

索引

1. 建立新目標並掃描
 - (1) 建立目標
 - (2) 掃描
2. 掃描結果與維護
 - (1) 掃描結果
 - (2) 弱點資料
 - (3) 編輯已知弱點
3. 資料輸出
 - (1) 報表輸出
4. 其他

1. 建立新目標並掃描

- (1) 建立目標

建立目標的視窗有2個方式開啟，首先在首頁下有個New static site能夠建立目標

The screenshot shows the Nexpose web interface. At the top, there are navigation tabs: Home, Assets, Vulnerabilities, Policies, Reports, and Administration. Below the navigation is a search bar. The main content area is divided into several sections:

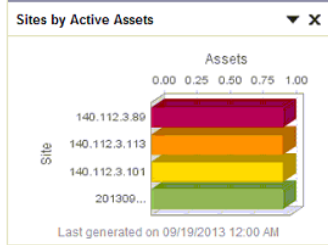
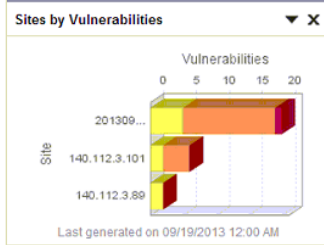
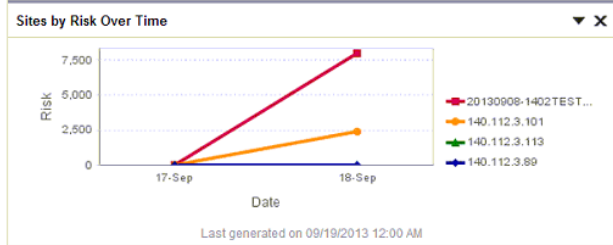
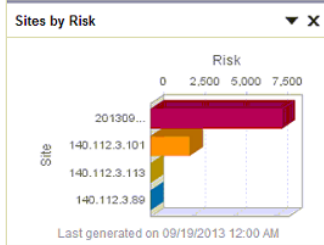
- Most Vulnerable Sites:** A 3D bar chart showing the number of vulnerabilities for different sites. The sites listed are 201309..., 140.112.3.101, and 140.112.3.89.
- Most Vulnerable Sites Over Time:** A line graph showing the number of vulnerabilities over time for four different sites: 20130908-1402TEST..., 140.112.3.101, 140.112.3.113, and 140.112.3.89.
- Site Listing:** A table listing sites with columns for Name, Assets, Vulnerabilities, Risk, Type, Scan Status, Scan, Edit, and Delete. The table contains four rows of data. A red box highlights the 'New static site' button below the table.
- Current Scan Listing for All Sites:** A section that currently displays 'There are no scans to display.' and a 'Scan now' button.
- Asset Group Listing:** A section that currently displays 'There are no asset groups to display.' and buttons for 'New dynamic asset group' and 'New static asset group'.

其次，若在其他頁面，可以按下上方的Assets，並按下Sites 後面的 View，一樣能到達顯示目標清單與報表的頁面

The primary goal of Vulnerability Management is the protection of assets. The Security Console can be used to view assets in a variety of ways, including the sites or groups they belong to, as well as the operating system and software they are running.

- Sites [View assets by the sites they belong to.](#)
- Asset groups [View assets by the asset groups they belong to.](#)
- Operating systems [View assets by the Operating System they are running.](#)
- Services [View assets by the services they are running.](#)
- Software [View assets by the software installed on them.](#)
- All [View a listing of all assets.](#)

一樣在最下面有個New static site能夠建立目標



Site Listing

Name	Assets	Vulnerabilities	Risk	Type	Scan Status	Scan	Edit	Delete
20130908-1402TEST_KOU	1	20	7,951	Static	Scan finished on Wed Sep 18 2013			
140.112.3.101	1	6	2,380	Static	Scan finished on Wed Sep 18 2013			
140.112.3.113	1	0	0.0	Static	Scan finished on Wed Sep 18 2013			
140.112.3.89	1	2	0.0	Static	Scan finished on Wed Sep 18 2013			

New static site 建立新目標

按下New static site之後，會跳至資料輸入頁面，並開始一步一步填入

首先是輸入這個目標的命名，並輸入描述
中間有個Importance能夠標示重要度，那只是做為提醒而已，並不影響掃描的結果
填寫完畢後按下Next

Assets > Sites > New Site > Configuration

Site Configuration

Previous **Next** Save Cancel

General

A site is a collection of assets to be scanned. Basic site configuration includes sele

Assets

Name 1

Importance

Type

Description 2

Scan Setup

Credentials

Web Applications

Organization

Access

接著輸入IP位置或網址，請注意粉紅色框框部分的範例
 這個是可以搭配CIDR及其他輸入方式輸入多個IP位址
 若多個IP位址之中有不想掃描的目標，可以填寫在Excluded Assets欄位中
 填寫完畢之後一樣按下Next

Assets > Sites > New Site > Configuration

Site Configuration

Previous **Next** Save Cancel

General

Assets

Scan Setup

Credentials

Web Applications

Organization

Access

Included Assets

The listed IP addresses and host names are included in this site.

4

Import list from file 未選擇檔案

Excluded Assets

The listed IP addresses and host names will not be scanned as part of this site.

5

Import list from file 未選擇檔案

Enter one IP address or host name per line using any of the following notations:

```

10.0.0.1
10.0.0.1 - 10.0.0.255
10.0.0.0/24
2001:db8::1
2001:db8::0 - 2001:db8::ffff
2001:db8::/112
2001:db8:85a3:0:0:8a2e:370:7330/124
www.example.com

IPv6 addresses can be fully compressed, partially uncompressed, or uncompressed. The following are equivalent:
2001:db8::1
2001:db8:0:0:0:0:0:1
2001:0db8:0000:0000:0000:0000:0000:0001

If you use CIDR notation for IPv4 addresses (x.x.x.x/24) the Network Identifier (.0) and Network Broadcast Address(.255) will be ignored, and the entire network is scanned.
10.0.0.0/24 will become 10.0.0.1 - 10.0.0.254
10.0.0.0/16 will become 10.0.0.1 - 10.0.255.254

```

Scan Template可以選擇所掃描的威脅種類，預設是全部
 Scan Engine裡面沒有別的選項，不用更動
 若將Scan Schedule裡的Enable schedule勾選，可以設定掃描的時間、頻率
 除非有特殊需要，一般來說這一頁什麼都不用動(Enable schedule也不勾選)，直接按下Next就好

Site Configuration

Previous **Next** Save Cancel

- General
- Assets
- Scan Setup**
- Credentials
- Web Applications
- Organization
- Access

Scan Template

Select or customize a scan template, which controls how assets are scanned and which checks are performed for this site. [Learn about built-in scan templates.](#)

Full audit

Scan Engine

Select a Scan Engine for this site. A distributed Scan Engine must be paired with the Security Console before it can appear in the list. [Learn about distributed Scan Engines and pairing.](#)

Local scan engine

Scan Schedule

Schedule starting dates and times for scans, and set their frequency. Determine whether incomplete, repeating scans start again from the beginning or continue where they previously stopped. If the scan does not complete within its duration, it will automatically pause. You can then manually resume it. Once a repeating scan completes, it will stop until the next start date and time.

Enable schedule

Start date and time : : AM

Maximum scan duration (minutes)

Repeat scan every months on the specified date

If a scan reaches the maximum duration

這裡可以建立目標的帳戶資訊，應是能提供更完整的弱點掃描，誤判率會降低
按下New能夠建立帳戶資訊
若不輸入也能夠掃描，只需要按下Next到下一步驟就可以了

Site Configuration

Previous **Next** Save Cancel

- General
- Assets
- Scan Setup
- Credentials**
- Web Applications
- Organization
- Access

Create or edit credentials for authenticated scans that will be used specifically for this site. You can only edit site-specific credentials in a site configuration.

Credential Listing

There are no entries to display.

===== 若不需要輸入帳戶資訊就請跳過以下步驟 =====

若按下New可以看到以下資料輸入頁面

輸入對這個帳戶資料的命名與描述，並按下Next到下一步驟

Site Credential Configuration

Previous **Next** Save Cancel

- General**
- Account
- Restrictions

Create or edit shared credentials for authenticated scans.

Name

Description

接著依序輸入 目標的系統種類、命名、使用者帳戶名稱、密碼兩次
下方有個測試是否能夠正常連接並登入的功能，
只需要輸入IP及 Port 445，按下Test credentials就可以測試了

按下Save到下一步驟

Site Credential Configuration

Previous Next **Save** Cancel

General **8** Select a service and enter all information required for authentication on the service during scans.

Account **4** Service

Restrictions Domain

User name **5**

Password **6**

Confirm password **7**

▼ Test Credentials (Learn how.)
 Test these credentials to ensure they are valid.
 Host name/IP address
 Port

輸入目標的IP及Port 445後，按下Save儲存目標帳戶資訊

Site Credential Configuration

Previous Next **Save** Cancel

General **11** You can restrict the use of these credentials to one IP address or host name. You can also restrict their use to a single port.

Account IP address/host name

Restrictions Port

====若不需要輸入帳戶資訊就請跳過以上步驟=====

這裡如同先前的使用者帳戶資料，若有Web Applications需要登入做掃描也能輸入資料
繼續按下Next到下一步驟

Assets > Sites > New Site > Configuration >

Site Configuration

Previous **Next** Save Cancel

General **9** You can use HTML forms or HTTP headers to authenticate scans on target Web applications.

Assets

Scan Setup

Credentials

Web Applications

Organization

Access

Authentication on Web Applications

這裡可以輸入這個目標設備的聯絡人資料
不輸入也可以，按下Next到下一步驟

Assets Sites New Site Configuration

Site Configuration

Previous Next Save Cancel

General These optional fields capture information about your organization that Nexpose may use in certain reports.

Assets **Organization Name**

Scan Setup **URL**

Credentials **Primary Contact**

Web Applications **Job Title**

Organization **Email**

Access **Telephone**

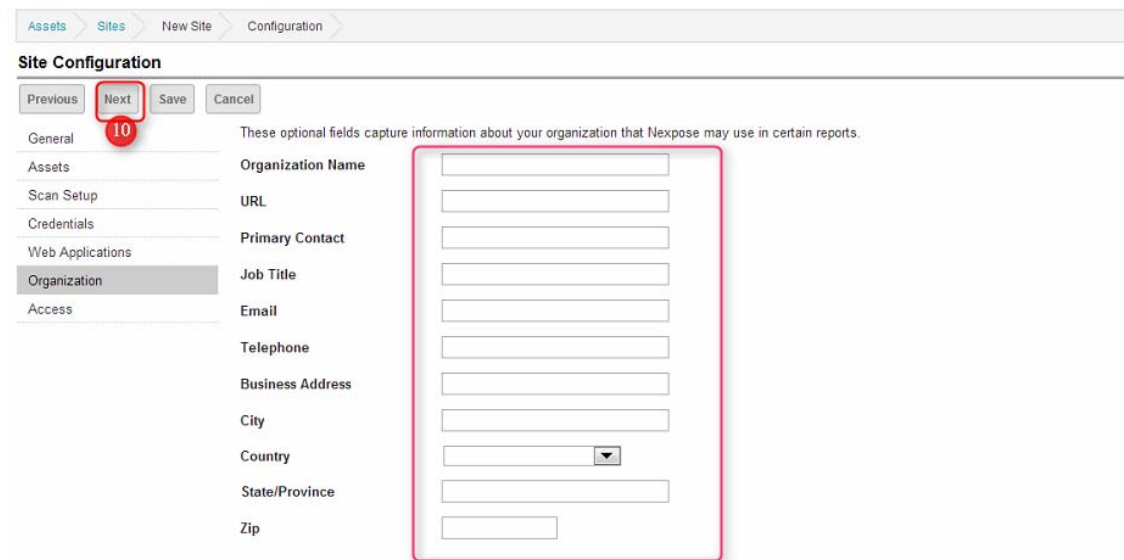
Business Address

City

Country

State/Province

Zip



按下Save就可以完成建立

Assets Sites New Site Configuration

Site Configuration

Previous Next Save Cancel

General Only Global Administrators and users on this site's access list can view this site. To add user(s) to the list, click **Add users**.

Assets **Access Listing**

Scan Setup There are no entries to display

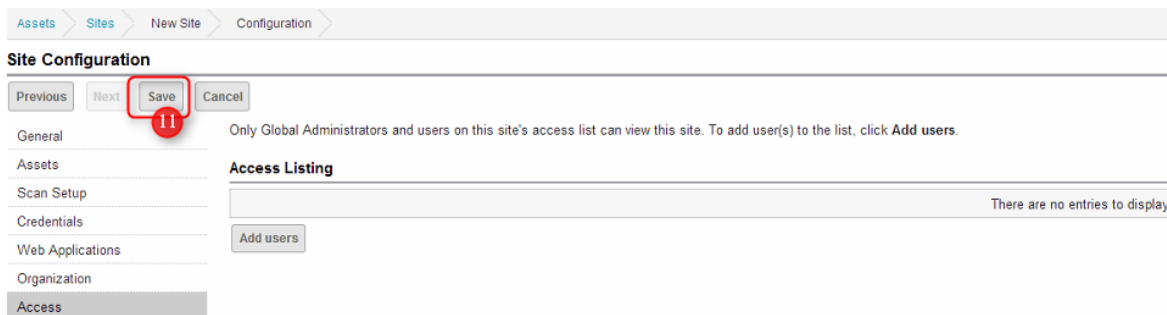
Credentials

Web Applications

Organization

Access

Add users



(2) 掃描

在建立一個新目標之後，會回到首頁
可以看到之前我們所建立過的目標，以及被掃描到的弱點、何時掃描
最後面的按鈕可以執行立即掃描、編輯目標資訊或刪除此目標
剛剛所設定的目標還沒有掃描過，如同下圖所示
此時對剛剛設定的目標按下後方的Scan按鈕立即掃描

Home

Most Vulnerable Sites

Last generated on 09/19/2013 12:00 AM

Most Vulnerable Sites Over Time

Last generated on 09/19/2013 12:00 AM

Site Listing

Name	Assets	Vulnerabilities	Risk	Type	Scan Status	Scan	Edit	Delete
20130908-1402TEST_KOU		1	20	7,951 Static	Scan finished on Wed Sep 18 2013			
140.112.3.101		1	6	2,380 Static	Scan finished on Wed Sep 18 2013			
140.112.3.113		1	0	0.0 Static	Scan finished on Wed Sep 18 2013			
140.112.3.89		1	2	0.0 Static	Scan finished on Wed Sep 18 2013			
Tmp_140.112.3.82_Kouitsuhou		0	0	0.0 Static	Not scanned			

New static site

Current Scan Listing for All Sites

There are no scans to display.

Scan now

Asset Group Listing

There are no asset groups to display.

New dynamic asset group New static asset group

立即掃描

編輯目標

刪除目標

接著會跳出視窗，按下Start now就會開始掃描

Start New Scan

Site: Tmp_140.112.3.82_Kouitsuhou

Site Details

Scan template: Full audit

Included assets: 140.112.3.82

Excluded assets:

Manual Scan Targets

You can scan one or more assets within this site by entering IP addresses, IP address ranges or host names.

Scan all assets within this site

Specify one or more assets within this site to scan

Assets to scan:

2 Start now Cancel

接著可以看到狀態視窗，顯示掃描開始的時間，掃到的弱點數量及當前狀態

Assets Sites Tmp_140.112.3.82_Kouitsuhou Scans Full audit

Scan Progress

Scan Type	Started	Assets	Active	Completed	Pending	Vulnerabilities	Elapsed	Remaining	Status
Manual	2013年9月19日 上午8:17:03	0	0	0	0	0		0 seconds	In progress

Stop scan Pause scan

Discovered Assets

Asset discovery is still in progress.

掃描通常很快，在十分鐘以內就能夠完成。這次掃描只花了25秒
若超過十分鐘則有可能設定目標時有資料誤植，此時就需要將目標刪除之後，另創新目標再度掃描

Assets Sites Tmp_140.112.3.82_Kouitsuhou Scans Full audit Search

Scan Progress

Scan Type	Started	Assets	Vulnerabilities	Elapsed	Status
Manual	2013年9月19日 上午8:17:03	1	4	53 seconds	Completed successfully

A scan type refers to whether it was scheduled to start automatically or started manually by a user

Discovered Assets

Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status
140.112.3.82	davisyoupc.cc.ntu.edu.tw	Microsoft Windows 7 Enterprise Edition SP1	4	25 seconds	Completed

2. 掃描結果與維護

(1) 掃描結果

觀看掃描結果的方式有2個，首先就是如同前圖，掃描完成後按下IP即可顯示，但是資料會少了一些
比較完整的資料需要以下方方式開啟

首先回到首頁，或者照前面步驟一樣按下上方的Assets→Sites View，接著按下我們所掃描的目標名稱

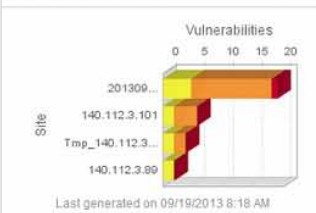
Sites by Risk



Sites by Risk Over Time



Sites by Vulnerabilities



Sites by Active Assets



Site Listing

Name	Assets	Vulnerabilities	Risk	Type	Scan Status	Scan	Edit	Delete
20130908-1402TEST_KOU	1	20	7,951	Static	Scan finished on Wed Sep 18 2013			
140.112.3.101	1	6	2,380	Static	Scan finished on Wed Sep 18 2013			
tmp_140.112.3.82_Koutsuhou	1	4	1,489	Static	Scan finished on Thu Sep 19 2013			
140.112.3.113	1	0	0.0	Static	Scan finished on Wed Sep 18 2013			
140.112.3.89	1	2	0.0	Static	Scan finished on Wed Sep 18 2013			

接著可以看到先前掃描結果的圖表，如有一次掃描多個目標，這些結果將是總和後的圖表
按下方想要找尋的特定IP

Assets Sites Tmp_140.112.3.82_Koultuhou Search

Site Summary

Defined Assets	Active Assets	Inactive Assets	Vulnerabilities	Last Scanned	Next Scan
	1	1	0	4 2013年9月19日 上午8:17:56	Not set

Manage site Create site report View scan history

Current Scan Listing

There are no scans to display.

Scan now

Vulnerabilities by Severity

Last generated on 09/19/2013 8:18 AM

Vulnerabilities over Time

Last generated on 09/19/2013 8:18 AM

Assets by Vulnerability Severity

Last generated on 09/19/2013 8:18 AM

Risk Over Time

Last generated on 09/19/2013 8:18 AM

Asset Listing

View details about assets, including those no longer active. To delete an asset, select a row. To delete all displayed assets, select the top row and use **Select Visible**. Cancel all selections using **Clear All**. [Learn more](#).

Delete Assets Total Assets Selected: 0 of

<input type="checkbox"/>	Address	Name	OS	<input type="checkbox"/>	<input type="checkbox"/>	Vulnerabilities	Risk	Last Scan
<input type="checkbox"/>	140.112.3.82	DAVISYOU-PC	Microsoft Windows 7 Enterprise Edition SP1	0	0	4	1,489	Thu Sep 19 2013

Showing 1 to 1 of 1 Export to CSV Rows per page: 10 1 of 1

然後就能看到比較完整的結果了，與掃描後直接按下IP觀看的內容比較，這裡多了更多有關於弱點的資料

nexpose Assets Vulnerabilities Policies Reports Administration

Assets Sites Tmp_140.112.3.82_Kouitsuhou 140.112.3.82

Search

Asset Properties

Addresses	140.112.3.82	Operating system	Microsoft Windows 7 Enterprise Edition SP1
Hardware address	D4 BE D9 8B AB 44	CPE	
Aliases	davisyoupc.cc.ntu.edu.tw, DAVISYOU-PC	Last scan	2 hours ago
Host type	Unknown	Next scan	Not set
Site	Tmp_140.112.3.82_Kouitsuhou		

Scan asset now Create asset report

Vulnerability Listing

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures: Susceptible to malware attacks Metasploit-exploitable Exploit published

Exclude Recall Resubmit

Total Vulnerabilities Selected: 0 of 4

Title			CVSS	Risk	Published On	Severity	Instances	Exceptions
SMB signing disabled			7.3	753	Mon Nov 01 2004	Severe	2	Exclude
SMB signing not required			6.2	736	Mon Nov 01 2004	Severe	2	Exclude
TCP timestamp response			0	0.0	Fri Aug 01 1997	Moderate	1	Exclude
ICMP timestamp response			0	0.0	Fri Aug 01 1997	Moderate	1	Exclude

Showing 1 to 4 of 4 Export to CSV Rows per page: 10 1 of 1

Vulnerability Exception Listing

There are no vulnerability exceptions to display.

Exploit Listing

There are no exploits to display.

Malware Kit Listing

Malware Kit

(2) 弱點資料

首先必須提到的一點是，這張圖是做出來的，絕無此案例

我們可以看到紅色的病毒圖示、藍底白字M圖示及白底三角形黑點圖示

若標題後方有出現紅色病毒圖示，則代表弱點有被惡意軟體來作為攻擊用途

若標題後方有藍底白字M圖示，則代表此弱點在Metasploit內含有工具，能夠以此弱點進行攻擊

若標題後方有白底三角形黑點圖示，則代表此弱點有建立在資料庫內，可以點選並自行編譯出來，然後攻擊

CVSS為Common Vulnerability Scoring System之縮寫，範圍是0-10，分數越高則問題越嚴重

Risk為風險值，這部分的範圍應是0-1000，同樣的分數越高則問題越嚴重

Published On為弱點被發現的時間

Severity為威脅的危險分級，通常以Critical為優先通報及處理

Exposures: Susceptible to malware attacks Metasploit-exploitable Exploit published

Exclude Recall Resubmit

Total Vulnerabilities Selected: 0 of 4

Title			CVSS	Risk	Published On	Severity	Instances	Exceptions
SMB signing disabled			7.3	753	Mon Nov 01 2004	Severe	2	Exclude
SMB signing not required			6.2	736	Mon Nov 01 2004	Severe	2	Exclude
TCP timestamp response			0	0.0	Fri Aug 01 1997	Moderate	1	Exclude
ICMP timestamp response			0	0.0	Fri Aug 01 1997	Moderate	1	Exclude

Showing 1 to 4 of 4 Export to CSV Rows per page: 10 1 of 1

(2) 編輯已知弱點

當有些弱點是我們已知且需要疏忽的時候，可以將

同上圖，最後面有個Exclude可以按，按了之後會跳出視窗，可以輸入刪除的原因
 Scope可以選擇刪除這一次掃描內容的單個弱點，或是刪除其他所有掃描的相同弱點
 Reason有內建數個原因可以選，或者將原因打入在下方Additional comments
 再按下Submit即可

Vulnerability Exception X

An exception request will be sent to reviewer for the following vulnerability.

Vulnerability Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687)

Asset 140.112.2.208

Scope All instances on this asset

Reason False Positive

Additional comments

3. 資料輸出

(1) 報表輸出

若要輸出報表，首先按下上方的Reports

The screenshot shows the Nexpose web interface. The 'Reports' menu item is highlighted with a red circle and a red '1'. Below the navigation bar, there are two charts:

Most Vulnerable Sites: A 3D bar chart showing the number of vulnerabilities for different sites. The x-axis represents the number of vulnerabilities (0 to 20), and the y-axis represents the site. The data points are: 201309... (approx. 18), 140.112.3.101 (approx. 15), Temp_140.112.3... (approx. 10), and 140.112.3.89 (approx. 5). Last generated on 09/19/2013 10:48 AM.

Most Vulnerable Sites Over Time: A line chart showing the number of vulnerabilities over time for different sites. The x-axis represents the date (18-Sep to 19-Sep), and the y-axis represents the number of vulnerabilities (0 to 20). The data points are: 20130908-1402TEST... (red line, increasing from 0 to 20), 140.112.3.101 (orange line, increasing from 0 to 5), Temp_140.112.3.82... (green line, increasing from 0 to 3), 140.112.3.113 (blue line, increasing from 0 to 2), and 140.112.3.89 (purple line, increasing from 0 to 1). Last generated on 09/19/2013 10:48 AM.

Site Listing: A table listing the sites and their corresponding assets.

Name	Assets
20130908-1402TEST_KOU	1
140.112.3.101	1
Temp_140.112.3.82_Kouitsuhou	1
140.112.3.113	1
140.112.3.89	1

接著按下上方的Create a report，並輸入報告的名稱、選擇報告的種類、輸出格式(有PDF及HTML可選擇)
 在Scope按下 Select Sites, Assets, or Asset Groups 的會跳出視窗，
 選擇掃描過的目標並按下Done會回到Create a report的畫面
 最後按下Run the report就會到View reports的頁面

2 Create a report

View reports

Manage report templates

Name Report time zone (GMT +0800) Taipei

Template 3

Document Export All Search templates

4

1. Executive Summary Selected

Audit Report Executive Overview Top 10 Assets by Vulnerabilities Top 10 Assets by Vulnerability Risk

Displaying 4 of 7

File format 5 PDF

Scope 6

1 Selected Sites + Select Sites, Assets, or Asset Groups Filter report scope based on vulnerabilities

Frequency 9 Run a one-time report now

Run the report Configure advanced settings...

下圖是Select Sites,Assets, or Asset Groups 的畫面

Select Report Scope

Use the last scan data only

Select to report on

Total Selected 1

<input type="checkbox"/>	Name	Assets	Vulnerabilities	Risk Score	Type	Last Scan
<input type="checkbox"/>	20130908-1402TEST_KOU	1	20	7,951	Static	2013年9月18日 下午2:05:48
<input type="checkbox"/>	140.112.3.101	1	6	2,380	Static	2013年9月18日 下午4:40:58
<input checked="" type="checkbox"/>	Tmp_140.112.3.82_Kouitsuhou	1	4	1,489	Static	2013年9月19日 上午8:17:56
<input type="checkbox"/>	140.112.3.113	1	0	0.0	Static	2013年9月18日 下午7:00:33
<input type="checkbox"/>	140.112.3.89	1	2	0.0	Static	2013年9月18日 下午5:35:56

Cancel Done

8

在View reports找到我們所建立的報告，可以左鍵點選開啟，或右鍵另存目標
 在報告名稱前方的齒輪按鍵可以對報告進行複製、刪除等動作
 報告內容會對每一個弱點做更詳細的說明

Create a report

View reports

10



Manage report templates

New

Rows 10 1 - 2 of 2

Report Name

Most Recent Report

Report Name	Most Recent Report
  tmp_140.112.3.113_Kouitsuhou 11	2013年9月19日 8:20 AM
Run Edit Copy Delete History	140.112.2.208_AT1411 2013年9月18日 3:06 PM