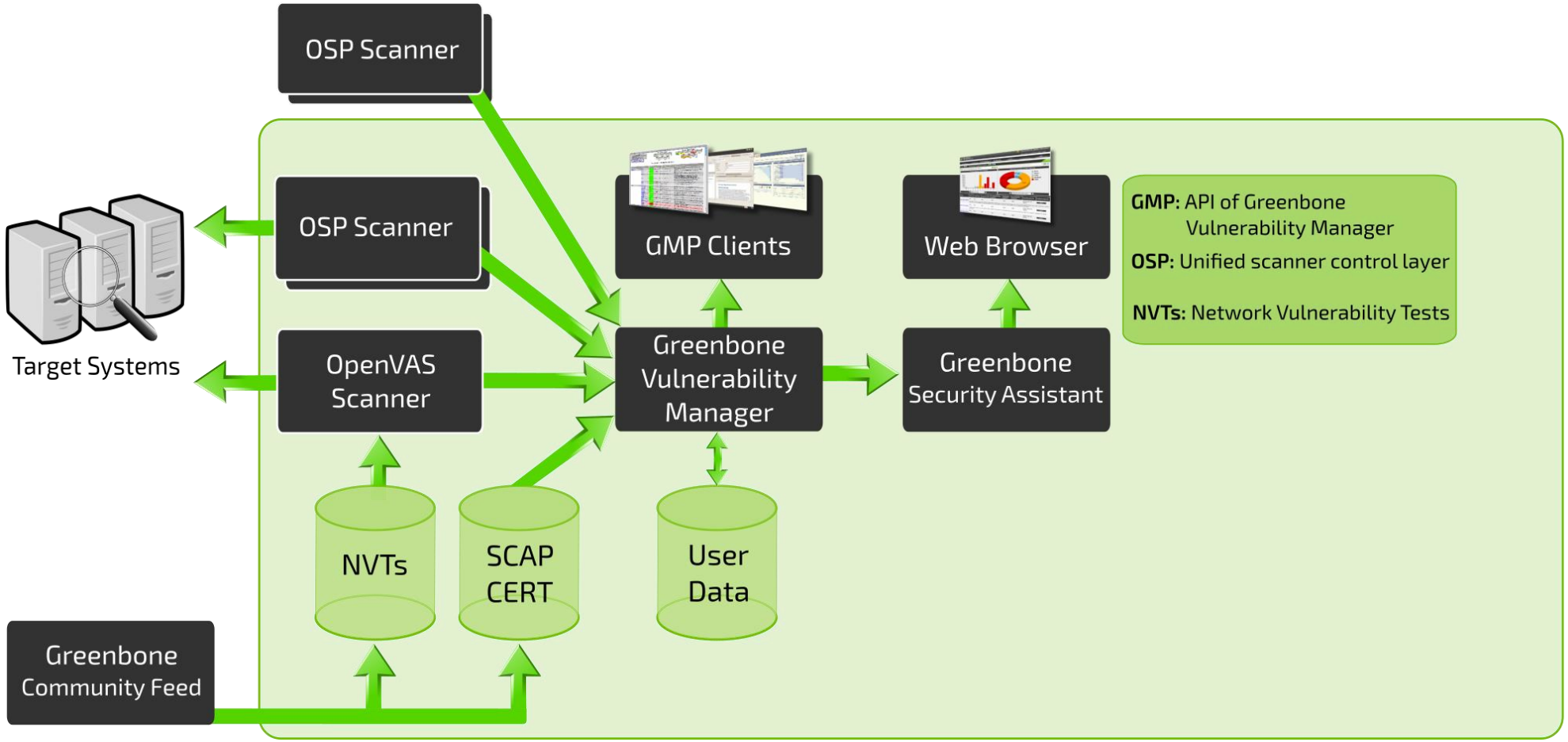
Features	Greenbone Security Feed	Greenbone Community Feed
NVTs included	Every NVT	Only basic NVTs
Quality Assurance (QA)	Consistent	Variable
Availability	Assured with SLA	No promise
Fixes / Improvements	Assured with SLA	No promise
Support	Assured with SLA	Via community on voluntary basis
Updates	Constantly / daily	Constantly / daily, but without enterprise features
Transfer	Encrypted	Unencrypted
NVT Signatures	SLA for QA / Fixes	Transfer Integrity

Reference : Greenbone Networks - The Different Flavors of Greenbone's Technology

vulners.com

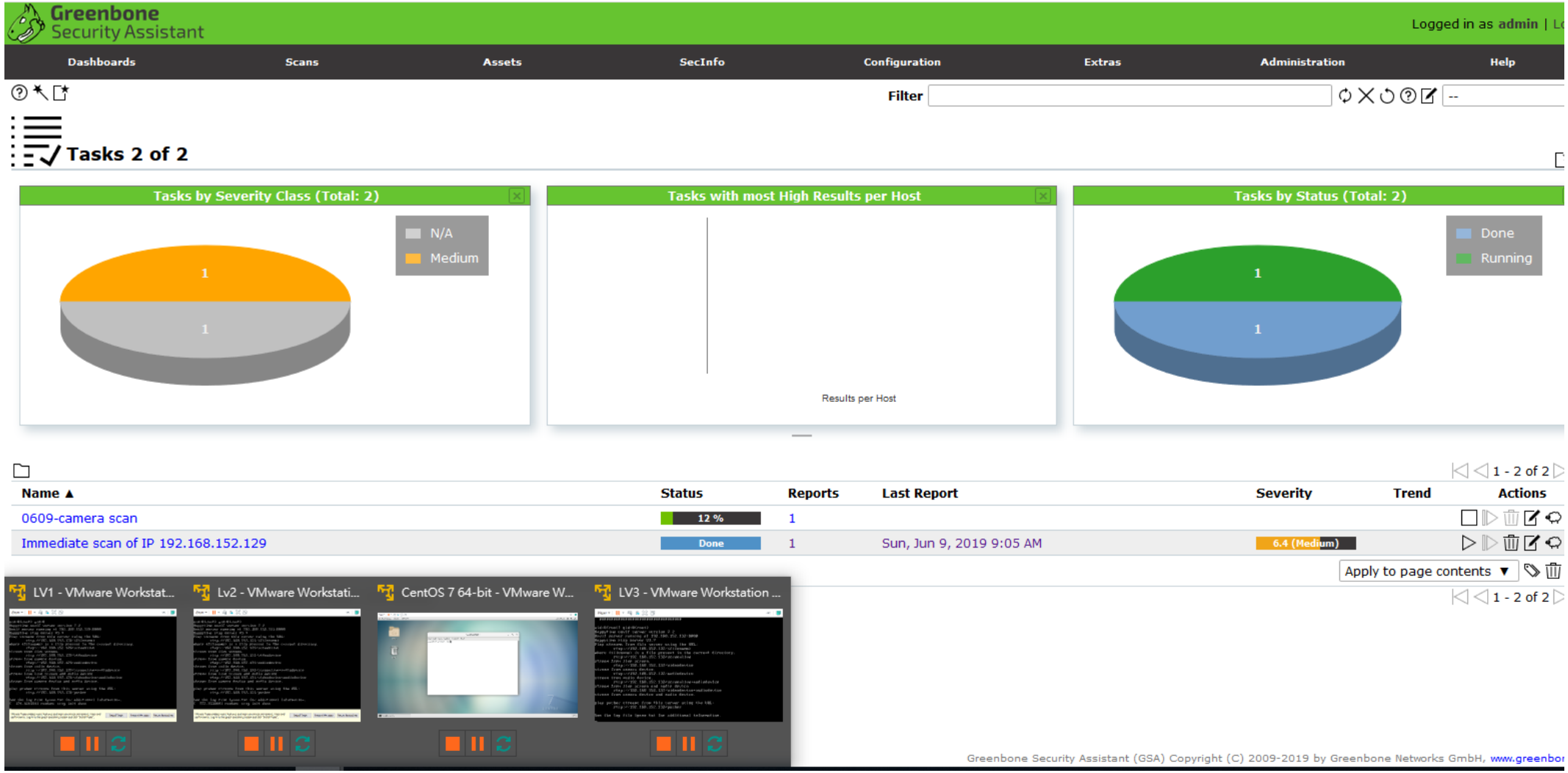

type:openvas order:published
SEARCH
PRODUCTS
STATS
TEAM
BLOG
Exim 4.87 - 4.91 RCE Vulnerability
2019-06-07 00:00:00
CVSS 7.5
7.6
Exim is prone to an unauthenticated remote code execution...
192
Debian LTS Advisory ([SECURITY] [DLA 1815-1] poppler security u...
2019-06-07 00:00:00
CVSS 6.8
5.5
The remote host is missing an update for...
181
NUUO NVR 1.7.x - 3.3.x RCE Vulnerability
2019-06-07 00:00:00
CVSS 10
7.1
NUUO Network Video Recorder (NVR) is prone to an unauthenticated remote code execution...
196

OpenVAS 架構



Reference : https://www.greenbone.net/en/community-edition/

掃描測試


Greenbone
Security Assistant
Logged in as admin
Dashboards
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help
Filter
Tasks 2 of 2
Tasks by Severity Class (Total: 2)
N/A
Medium
1
1
Tasks with most High Results per Host
Results per Host
Tasks by Status (Total: 2)
Done
Running
1
1
1 - 2 of 2
Name
Status
Reports
Last Report
Severity
Trend
Actions
0609-camera scan
12 %
1
Immediate scan of IP 192.168.152.129
Done
1
Sun, Jun 9, 2019 9:05 AM
6.4 (Medium)
Apply to page contents
1 - 2 of 2
LV1 - VMware Workstat...
Lv2 - VMware Workstati...
CentOS 7 64-bit - VMware W...
LV3 - VMware Workstation ...
Greenbone Security Assistant (GSA) Copyright (C) 2009-2019 by Greenbone Networks GmbH, www.greenbo

Scanning results

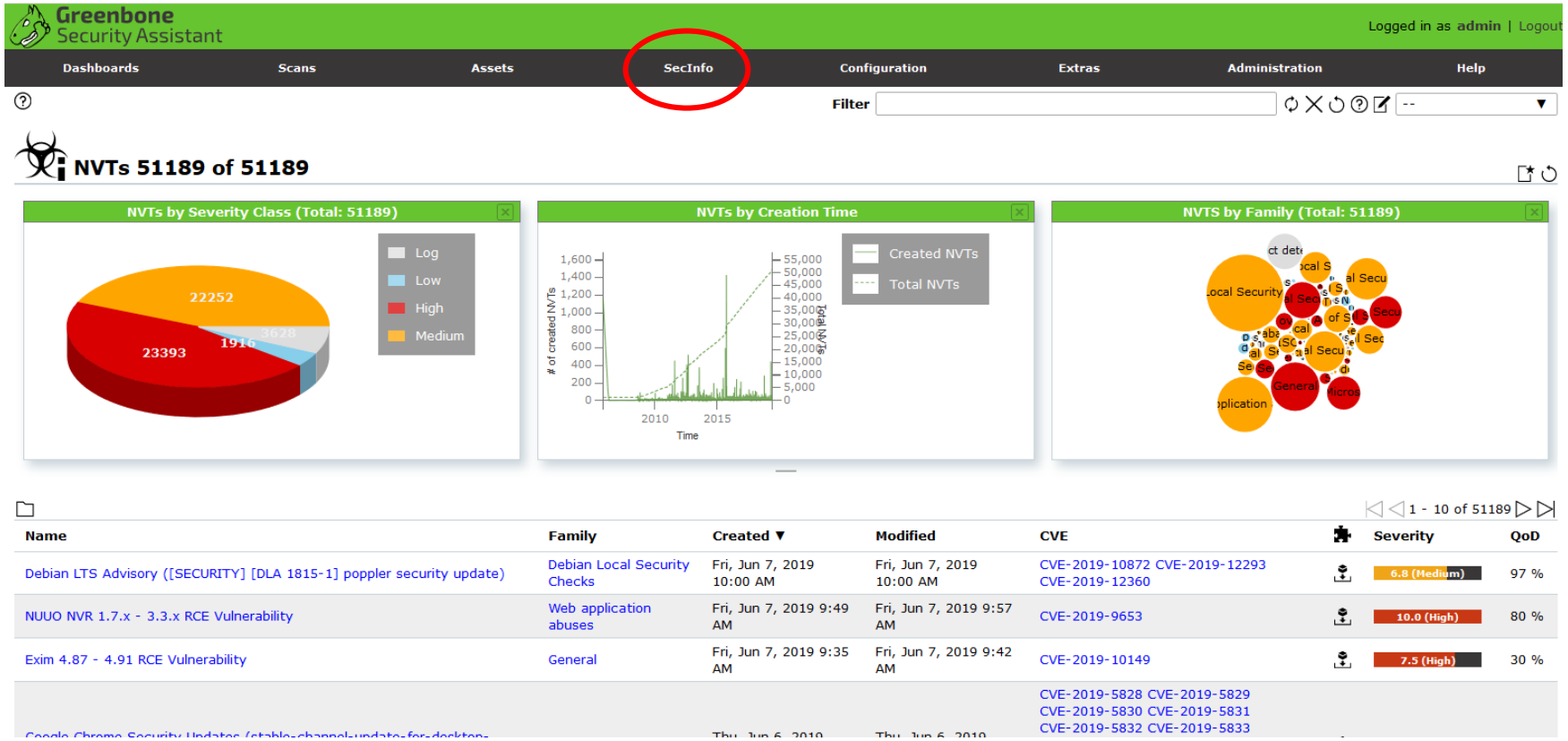
Information | Results (99 of 99) | Hosts (3 of 3) | Ports (6 of 6) | Applications (1 of 1) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (4 of 4) | User Tags (0)

1 - 10 of 99

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.152.129		21/tcp	Sun, Jun 9, 2019 10:16 AM
FTP Writeable Directories	5.0 (Medium)	80 %	192.168.152.129		21/tcp	Sun, Jun 9, 2019 10:16 AM
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.152.129		80/tcp	Sun, Jun 9, 2019 10:13 AM
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.152.129		21/tcp	Sun, Jun 9, 2019 10:15 AM
Telnet Unencrypted Cleartext Login	4.8 (Medium)	70 %	192.168.152.129		23/tcp	Sun, Jun 9, 2019 10:15 AM
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	192.168.152.131		443/tcp	Sun, Jun 9, 2019 10:15 AM
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	192.168.152.132		443/tcp	Sun, Jun 9, 2019 10:14 AM
TCP timestamps	2.6 (Low)	80 %	192.168.152.129		general/tcp	Sun, Jun 9, 2019 10:15 AM
TCP timestamps	2.6 (Low)	80 %	192.168.152.131		general/tcp	Sun, Jun 9, 2019 10:15 AM
TCP timestamps	2.6 (Low)	80 %	192.168.152.132		general/tcp	Sun, Jun 9, 2019 10:15 AM

NVT
(Network Vulnerability Test)

- Openvas 用於滲透測試，檢測弱點之資料庫，包含程式碼及參考資料。
- https://secinfo.greenbone.net/login



NASL
(Nessus Attack Scripting Language)

- NVT 所用於弱點測試的程式碼腳本

- Example：

  Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability (KB4500331)

- CVE-2019-0708

- https://vulners.com

- Linux (CentOS 7) => /var/lib/openvas/plugins/2019/microsoft/gb_ms_kb4500331.nasl

```
include("smb_nt.inc");
include("version_func.inc");
include("secpod_reg.inc");
include("secpod_smb_func.inc");


sysPath = smb_get_system32root();
if(!sysPath ){
  exit(0);
}

fileVer = fetch_file_version(sysPath:sysPath, file_name:"\drivers\Termdd.sys");
if(!fileVer){
  exit(0);
}

if(hotfix_check_sp(xp:4) > 0)
{
  if(version_is_less(version:fileVer , test_version:"5.1.2600.7701"))
  {
    report = report_fixed_ver(file_checked:sysPath + "\drivers\Termdd.sys",
                              file_version:fileVer, vulnerable_range:"Less than 5.1.2600.7701");
    security_message(data:report);
    exit(0);
  }
}

else if(hotfix_check_sp(win2003:3, win2003x64:3, xpx64:3) > 0){

  if(version_is_less(version:fileVer , test_version:"5.2.3790.6787"))
  {
    report = report_fixed_ver(file_checked:sysPath + "\drivers\Termdd.sys",
                              file_version:fileVer, vulnerable_range:"Less than 5.2.3790.6787");
    security_message(data:report);
    exit(0);
  }
```

NVT for CVE-2019-0708

1 - 1 of 1

Name	Family	Created ▼	Modified	CVE	Severity	QoD
Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability (KB4500331)	Windows : Microsoft Bulletins	Fri, May 17, 2019 5:57 PM	Wed, May 22, 2019 3:03 PM	CVE-2019-0708	10.0 (High)	80 %

Apply to page contents ▼

(Applied filter: ~"Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability" sort-reverse=created rows=10 first=1)

1 - 1 of 1

Vulnerable Products

cpe:/o:microsoft:windows_7:-:sp1
cpe:/o:microsoft:windows_server_2003:-:sp2:~~~~x64~
cpe:/o:microsoft:windows_server_2003:-:sp2:~~~~x86~
cpe:/o:microsoft:windows_server_2003:r2:sp2
cpe:/o:microsoft:windows_server_2008:-:sp2
cpe:/o:microsoft:windows_server_2008:r2:sp1:~~~~itanium~
cpe:/o:microsoft:windows_server_2008:r2:sp1:~~~~x64~
cpe:/o:microsoft:windows_vista:-:sp2
cpe:/o:microsoft:windows_xp:-:sp2:~~professional~~x64~
cpe:/o:microsoft:windows_xp:-:sp3:~~~~x86~

NVTs addressing this CVE

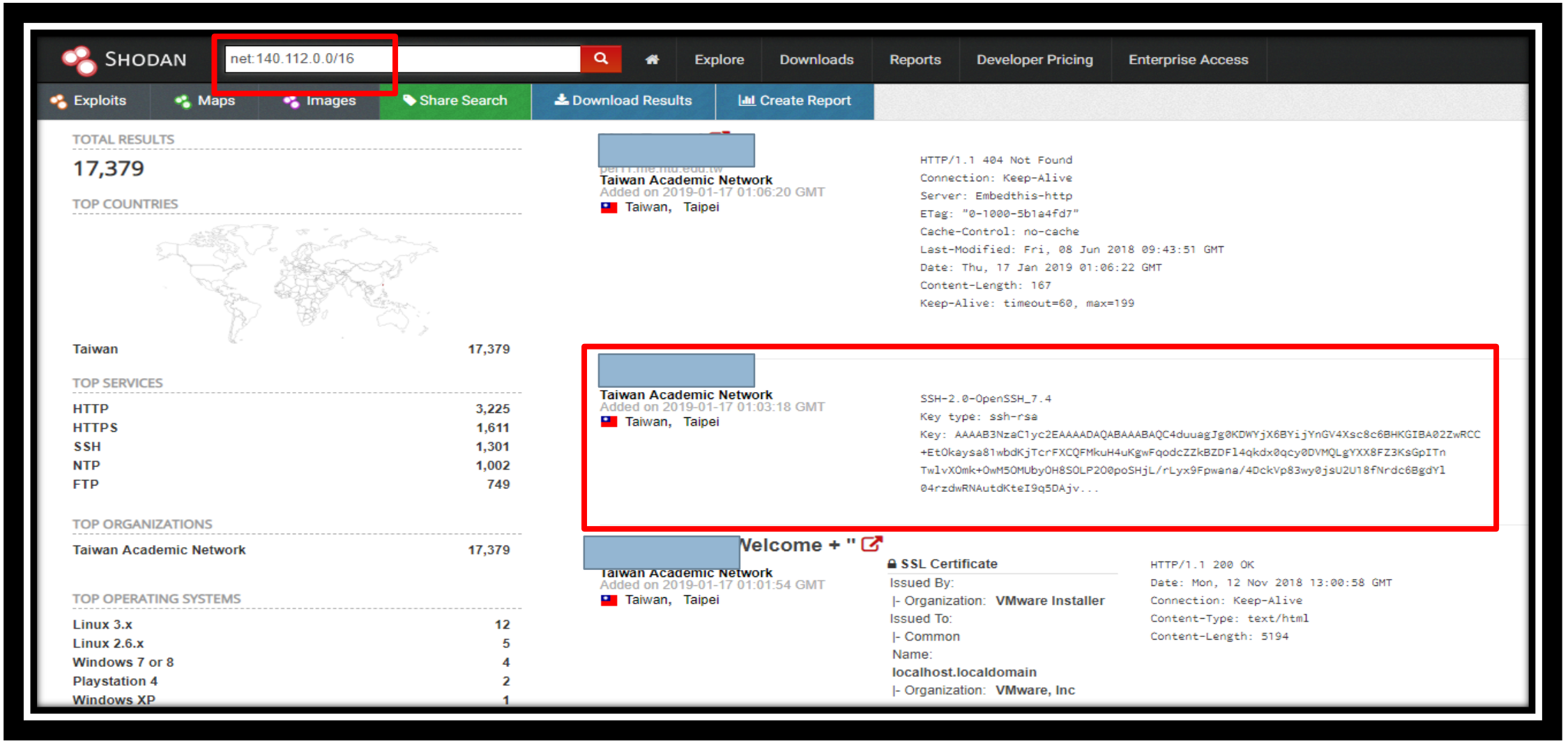
Microsoft Windows Multiple Vulnerabilities (KB4499149)
Microsoft Windows Multiple Vulnerabilities (KB4499164)
Microsoft Windows Remote Desktop Service Remote Code Execution Vulnerability (KB4500331)

11

實際環境中的實作

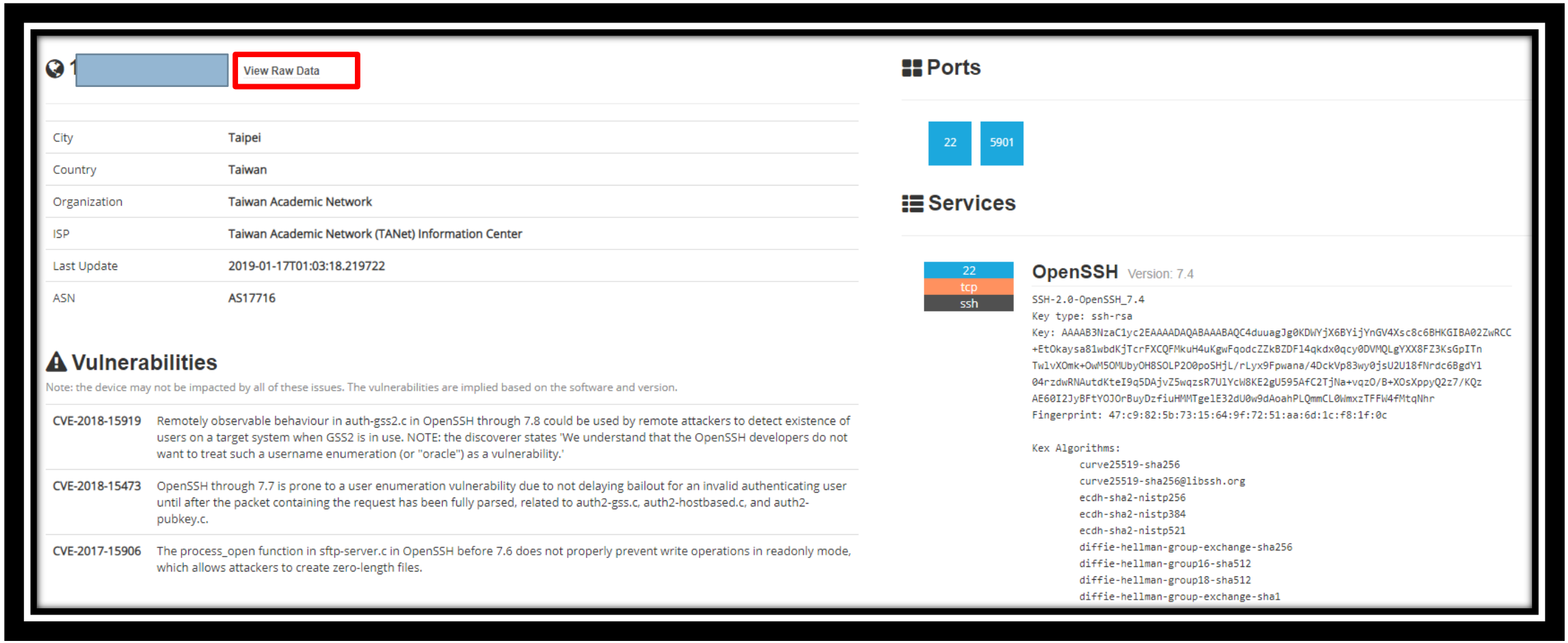
IOT分類 - 資料來源

Shodan就像Google一樣，可以利用關鍵字尋找需要的資料。



IOT分類 - 資料來源

承上一頁，點擊進入觀看該IP的資料。點ViewRawData可以看到更詳細資料。



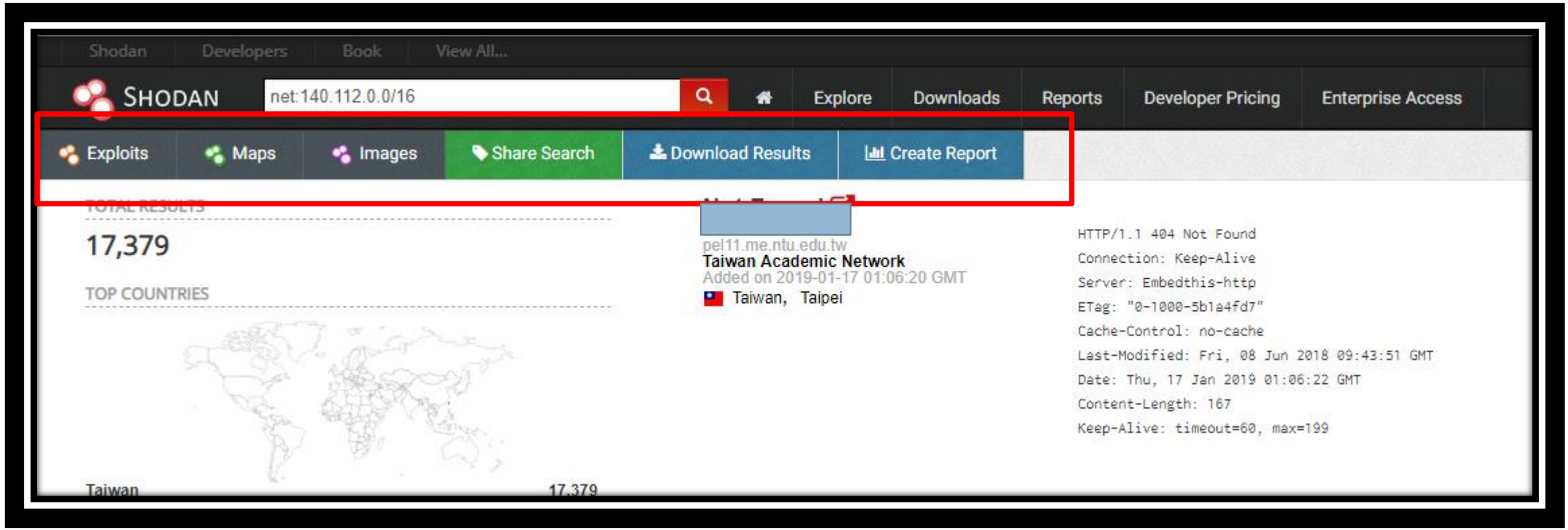
IOT分類 - 資料來源

下圖為ViewRawData資料。Shodan內建約有80個標籤，如紅框處。
標籤數量因每台主機開啟port和CVE數量不同等，而有所增減。

Property Name	Value
area_code	null
asn	AS17716
city	Taipei
country_code	TW
country_code3	TWN
country_name	Taiwan
data.0._shodan.crawler	8cd926590a400feb4b683f8337a77287ddf3d2c7
data.0._shodan.id	null
data.0._shodan.module	ssh
data.0._shodan.ptr	True
data.0.cpe	['cpe:/a:openbsd:openssh:7.4']
data.0.data	SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC4duuagJg0KDWYjX6BYijYnGV4Xsc8c6BHKGIBA02ZwRCC +EtOkaysa81wbdKjTcrFXCQ TwlvXOmk+OwM5OMUbyOH8SOLP2O0poSHjL/rLyx9Fpwana/4DckVp83wy0jsU2U18fNrdc6BgdY1 04rzdwRNAutdKteI9q5DAjvZ5wqzsR7UlYcW8KE2gU595AfC2TjNa+vqzO/B+XOsXp Fingerprint: 47:c9:82:5b:73:15:64:9f:72:51:aa:6d:1c:f8:1f:0c Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-gro sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com

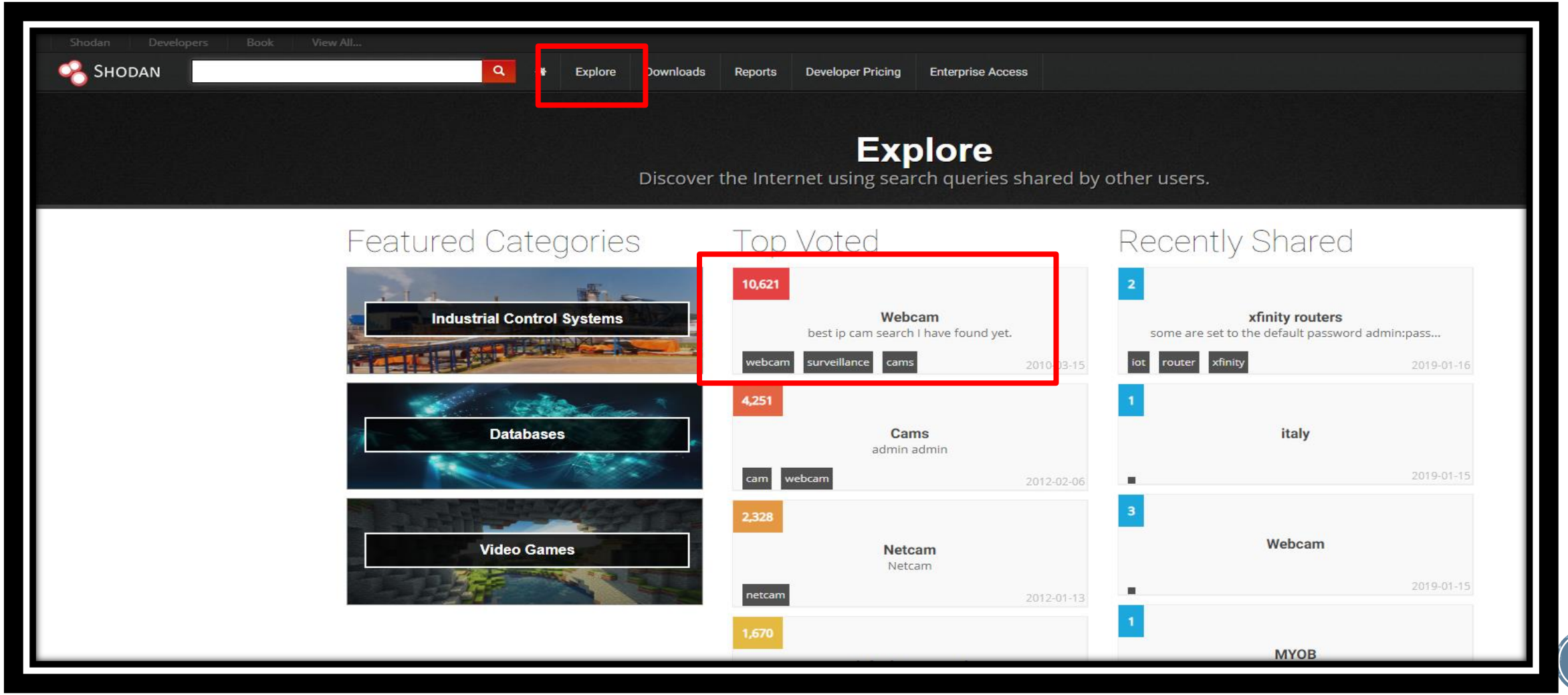
IOT分類 - 資料來源

搜尋到的資料，可以下載、分享等，並用於大數據分析。



IOT分類 - 資料來源

Shodan本身有提供一些**Explore**資料可以參考。



IOT分類 – 第一次過濾

NTU資料如下，ASOC分析歸類這些資料是否可以辨識為IOT。
並撰寫成Python過濾條件。


NTU_Nov14th.json - 記事本

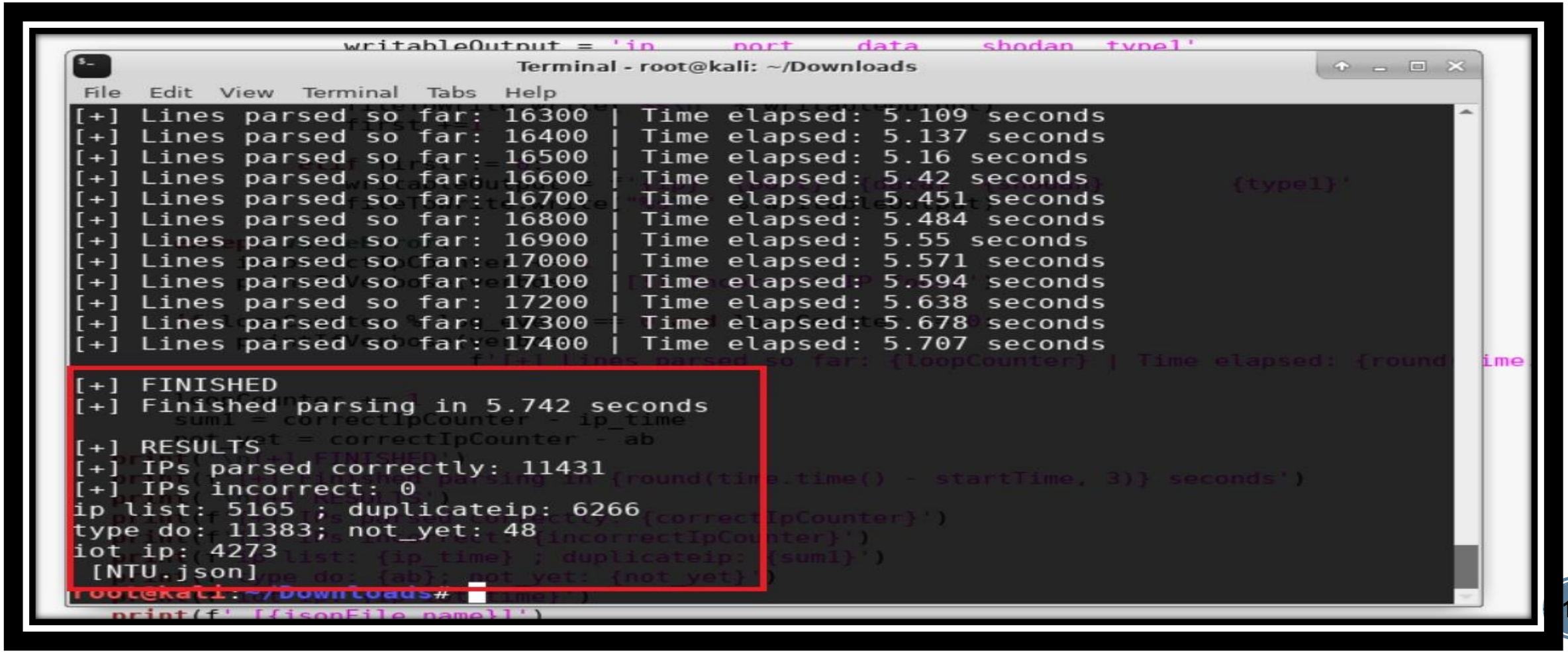
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

{"domains": ["ntu.edu.tw"], "_shodan": {"module": "http", "id": "bad000b6-563b-49ca-8a5c-72760799f2d8", "crawler": "62861a86c4e4b71dceed5113ce9593b98431f89a", "options": {}}, "os": null, "hostnames": ["xdn33o251.ee.ntu.edu.tw"], "ip_str": "[redacted]", "opts": {}, "link": "Ethernet or modem", "hash": -1761809039, "timestamp": "2018-11-14T00:25:51.878198", "port": 80, "org": "Taiwan Academic Network", "isp": "Taiwan Academic Network (TANet) Information Center", "ip": [redacted] "product": "Cisco IOS http config", "location": {"dma_code": null, "region_code": "03", "area_code": null, "city": "Taipei", "country_code3": "TWN", "latitude": 25.047799999999995, "country_name": "Taiwan", "postal_code": null, "longitude": 121.53179999999998, "country_code": "TW"}, "cpe": ["cpe:/o:cisco:ios"], "asn": "AS17716", "data": "HTTP/1.1 401 Unauthorized\r\nDate: Wed, 14 Nov 2018 00:16:39 GMT\r\nServer: cisco-IOS\r\nConnection: close\r\nAccept-Ranges: none\r\nWWW-Authenticate: Basic realm=\"level_15_access\"\r\n\r\n", "transport": "tcp", "http": {"components": {}, "robots_hash": null, "title": null, "securitytxt": null, "host": "[redacted]", "robots": null, "redirects": [], "html_hash": 819126370, "location": "/", "server": "cisco-IOS", "sitemap_hash": null, "sitemap": null, "favicon": null, "html": "401 Unauthorized\r\n", "securitytxt_hash": null}} {"domains": [], "ftp": {"features_hash": null, "features": {}, "anonymous": false}, "os": null, "hostnames": [], "asn": "AS17716", "opts": {}, "timestamp": "2018-11-14T00:24:43.952035", "version": "1.0", "_shodan": {"module": "ftp", "id": "f2ce95dc-0269-41e7-961e-83ce2dfe9576", "crawler": "93b89eaabe5431ba7f29e8d442c5903ef6e244f6", "options": {}}, "hash": -1608643738, "port": 21, "org": "Taiwan Academic Network", "isp": "Taiwan Academic Network (TANet) Information Center", "product": "NET+ARM ftpd", "location": {"dma_code": null, "region_code": "03", "area_code": null, "city": "Taipei", "country_code3": "TWN", "latitude": 25.047799999999995, "country_name": "Taiwan", "postal_code": null, "longitude": 121.53179999999998, "country_code": "TW"}, "transport": "tcp", "data": "220 NET+ARM FTP Server 1.0 ready.\r\n530 The user name is not valid.\r\n502 Command not implemented.\r\n502 Command not implemented.", "ip": [redacted] ip_str": "1[redacted]"} {"domains": [], "_shodan": {"module": "https", "id": "2b53d7e3-30a9-4db7-bffc-eebbdf20757c", "crawler": "5faf2928ceb560cb4276cc1b4660b2d763cc6397", "options": {}}, "tags": ["self-signed"], "hostnames": [], "ssl": {"chain": ["-----BEGIN CERTIFICATE-----\nMIIDMDCCAhigAwIBAgIBATANBgkqhkiG9w0BAQUFADAxMS8wLQYDVQQDEyZJT1Mt\nU2VsZi1TaWduZWQtQ2VydGlmaWNhdGUtMTE2NDgwNjE1NzAeFw0xODA5MjYwMjMz\nNDhaFw0yMDAxMDEwMDAwMDBaMDExLzAtBgNVBAMTJk1PUy1TZWxmLVNpZ251ZC1D

IOT分類 – 第一次過濾

下圖為透過ASOC自寫的Python過濾出IOT的資料，

全部約17400筆資料，過濾掉非IOT 後剩11431筆。共5165個IP，重複6266筆，已定義11383個，未定義48，IOT設備約有4273個。



IOT研究分類 – Python IOT標籤設定

根據shodan裡面的資料判斷是否為IOT。(陸續增加及調整中)

```
elif data.find("linux") >= 1 or shodan.find("linux") >= 1 :
    typel = str('linux')

elif data.find("canon") >= 1 or
    typel = str('canon')

elif data.find("d-link") >= 1 o
    typel = str('d-link')

elif data.find("tp-link") >= 1
    typel = str('tp-link')

elif data.find("http/1.1 401 una
    typel = str('unknow but can

elif data.find("moxa") >= 1 :
    typel = str('Moxa')

elif shodan.find("ethernetip")
    typel = str('ethernetip')
```

```
elif port == str(161) and shodan.find(
    typel = str('wirekess')

elif port != str(161) and shodan.find(
    typel = str('snmp')

elif shodan.find("apple-airport-admin")
    typel = str('apple-airport')

elif shodan.find("iscsi") >= 1 :
    typel = str('online drive')

elif shodan.find("telnet") >= 1 or port
    typel = str('Can telnet')

elif data.find("http") >= 1 and data.fi
    typel = str('web login')

elif data.find("ssh") >= 1 :
    typel = str('ssh')

elif port == str(2000) :
    typel = str('Cisco SCCP or get virus
```

```
elif data.find("zookeeper") >= 1 or shodan.find("zookeeper") >= 1
    typel = str('zookeeper')

elif data.find("imap") >= 1 or shodan.find("imap") >= 1  :
    typel = str('imap')

elif data.find("netsarang") >= 1  :
    typel = str('netsarang web server')

elif data.find("vpn") >= 1  :
    typel = str('vpn')

elif shodan.find("coin") >= 1  :
    typel = str('mining serveer')

elif port == str(389) :
    typel = str('ldap')

elif port == str(503) or shodan.find("modbus") >= 1  :
    typel = str('modbus')

elif data.find("amqp") >= 1 or shodan.find("amqp") >= 1 :
    typel = str('amqp')

elif shodan.find("torrent") >= 1 :
    typel = str('BT')
```

IOT研究分類 – Python IOT標籤設定

IOT標籤也有參考網路上資料。

```
elif data.find("goahead") >= 1 :
    typel = str('goahead')
    #https://research.checkpoint.com/new-iot-botnet-storm-coming/
elif data.find("avtech") >= 1 :
    typel = str('avtech')
    #https://research.chec
elif data.find("mikrotik"
    typel = str('mikrotik'
    #https://research.chec
elif data.find("linksys")
    typel = str('linksys')
    #https://research.chec
elif data.find("synology"
    typel = str('synology'
    #https://research.chec
```

A New IoT Botnet Storm is Coming

Key Points:

- A massive Botnet is forming
- An estimated million organiz
  amount actually infected.
- The Botnet is recruiting IoT d
  attack.

Vendor	Protection Name	Seen in the Context of the current Attack?
GoAhead	Wireless IP Camera (P2P) WIFICAM Cameras Information Disclosure	+
	Wireless IP Camera (P2P) WIFICAM Cameras Remote Code Execution	+
	D-Link 850L Router Remote Code Execution	+
	D-Link DIR800 Series Router Remote Code Execution	+
	D-Link DIR800 Series Router Information Disclosure	+
	D-Link 850L Router Remote Unauthenticated Information Disclosure	+
	D-Link 850L Router Cookie Overflow Remote Code Execution	+

IOT分類 – 過濾成果

使用Python過濾成果如下，D-link為Python自動標記的標籤

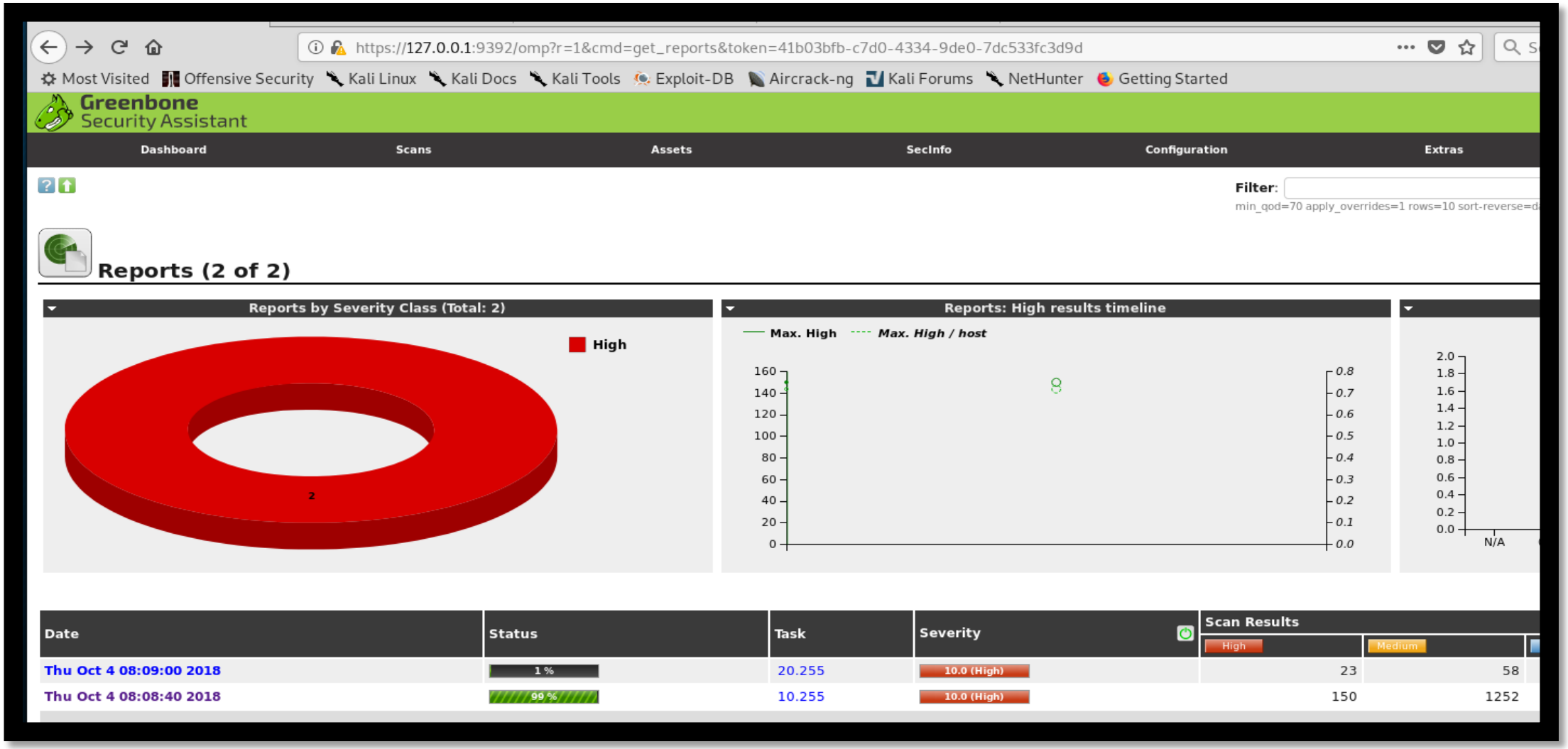
IOT分類 – 過濾成果

過濾後的EXCEL檔案，11個欄位

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	ip	port	data	shodan:mo	product	title	issuer	cpe	devicetype	server	type1			
2	140.11	9100	['@pjl info	['printer-jol	['epson al-c	[']	[']	[']	[']	[']	Printer			
3	140.11	49153	['http/1.1 5(	['wemo-htt	[']	[']	[']	[']	[']	[']	linux			
4	140.11	143	['* ok the n	['imap']	[']	[']	['{'cn': 'iam	[']	[']	[']	imap,mail use			
5	140.11	443	['http/1.1 4(	['https']	[']	['aicloud']	['{'cn': '192	[']	[']	['lighttpd/1	Asus aicloud, a service of asus wifi router			
6	140.11	8000	[']	['http-simpl	[']	[']	[']	[']	[']	[']	data is No data			
7	140.11	80	['http/1.1 4(	['http']	['cisco ios h	[']	[']	['['cpe:/o:c:	[']	['cisco-ios']	cisco router or switch			
8	140.11	22	['ssh-2.0-op	['ssh']	['openssh']	[']	[']	['['cpe:/a:o	[']	[']	openssh			
9	140.11	5901	['rfb 003.0(	['http-simpl	['vnc']	[']	[']	[']	[']	[']	VNC			
10	140.11	5555	['http/1.1 4(	['http-simpl	[']	['error: the	[']	[']	[']	['squid/3.3.	web login offline			
11	140.11	8000	['http/1.1 2(	['http-simpl	['nginx']	['cmdmmet	[']	['['cpe:/a:ig	[']	['nginx']	synology,NAS			
12	140.11	44818	['product n:	['ethernetip	[']	[']	[']	[']	[']	[']	ethernetip, power monitor			
13	140.11	8008	['http/1.1 3(	['http-simpl	[']	[']	[']	[']	[']	[']	online driver			
14	140.11	80	['http/1.0 4(	['http']	[']	['401 unaut	[']	[']	[']	[']	access control system			
15	140.11	2000	['\\x01\\x0(	['ikettle']	['mikrotik b	[']	[']	[']	[']	[']	Cisco SCCP or get virus			
16	140.11	80	['http/1.1 5(	['http']	['nginx']	['502 bad g	[']	['['cpe:/a:ig	[']	['nginx/1.3	synology,NAS			
17	140.11	21	['220 gener	['ftp']	[']	[']	[']	[']	[']	[']	ftp			
18	140.11	10000	['http/1.0 2(	['https-simp	[']	[']	[']	[']	[']	[']	online driver			
19	140.11	49153	['http/1.1 4(	['wemo-htt	[']	[']	[']	[']	[']	[']	online driver offline			
20	140.11	2222	['ssh-2.0-op	['ssh']	['openssh']	[']	[']	['['cpe:/a:o	[']	[']	openssh			
21	140.11	2000	[']	['ikettle']	[']	[']	[']	[']	[']	[']	Cisco SCCP or get virus			
22	140.11	631	['http/1.1 4(	['http-simpl	[']	['not found	[']	[']	[']	['cups/2.1 i	printer server IPP offline			
23	140.11	1723	['firmware:	['pptp']	[']	[']	[']	[']	[']	[']	Vigor,vigor is online tv or router			
24	140.11	22	['ssh-1.99-(	['ssh']	[']	[']	[']	[']	[']	[']	ssh			

IOT分類 - OpenVas

IOT設備有太多種類跟廠牌，也有太多漏洞，所以使用OpenVas去檢測是否有問題。

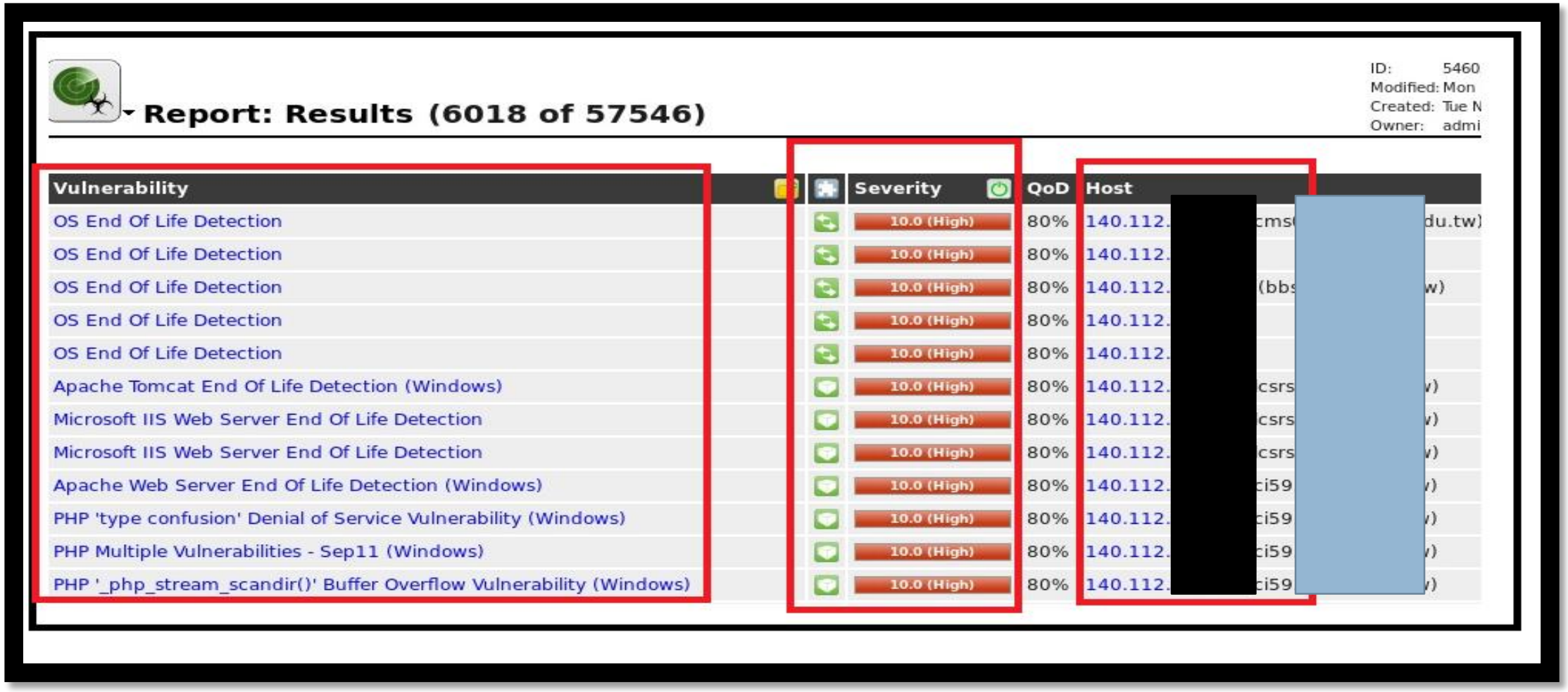


IOT分類 - OpenVas

掃描的報告如下，DVR 為ASOC歸類的影音類別IOT。

IOT分類 - OpenVas

下圖為檢測後的報告，左至右依序為名稱、嚴重等級、目標IP。



Report: Results (6018 of 57546)

ID: 5460
Modified: Mon
Created: Tue N
Owner: admi

Vulnerability	Severity	QoD	Host
OS End Of Life Detection	10.0 (High)	80%	140.112.
OS End Of Life Detection	10.0 (High)	80%	140.112.
OS End Of Life Detection	10.0 (High)	80%	140.112.
OS End Of Life Detection	10.0 (High)	80%	140.112.
OS End Of Life Detection	10.0 (High)	80%	140.112.
Apache Tomcat End Of Life Detection (Windows)	10.0 (High)	80%	140.112.
Microsoft IIS Web Server End Of Life Detection	10.0 (High)	80%	140.112.
Microsoft IIS Web Server End Of Life Detection	10.0 (High)	80%	140.112.
Apache Web Server End Of Life Detection (Windows)	10.0 (High)	80%	140.112.
PHP 'type confusion' Denial of Service Vulnerability (Windows)	10.0 (High)	80%	140.112.
PHP Multiple Vulnerabilities - Sep11 (Windows)	10.0 (High)	80%	140.112.
PHP '_php_stream_scandir()' Buffer Overflow Vulnerability (Windows)	10.0 (High)	80%	140.112.

IOT分類 - OpenVas

驗證結果

Result: Cisco Default Telnet Login

Vulnerability		Severity	QoD
Cisco Default Telnet Login		9.0 (High)	99%

Summary
It was possible to login into the remote host using default credentials.

Vulnerability Detection Result

It was possible to login as user "cisco" with password "cisco".

Solution
Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method
Details: Cisco Default Telnet Login (OID: 1.3.6.1.4.1.25623.1.0.103807)

Version used: $Revision: 9567 $

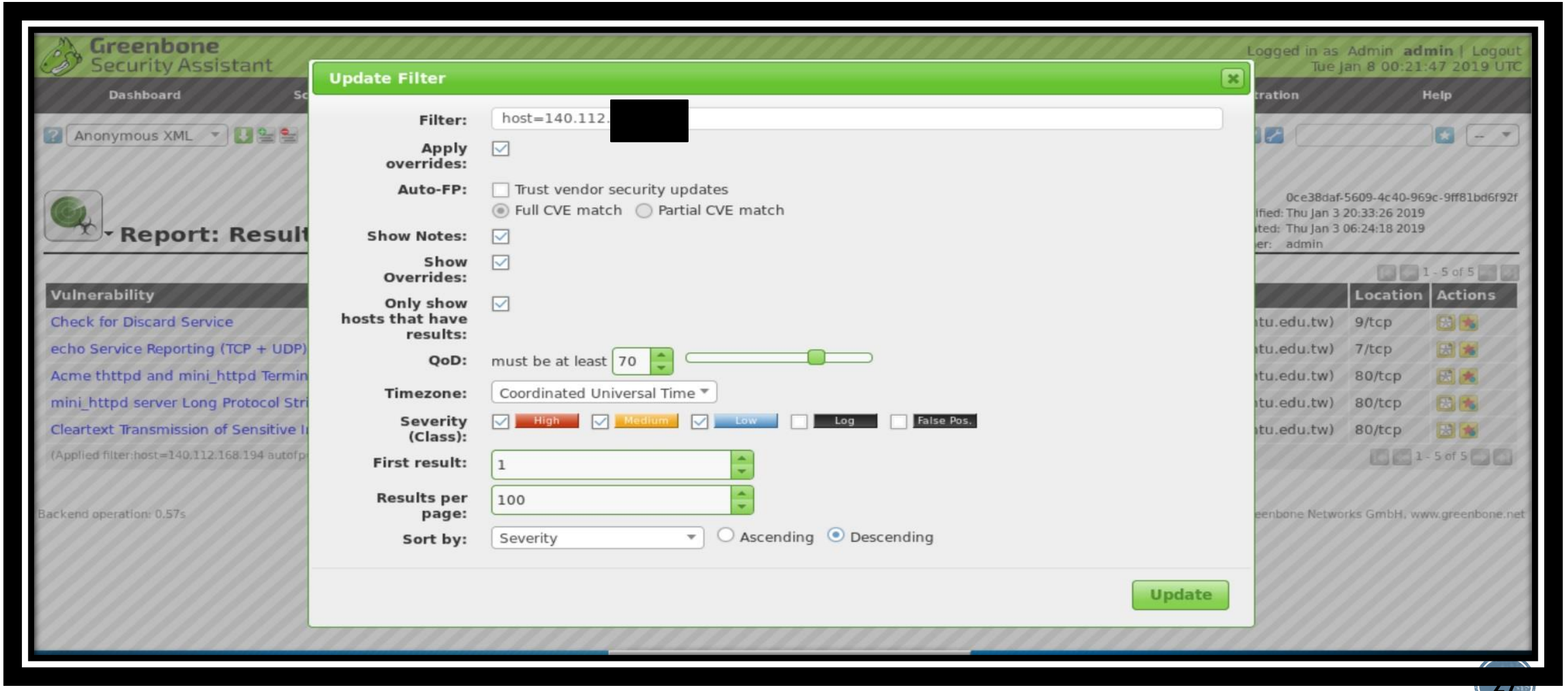
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# telnet 140.112.
Trying 140.112..
Connected to 140.112.
Escape character is '^]'.


User Access Verification

Password:
3850>
```

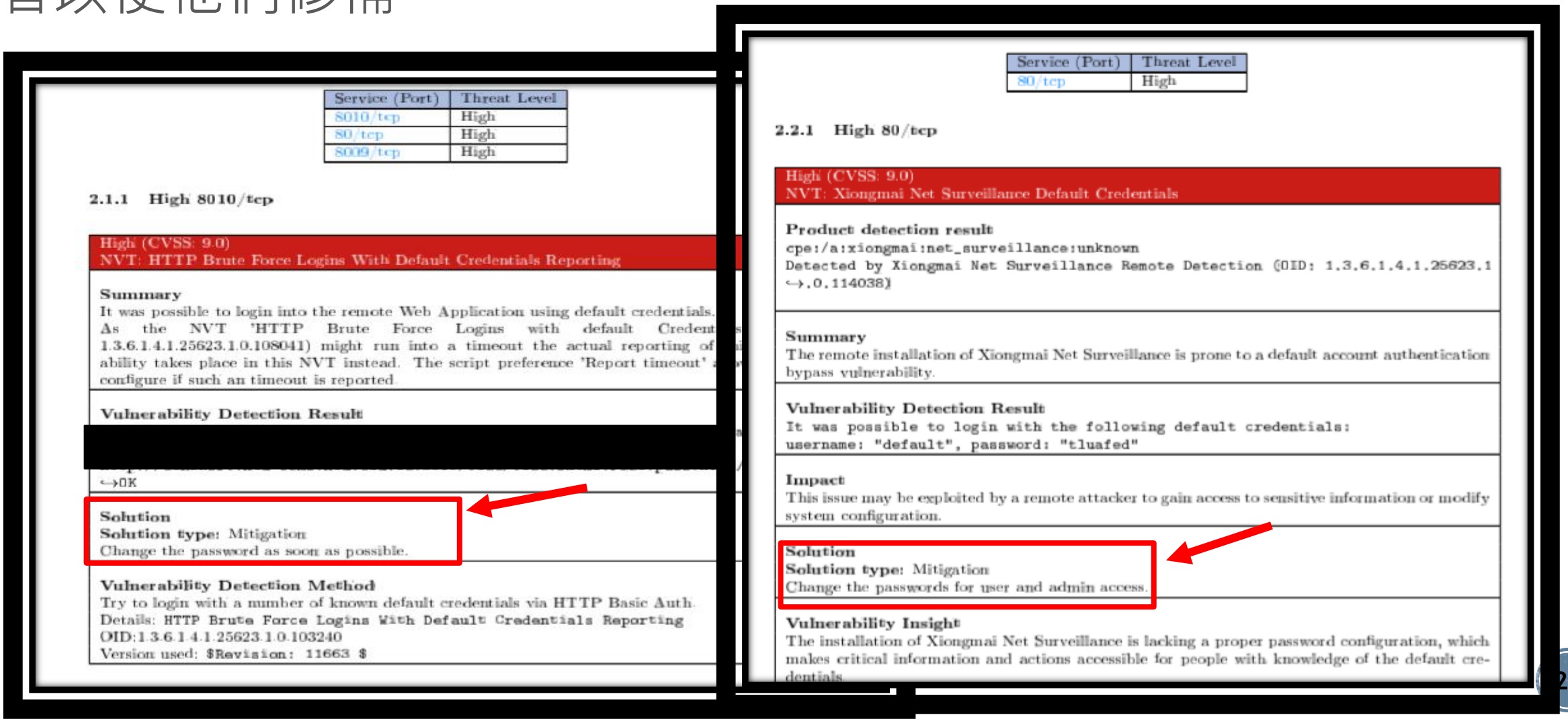
IOT分類 – OpenVas產出報告

下圖為詳細設定畫面。可選擇下載想要的威脅等級等等。



IOT分類 – OpenVas產出報告

OpenVas掃描報告，以及修復方法(紅箭頭處)。將提供給管理者以便他們修補。



Service (Port)	Threat Level
8010/tcp	High
80/tcp	High
8009/tcp	High

2.1.1 High 8010/tcp

High (CVSS: 9.0)
NVT: HTTP Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote Web Application using default credentials. As the NVT 'HTTP Brute Force Logins with default Credent 1.3.6.1.4.1.25623.1.0.108041) might run into a timeout the actual reporting of ability takes place in this NVT instead. The script preference 'Report timeout' configure if such an timeout is reported.

Vulnerability Detection Result

↪OK

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Try to login with a number of known default credentials via HTTP Basic Auth.
Details: HTTP Brute Force Logins With Default Credentials Reporting
OID:1.3.6.1.4.1.25623.1.0.103240
Version used: $Revision: 11663 $

Service (Port)	Threat Level
80/tcp	High

2.2.1 High 80/tcp

High (CVSS: 9.0)
NVT: Xiongmai Net Surveillance Default Credentials

Product detection result
cpe:/a:xiongmai:net_surveillance:unknown
Detected by Xiongmai Net Surveillance Remote Detection (OID: 1.3.6.1.4.1.25623.1 ↪.0.114038)

Summary
The remote installation of Xiongmai Net Surveillance is prone to a default account authentication bypass vulnerability.

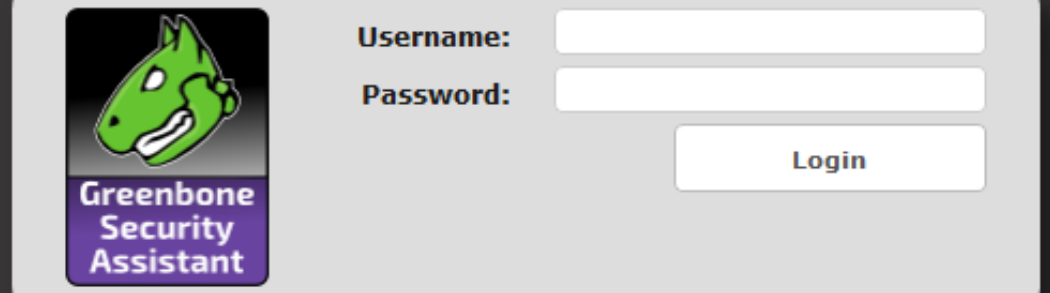
Vulnerability Detection Result
It was possible to login with the following default credentials:
username: "default", password: "tluafed"

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution
Solution type: Mitigation
Change the passwords for user and admin access.

Vulnerability Insight
The installation of Xiongmai Net Surveillance is lacking a proper password configuration, which makes critical information and actions accessible for people with knowledge of the default credentials.

OpenVAS Setup



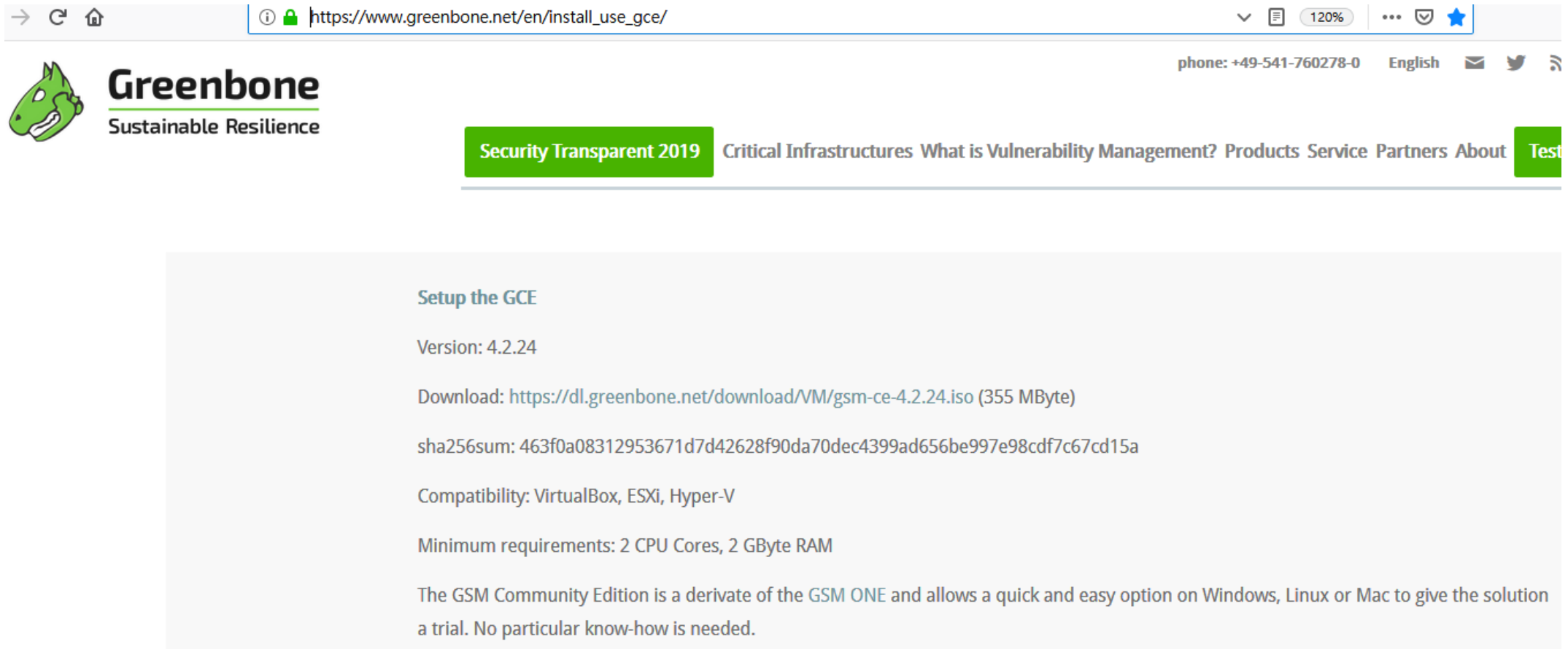
Reference : https://www.linuxincluded.com/installing-openvas-on-centos-7/

自行安裝

- OpenVAS能自行透過 package的方式，安裝於Debian/RedHat 系統。
- 如：Ubuntu、kali => apt install openvas
- 如：CentOS => yum install greenbone-vulnerability-manager (or yum install openvas)

- 優點：自行調整參數、設定排程自動更新…等，適合喜歡自行調教之使用者。
- 缺點：安裝及設定過程，複雜繁瑣，不適合一般使用者。

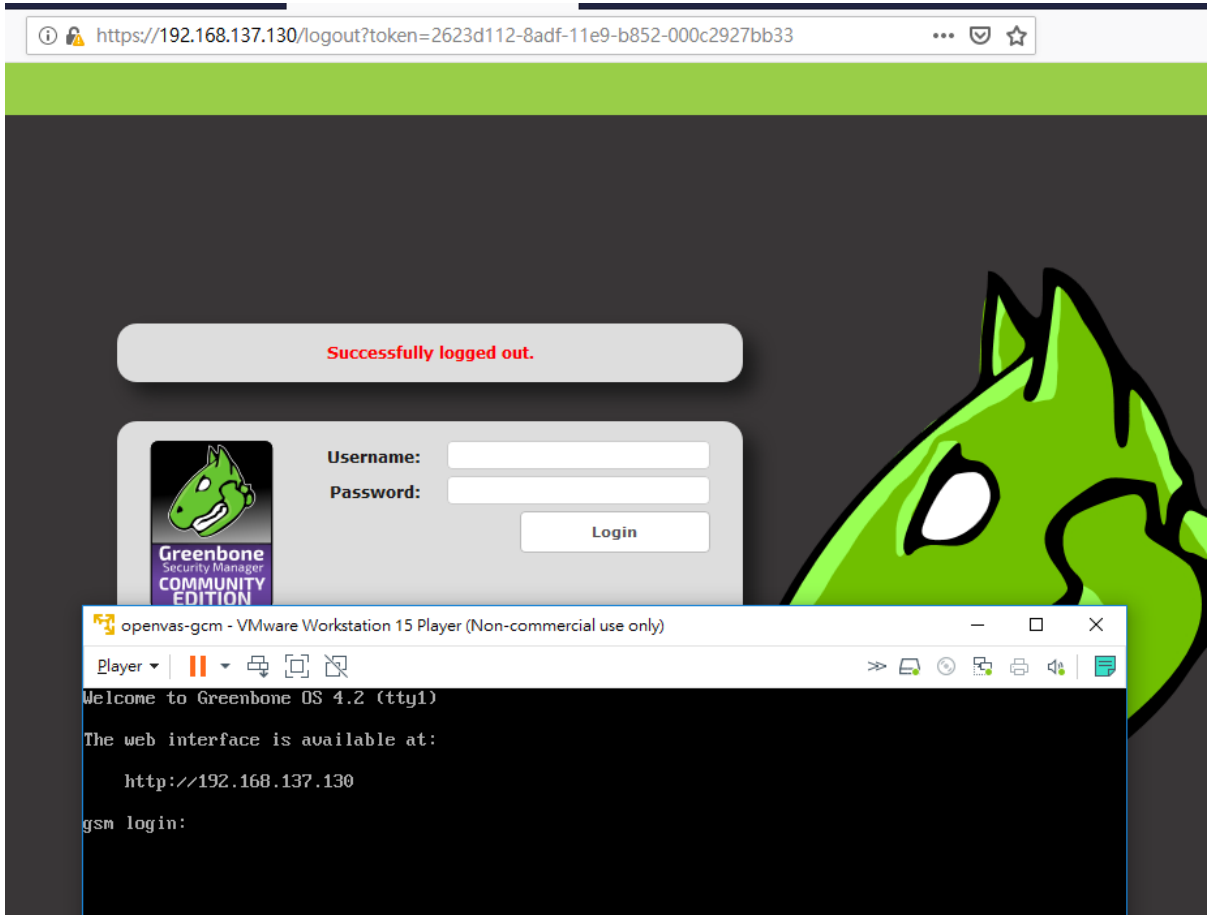
官方 virtual appliance

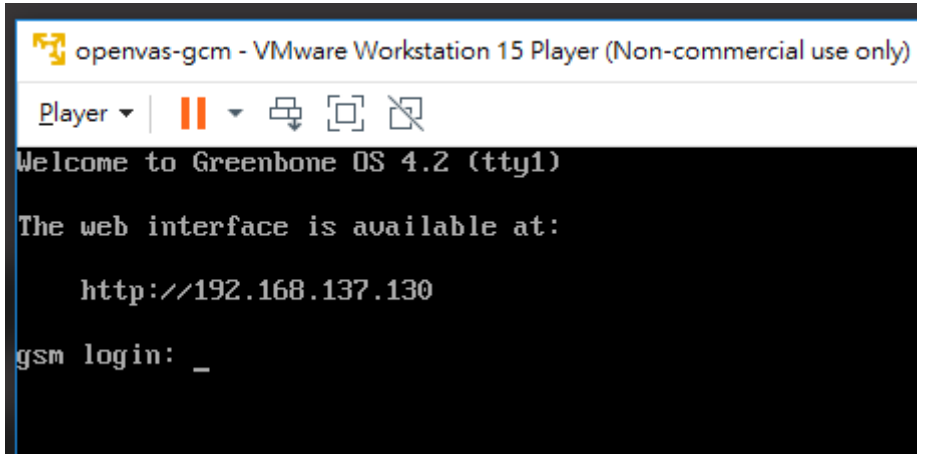


設備需求

- **最小需求**
  - Type: Linux
  - Version: Other Linux (64bit)
  - Memory: 2048M
  - Harddisk: 9G
  - CPUs: 2
- **建議：**
  - Memory： 8G 以上
  - CPUs：4 cores 以上

Greenbone
GSM Community Edition





OpenVAS 使用時機

- 校園內設備眾多，能先透過openvas，進行初步的盤點，及相關弱點的掌握。
- 設定排程定期盤點轄下資產，透過Openvas協助進行弱點掃描，及追蹤漏洞修復狀況。
- IoT 設備未來也將列入重點防護範圍，可以從shodan上找尋相關IoT特徵篩選後，再對疑似IoT的設備進行弱點掃描，掌握校園IoT設備之狀況。

Thanks

Reference

- https://www.linuxincluded.com/installing-openvas-on-centos-7/
- http://openvas.org/download.html
- https://vulners.com/