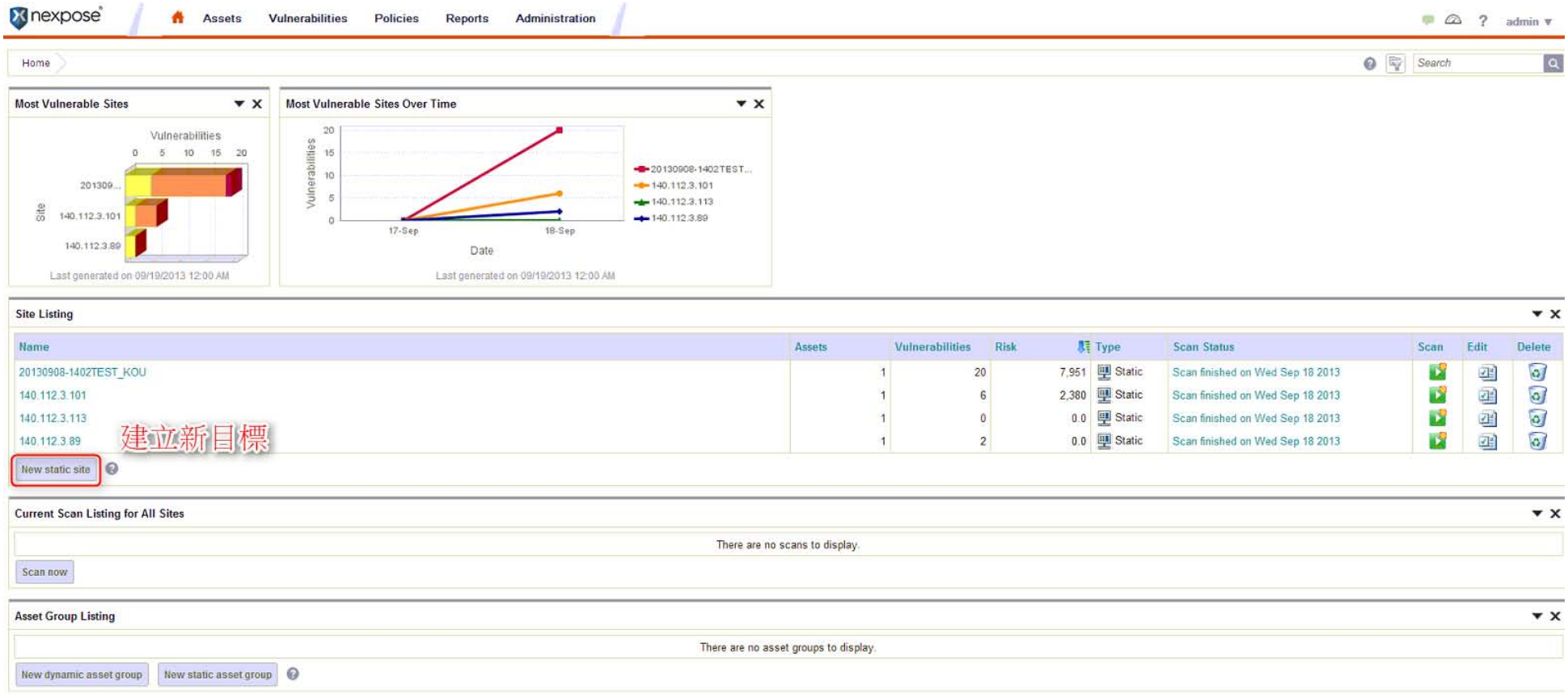
索引

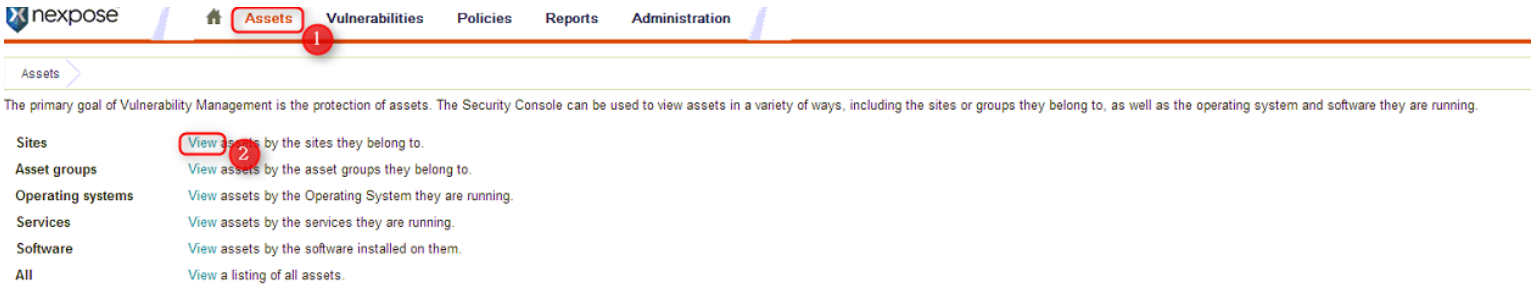
1.建立新目標並掃描

(1) 建立目標

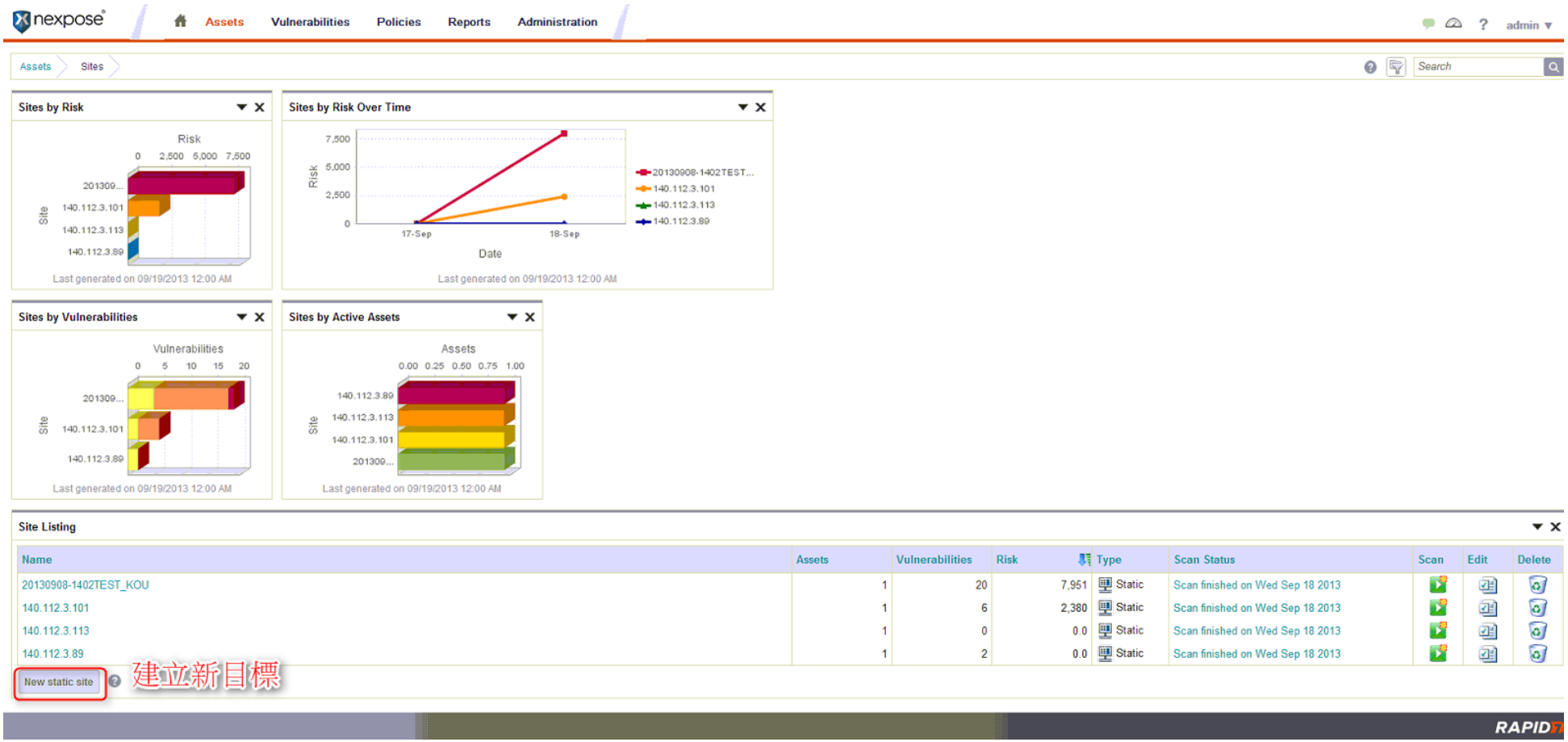
建立目標的視窗有2個方式開啟，首先在首頁下有個New static site能夠建立目標



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

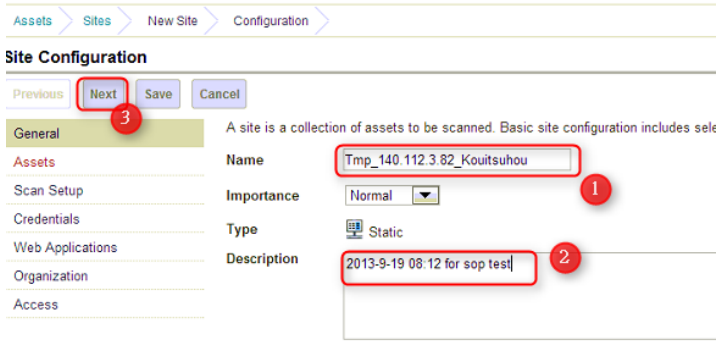


一樣在最下面有個New static site能夠建立目標

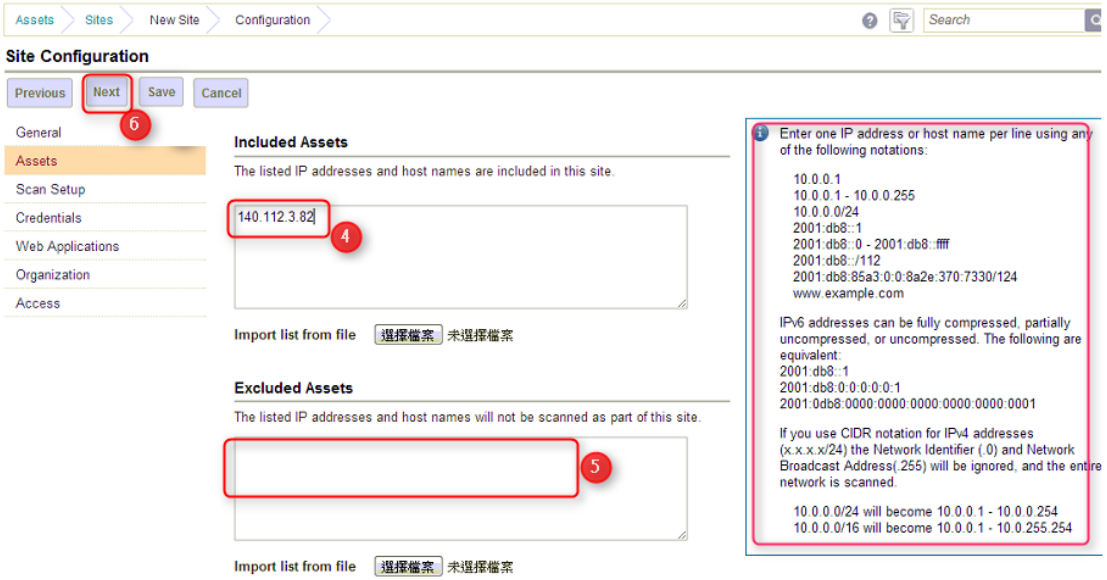


按下New static site之後，會跳至資料輸入頁面，並開始一步一步填入

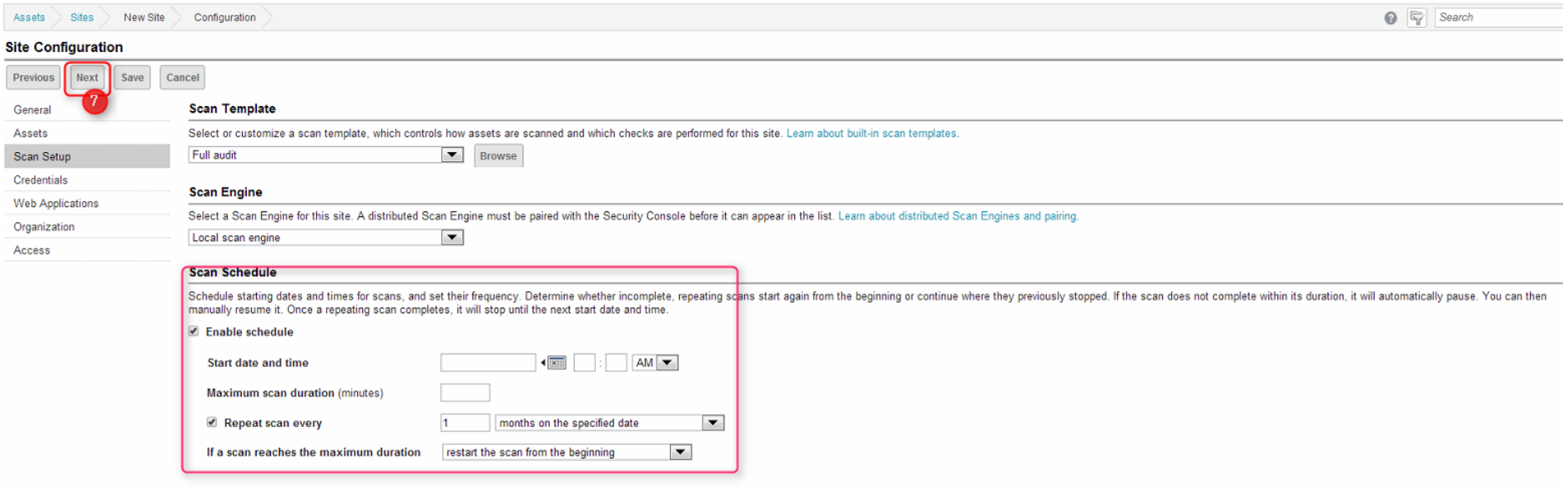
首先是輸入這個目標的命名，並輸入描述
中間有個Importance能夠標示重要度，那只是做為提醒而已，並不影響掃描的結果
填寫完畢後按下Next



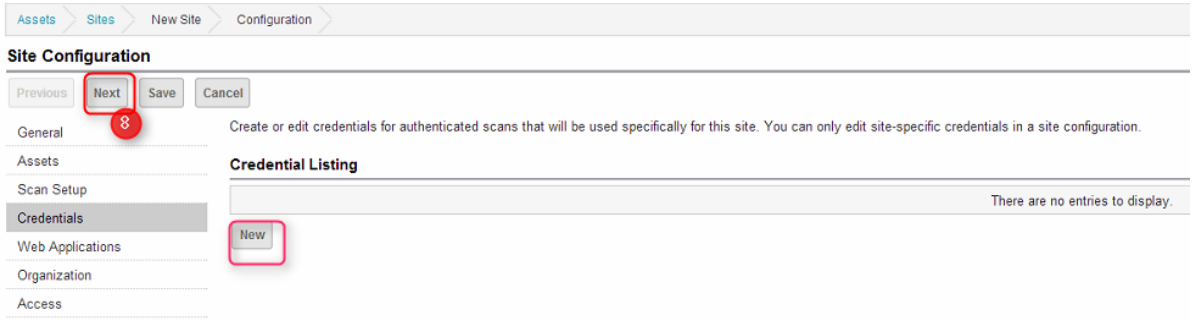
接著輸入IP位置或網址，請注意粉紅色框框部分的範例
這個是可以搭配CIDR及其他輸入方式輸入多個IP位址
若多個IP位址之中有不想掃描的目標，可以填寫在Excluded Assets欄位中
填寫完畢之後一樣按下Next



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



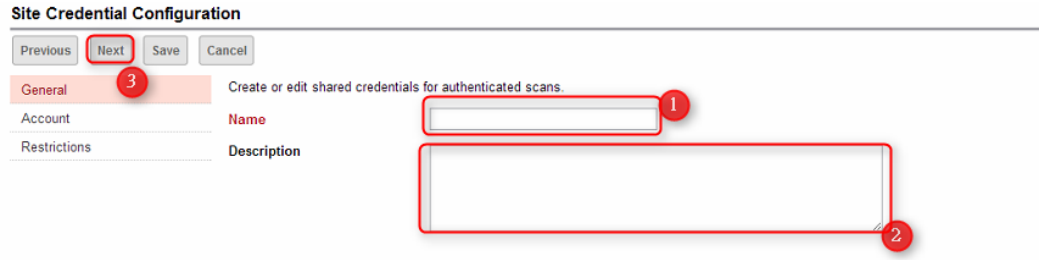
這裡可以建立目標的帳戶資訊，應是能提供更完整的弱點掃描，誤判率會降低
按下New能夠建立帳戶資訊
若不輸入也能夠掃描，只需要按下Next到下一步驟就可以了



==========若不需要輸入帳戶資訊就請跳過以下步驟==========

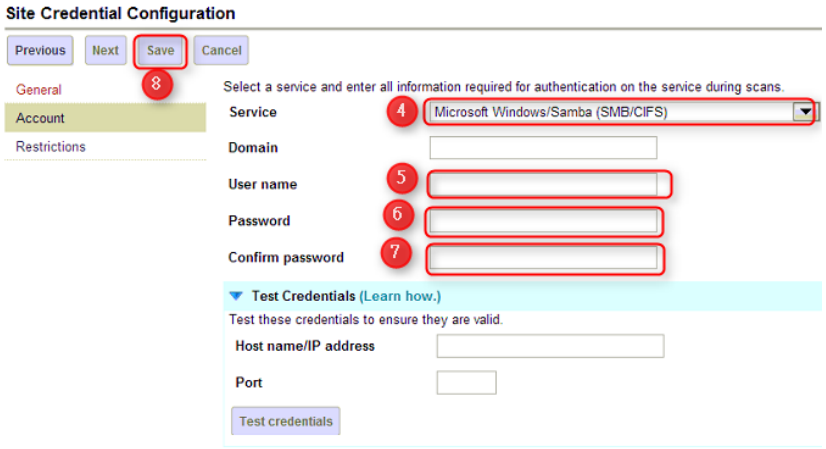
若按下New可以看到以下資料輸入頁面

輸入對這個帳戶資料的命名與描述，並按下Next到下一步驟

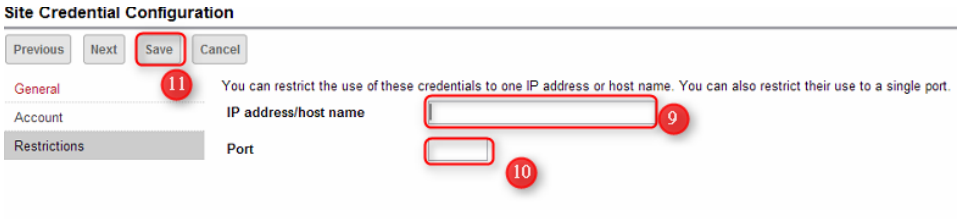


接著依序輸入 目標的系統種類、命名、使用者帳戶名稱、密碼兩次
下方有個測試是否能夠正常連接並登入的功能，
只需要輸入IP及 Port 445 ，按下Test credentials就可以測試了

按下Save到下一步驟

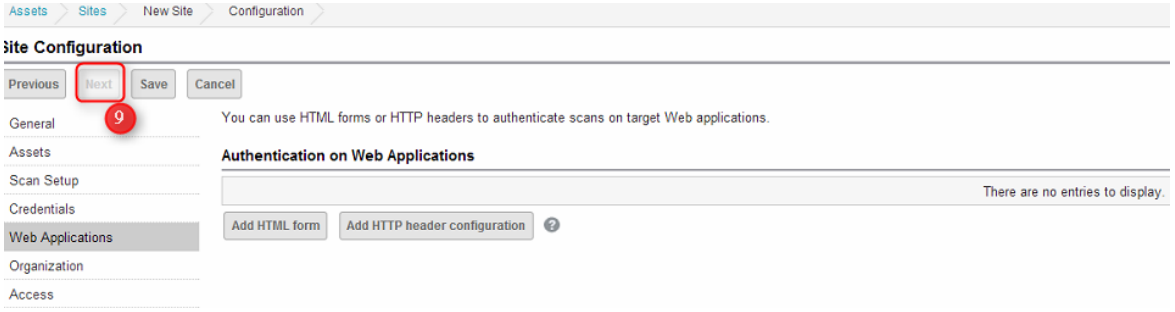


輸入目標的IP及Port 445後，按下Save儲存目標帳戶資訊

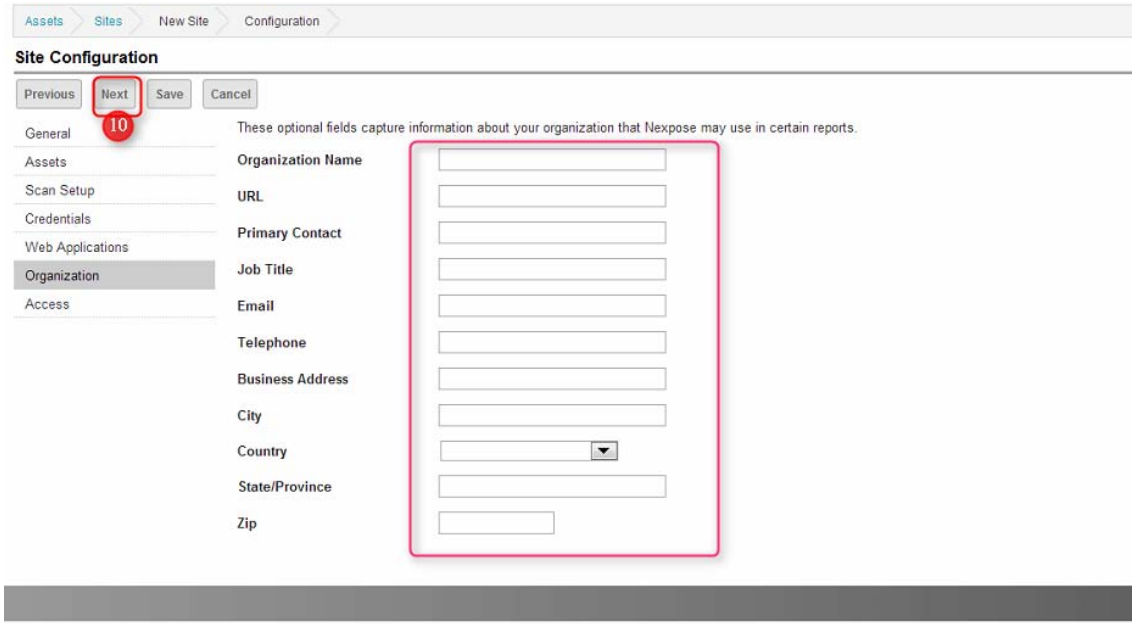


==========若不需要輸入帳戶資訊就請跳過以上步驟==========

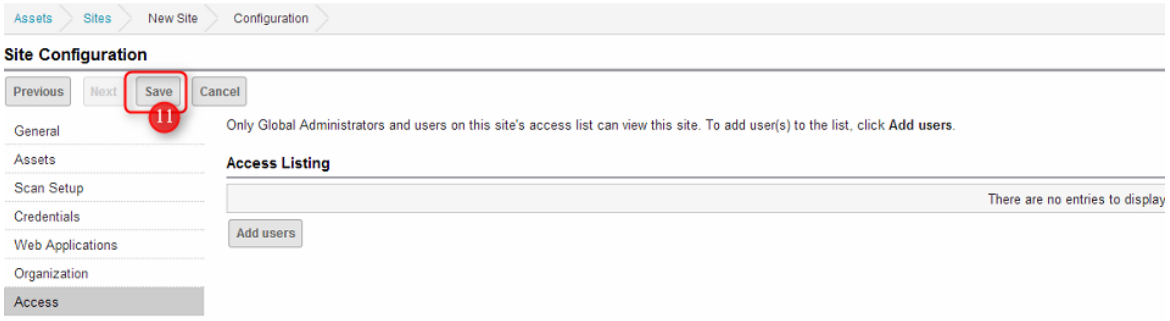
這裡如同先前的使用者帳戶資料，若有Web Applications需要登入做掃描也能輸入資料
繼續按下Next到下一步驟



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



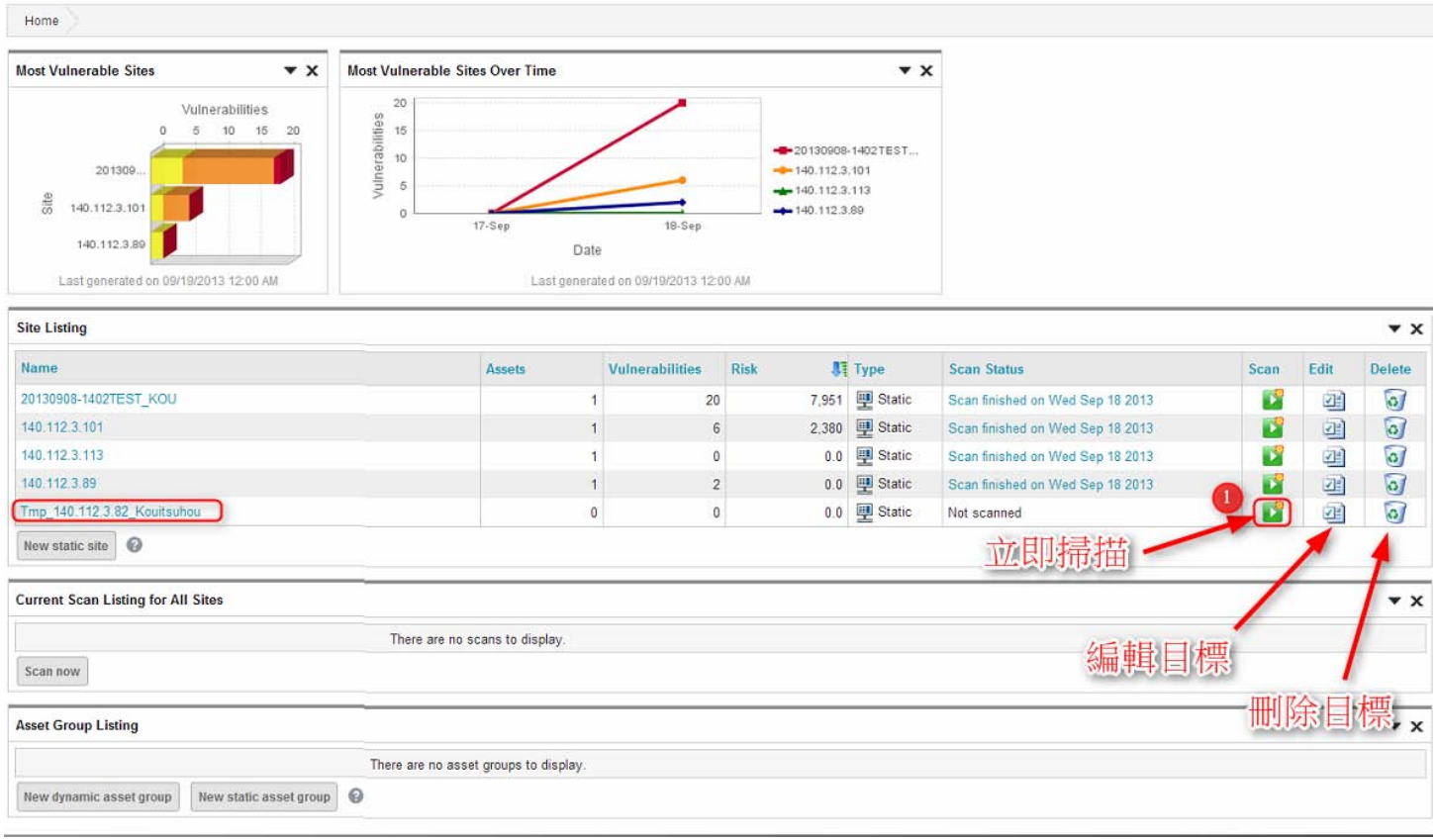
按下Save就可以完成建立



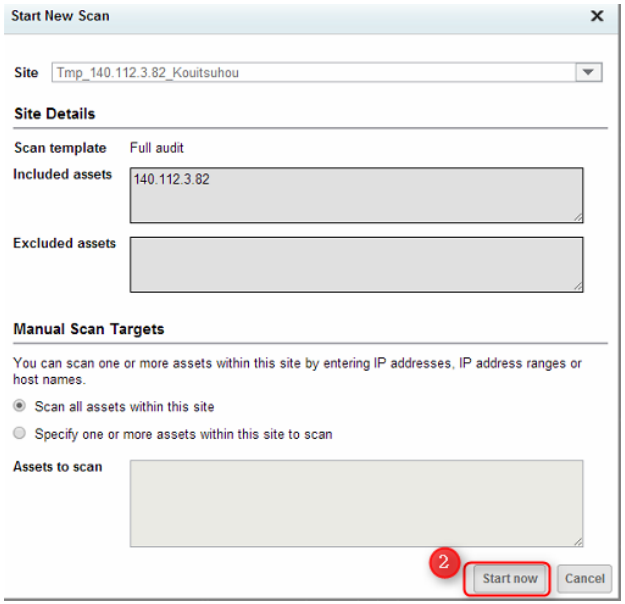
---

(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，以及被掃瞄到的弱點、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



接著會跳出視窗，按下Start now就會開始掃描



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

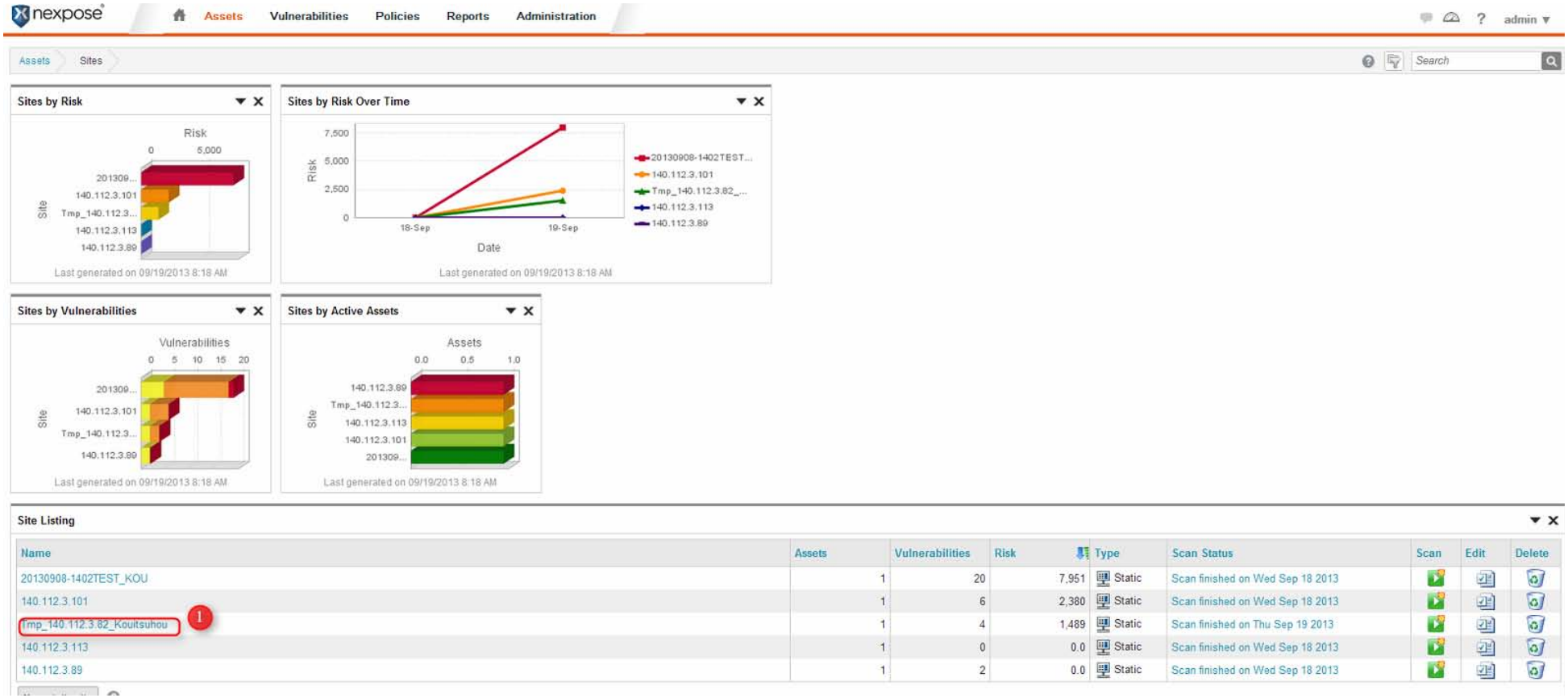
掃描通常很快，在十分鐘以內就能夠完成。這次掃描只花了25秒
若超過十分鐘則有可能設定目標時有資料誤植，此時就需要將目標刪除之後，另創新目標再度掃描

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用以下方式開啟

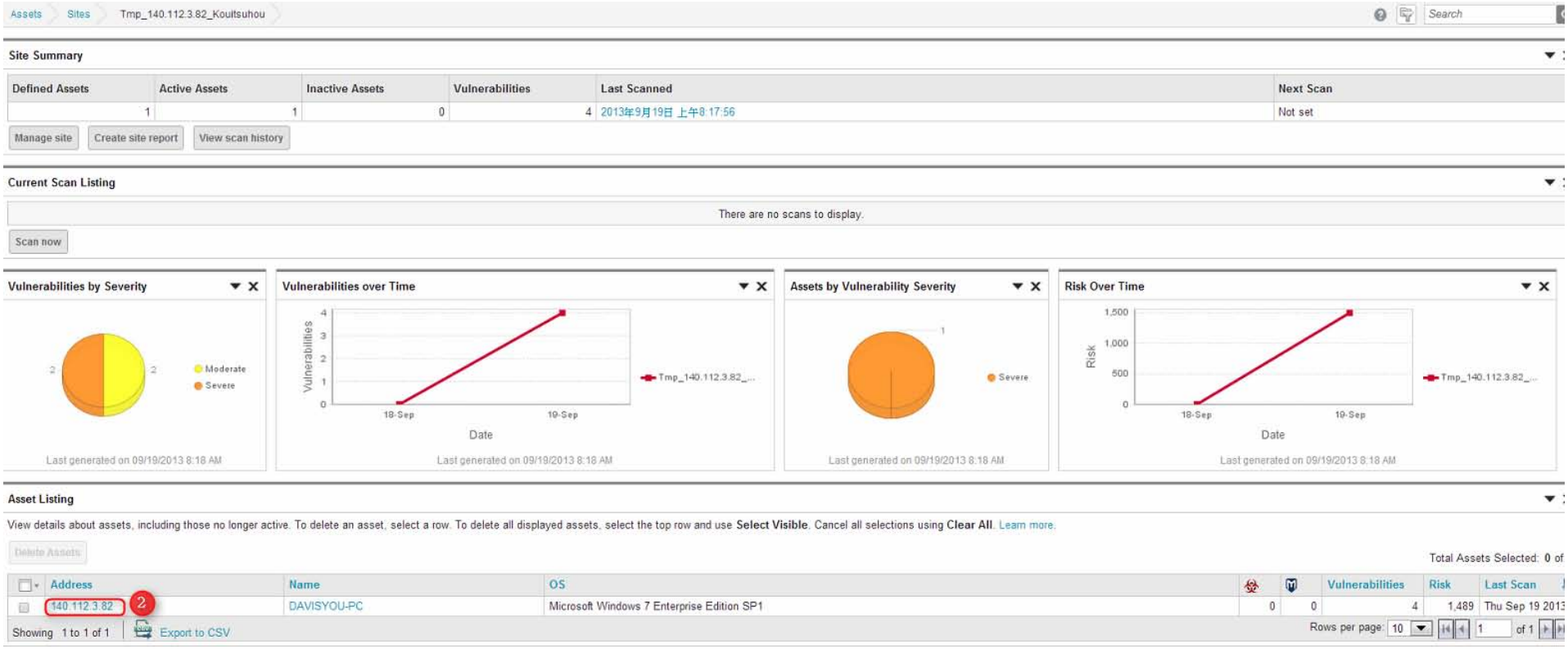
首先回到首頁，或者照前面步驟一樣按下上方的Assets→Sites View，接著按下我們所掃描的目標名稱



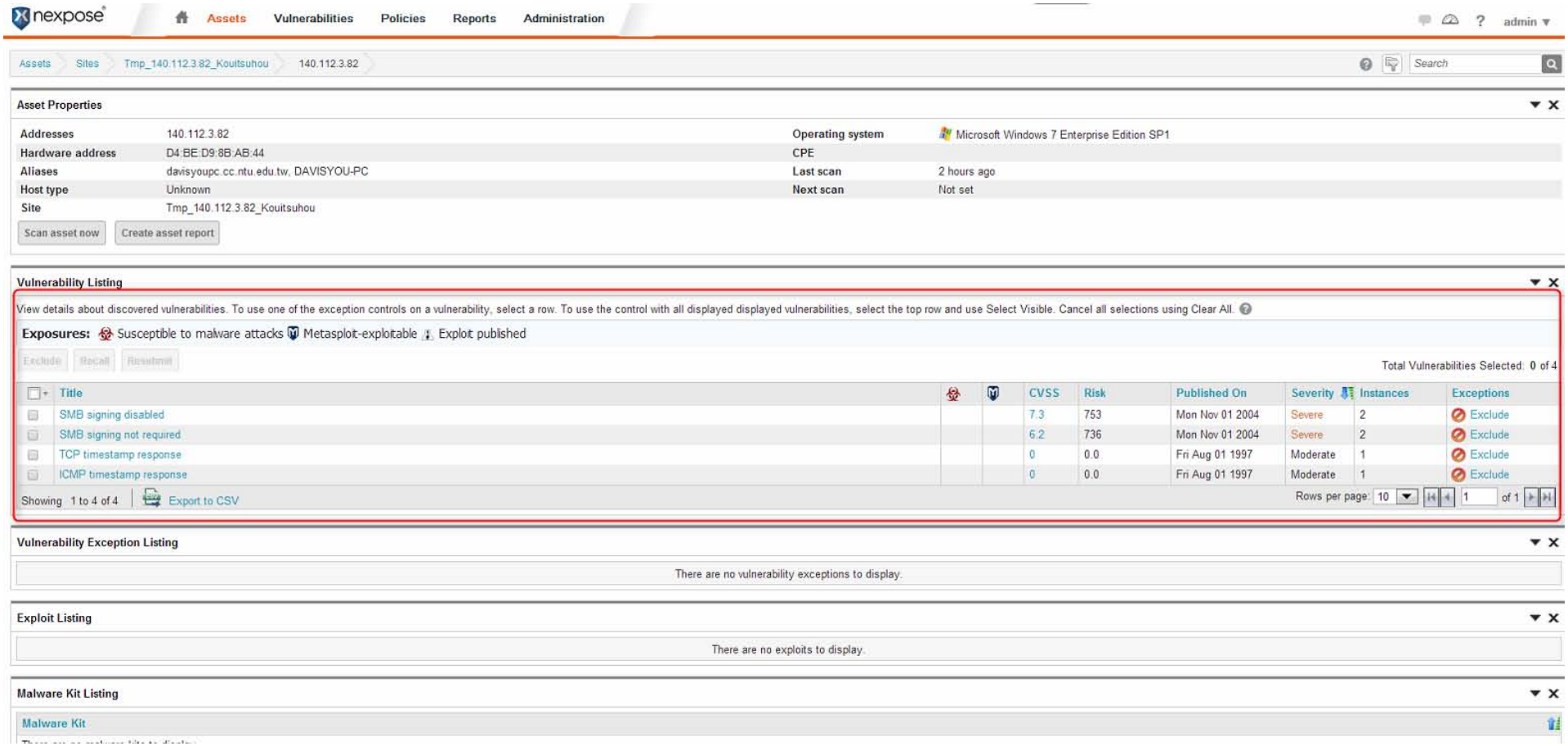
Site Listing

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_Kouitsuhou	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
按下下方想要找尋的特定IP



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



(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

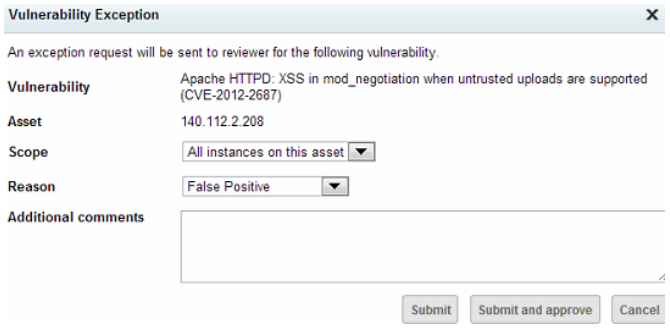
我們可以看到紅色的病毒圖示、藍底白字M圖示及白底三角形黑點圖示
若標題後方有出現紅色病毒圖示，則代表弱點有被惡意軟體來作為攻擊用途
若標題後方有藍底白字M圖示，則代表此弱點在Metasploit內含有工具，能夠以此弱點進行攻擊
若標題後方有白底三角形黑點圖示，則代表此弱點有建立在資料庫內，可以點選並自行編譯出來，然後攻擊

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Criticial為優先通報及處理

(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

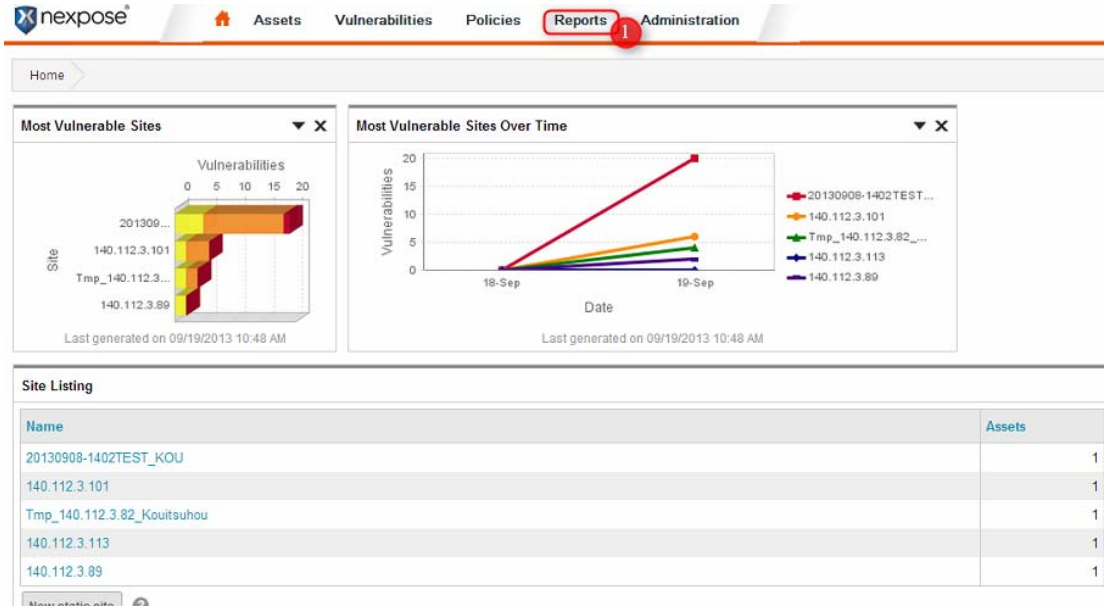
同上圖，最後面有個Exclude可以按，按了之後會跳出視窗，可以輸入刪除的原因
Scope可以選擇刪除這一次掃描內容的單個弱點，或是刪除其他所有掃描的相同弱點
Reason有內建數個原因可以選，或者將原因打入在下方Additional comments
再按下Submit即可



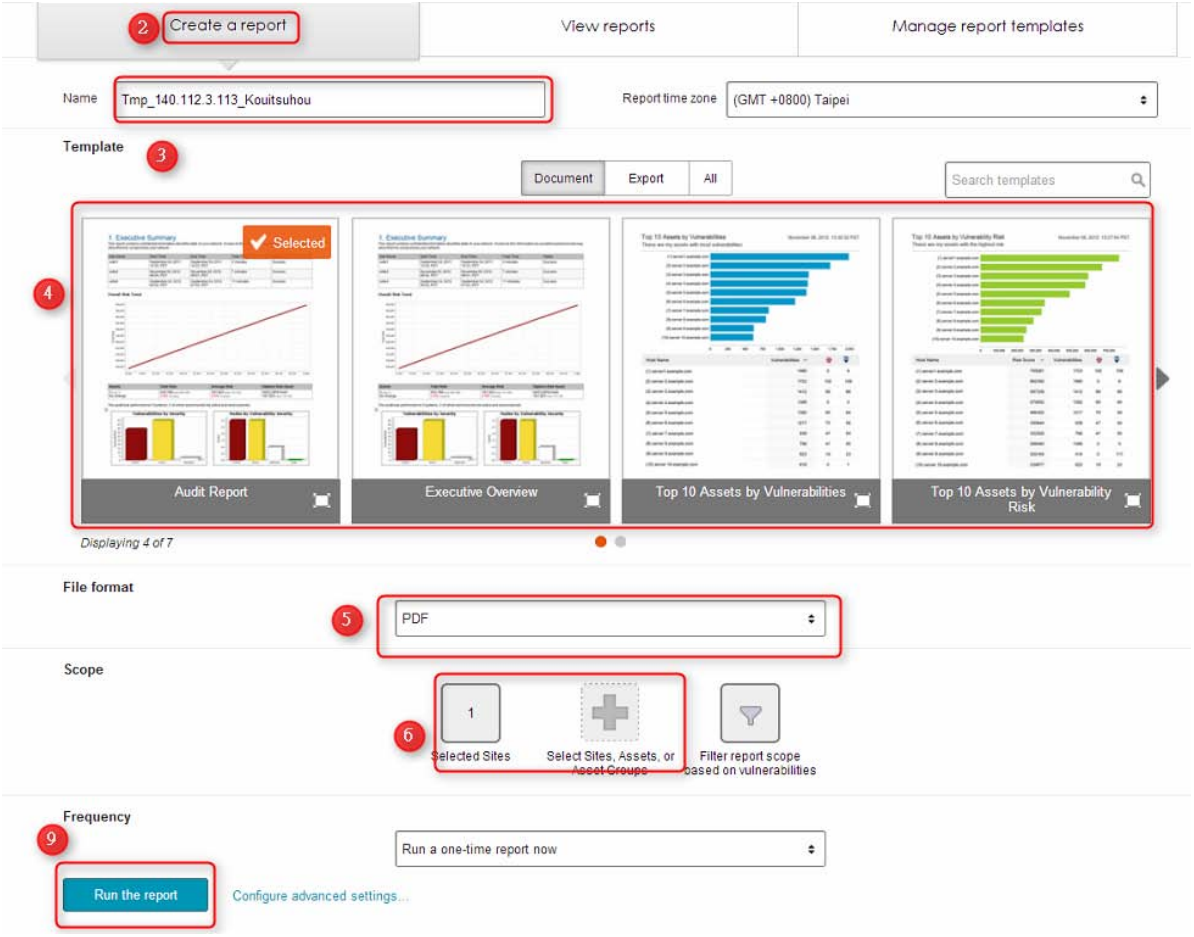
3.資料輸出

(1) 報表輸出

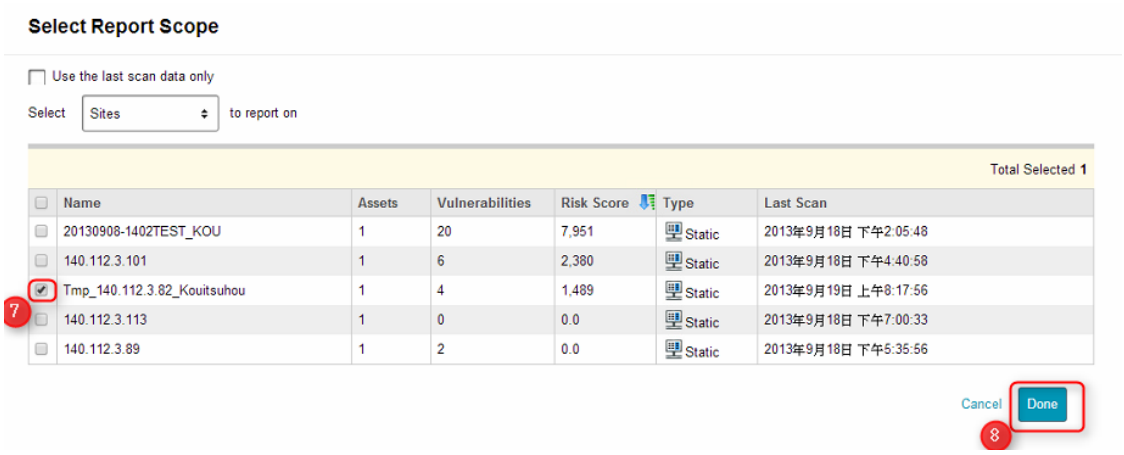
若要輸出報表，首先按下上方的Reports



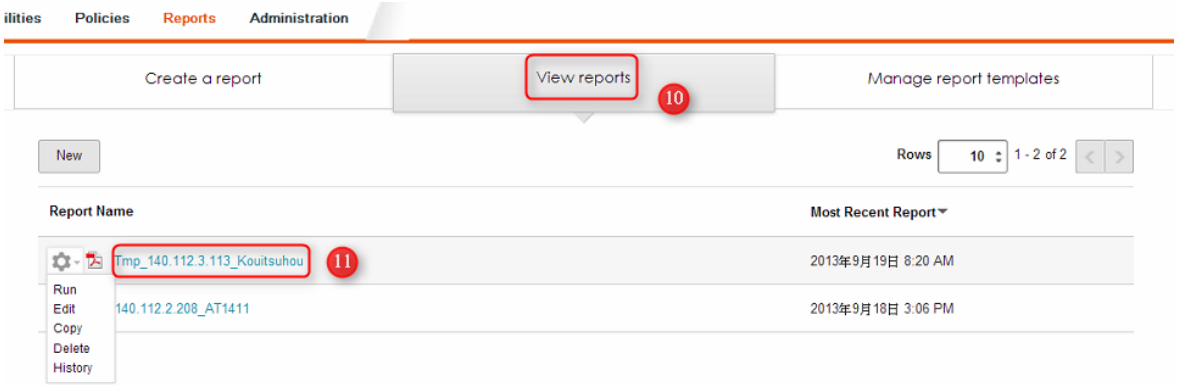
接著按下上方的Create a report，並輸入報告的名稱、選擇報告的種類、輸出格式(有PDF及HTML可選擇)
在Scope按下 Select Sites,Assets, or Asset Groups 的會跳出視窗，
選擇掃描過的目標並按下Done會回到Create a report的畫面
最後按下Run the report就會到View reports的頁面



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



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


ilities
Policies
Reports
Administration
Create a report
View reports
10
Manage report templates
New
Rows
10
1 - 2 of 2
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