

8. 弱點掃描

勞動部 產業人才投資計畫
中國文化大學 推廣教育部

張耀鴻 副教授
2022年 暑期班

綱要

- 弱點掃描概述和注意事項
- Nessus 弱點掃描
- Nmap 弱點掃描

弱點掃描概述和注意事項

- 弱點發現是任何資安評估的一個組成份子
- 雖然資安稽核期間常利用專業的知識和經驗手動執行任務
- 但在適當的環境中使用自動弱點掃描程序仍然是無價的
- 本單元將概述自動弱點掃描，討論其各種注意事項，並重點關注 **Nessus** 和 **Nmap** 作為不可或缺的工具
- 在深入研究工具之前，必須花一些時間討論弱點掃描過程，概述有關自動和手動掃描的基本注意事項，並討論關鍵的細微差別和最佳實務

Nessus 弱點掃描

- 弱點掃描器如何工作
- 手動與自動掃描
- Internet 掃描與內部掃描
- 認證與未認證掃描

弱點掃描器如何工作

- 弱點掃描程序通常遵循標準工作流程：
 1. 檢測目標是否已啟動並正在運行。
 2. 根據配置執行完整或部分通訊埠掃描。
 3. 使用常見的指紋辨識技術來識別操作系統。
 4. 使用常見技術，例如橫幅抓取(banner grabbing)、服務行為識別或檔案探索等，來辨識正在運行的服務。
 5. 執行簽名比對過程以發現弱點。

Banner Grapping

- 在簽名比對的過程中，許多掃描器使用橫幅抓取技術
- 這是一種簡單的技術，可以獲取並分析在與應用程式剛開始進行互動時所產生的文字字串
- 有些應用程式會產生非常特定的banner，例如 OpenSSH，它可能會傳回 "SSH-2.0-OpenSSH_7.9p1 Debian-1"，讓我們能夠精確判定應用程式版本
- Apache Tomcat 版本 4.1.x 到 8.0.x，會傳回 "Apache-Coyote/1.1" 的通用HTTP標頭
- 越具體的標頭和banner使掃描程序越容易確定應用程式版本，來準確檢測潛在的弱點

Backporting

- 大多數自動掃描器在簽名比對過程中檢查各種其他目標資訊
- 然而，即使是強簽名比對也不能保證存在弱點
- 這意味著自動掃描程序可以產生相當多的false positive誤報
- 反之，false negative漏報則由於簽名不符合而忽略了弱點
- 套件維護者將軟體安全補丁回滾到舊版本(稱為反向移植(backporting))，也可能出現誤報和漏報
- 當弱點實際上已修復時，反向移植可能會導致掃描程序將軟體標記為易受攻擊的版本。

手動掃描的時機

- 因此，我們應該盡可能仔細檢查並手動查看弱點掃描結果
- 鑑於不斷變化和複雜的技術環境，弱點可能會出現在意想不到的地方
- 沒有一個掃描器是完美的。但是在每次掃描之前更新簽名資料庫，可確保掃描程序有最好的機會發現最新的弱點
- 這種簽名比對過程非常有效，並且比完全手動掃描要快得多，建議第一次先用自動弱點掃描程式加以評估再決定是否需要手動掃描

手動與自動掃描的優缺點比較

- 我們應該在評估過程中結合手動和自動掃描技術
- 適當的平衡點會隨著經驗而變得更加明顯
- 對遠端目標網路的手動掃描將不可避免地耗費大量資源和時間
- 由於手動方法在很大程度上依賴於人工交談和重複性任務，因此也容易出現可能忽略弱點的錯誤
- 然而，駭客需要確保攻擊的精確度和留下最少的網路足跡，以便盡可能長時間地保持不被發現
- 使用自動掃描器比較容易被發現。此外，手動分析允許發現使用任何類型的自動掃描器都很難發現的複雜和邏輯弱點。
- 但是，在與傳統安全評估相關的典型時間限制下處理大型專案時，自動化弱點掃描程式非常寶貴

手動與自動掃描的優缺點比較（續）

- 無論是在整個目標網路上使用通用掃描器還是針對單一專用主機，自動掃描都可以在較短的時間內建立基線
- 這些基線使我們能夠驗證容易檢測到的弱點，或者至少幫助我們了解目標的一般安全狀況
- 雖然非常寶貴，但自動弱點掃描也有缺點。掃描配置可能是廣泛而複雜的，預設的設定可能會對目標造成損害
- 例如，許多掃描程式可以嘗試暴力破解弱密碼，在參與過程中，暴力破解技術應該受到嚴格監管
- 由於嘗試暴力破解可能導致帳號被鎖定，這可能會造成客戶帶來大量的停機時間
- 在執行掃描之前，了解弱點掃描程序的工作原理及其功能非常重要。
- 請記住，在使用自動弱點掃描程序時，滲透測試人員的工作是提供超出任何工具輸出的價值

Internet 掃描與內部掃描

- 弱點掃描程式可以輕鬆掃描連接到 Internet 的目標以及連接到本地網路的目標
- 但是，如果我們平等對待這些目標，我們的掃描結果可能不完整或不準確
- 相對於目標的網路位置會影響速度閾值、存取權限、流量干擾的可能性和目標可見性
- 與目標網路的連接速度不僅決定了掃描器可用的原始頻寬，也決定了其他因素，例如到各個主機的躍點數
- 這意味著我們可以更快地對本地連接的主機進行更具侵入性和全面的掃描
- 但是，必須時刻注意流量，意識到舊設備可能會受到重度掃描的不利影響
- 為獲得最佳結果，請考慮前述的通訊埠掃描

目標網路位置的考量

- 網路位置會影響目標的可見性。例如，典型的弱點掃描器會嘗試使用 ping 掃描或 ARP 掃描來發現目標
- 但是，連接到 Internet 的目標將無法接收來自外部子網的 ARP 流量，並且可能會阻止 ICMP（ping）請求
- 這意味著掃描器如果設定為僅依賴 ping 掃描或 ARP 掃描選項，則可能會完全錯過目標
- 弱點掃描前需要花時間徹底了解目標網路、將使用的確切網路位置、以及網路位置提供了哪些目標存取方式
- 了解您的工具以及它們如何在幕後工作非常重要^{P.12}

認證與未認證掃描

- 大多數掃描器可以配置為運行經過身份驗證的掃描，其中掃描器使用一組有效憑據登錄到目標
- 在大多數情況下，經過身份驗證的掃描會使用特權帳號，以便獲得對目標系統的最佳可見性
- 要對 Linux 目標運行經過身份驗證的掃描，只需在 Linux 目標上啟用 SSH 服務並使用有效的使用者憑證來配置掃描器
- 大多數掃描程式將以此存取權限來查看套件版本並驗證配置，以嘗試發現潛在的弱點

Windows Management Instrumentation

- Windows 身份驗證通常需要 Windows 管理規範 (Windows Management Instrumentation, WMI) 以及具有遠端管理權限的網域或本地帳號的憑證
- 請注意，即使配置了 WMI，其他因素也可能會阻止身份驗證，包括 UAC 和防火牆設置
- 但是，一旦正確配置了存取權限，大多數掃描式都會分析系統配置、註冊表設置以及應用程式和系統補丁層級
- 他們還會審查 Program Files 目錄中的檔案以及 Windows 資料夾中的所有可執行檔和 DLL，這些都是為了檢測潛在的易受攻擊的軟體
- 經過身份驗證的掃描會產生大量附加資訊，並以更長的掃描時間為代價產生更準確的結果

Nessus 弱點掃描

- 安裝 Nessus
- 定義目標
- 配置掃描定義
- 使用Nessus進行未經身份驗證的掃描
- Nessus認證掃描
- 使用單個 Nessus 插件進行掃描

安裝 Nessus

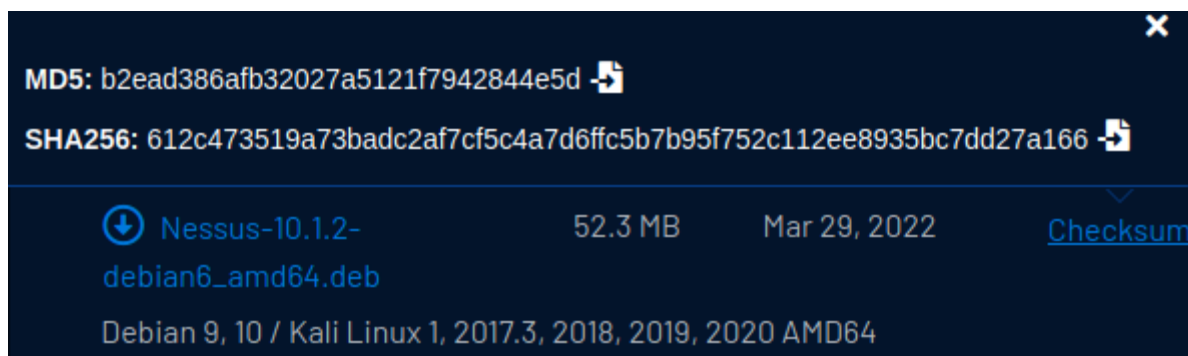
- Nessus 是一個相當強大的行業標準
- 免費的 “Essentials” 版本可掃描 16 個 IP
- 本節討論的總體概念通常也適用於其他商業掃描器
- VM 上需另外安裝 Nessus，在開始安裝之前，應更新 Kali 的套件清單並將現有封包升級最新版本：

```
└─$ sudo apt update && sudo apt upgrade
```

- 應注意弱點掃描程式通常為資源密集型，建議最低要求包括至少 2 個 CPU 核心以及 8GB 的 RAM

安裝 Nessus (續)

- 從以下網址下載Debian 64bit版(.deb)的Nessus:
<https://www.tenable.com/downloads/nessus>



- 可在命令列執行sha256sum，和網頁上的Checksum比對檔案的完整性

```
$ sha256sum Nessus-10.1.2-debian6_amd64.deb
612c473519a73badc2af7cf5c4a7d6ffc5b7b95f752c112ee8935bc7dd27a166
```

安裝 Nessus (續)

➤ 安裝Nessus套件

```
└─$ sudo apt install ./Nessus-10.1.2-debian6_amd64.deb
Reading package lists ... Done
Building dependency tree ... Done
```

➤ 安裝完成後畫面會出現以下訊息:

```
Preparing to unpack ... /Nessus-10.1.2-debian6_amd64.deb ...
Unpacking nessus (10.1.2) ...
Setting up nessus (10.1.2) ...
Unpacking Nessus Scanner Core Components ...

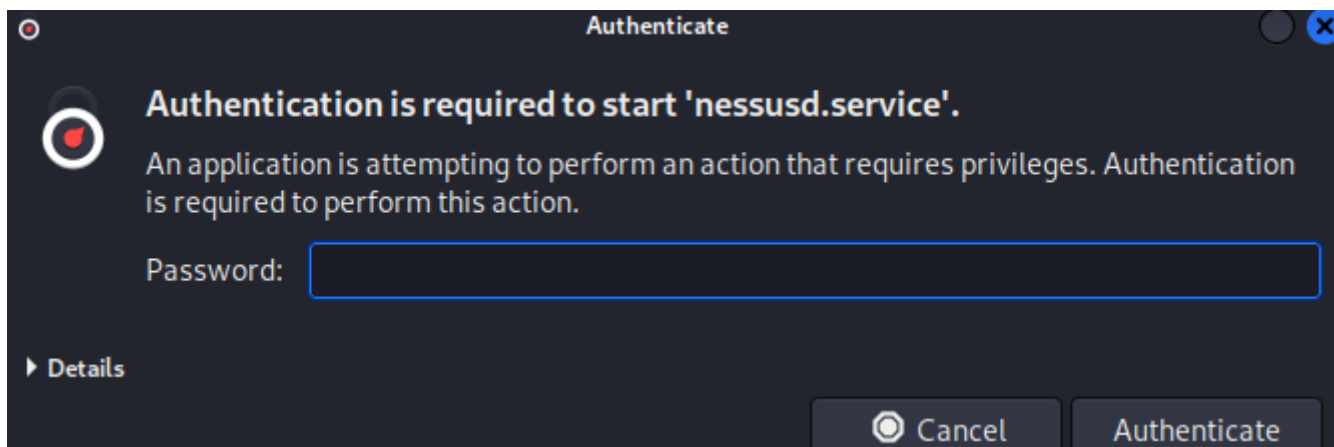
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

➤ 啟動nessusd服務:

```
└─$ /bin/systemctl start nessusd.service
```

安裝 Nessus (續)

- 彈出驗證視窗，輸入kali密碼



- 用firefox開啟網頁 <https://kali:8834>
- 會出現安全性警告，按Advanced接受並確認

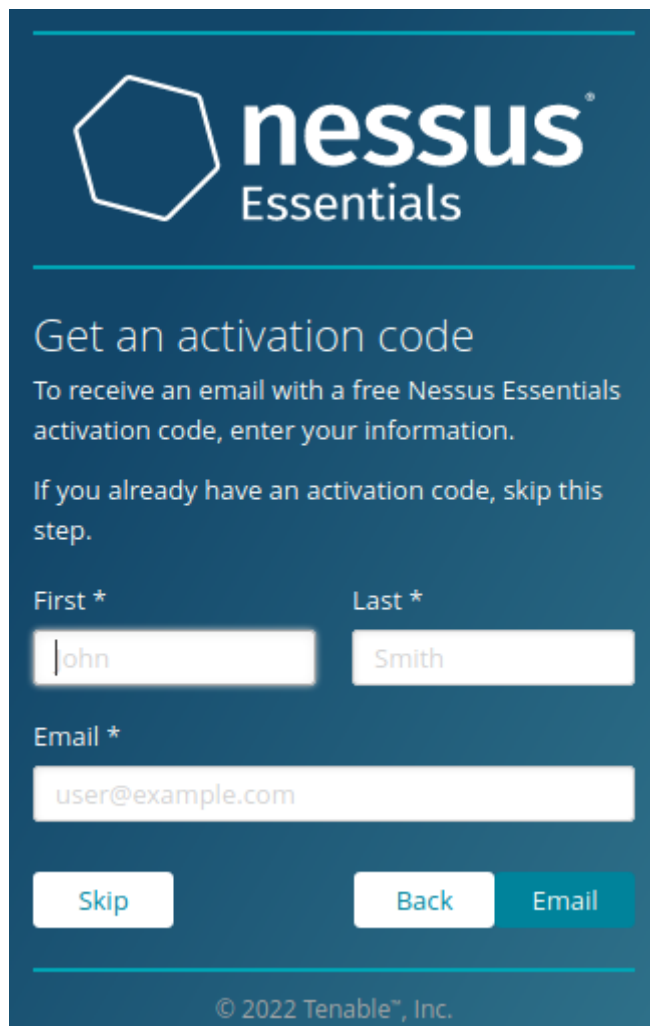
安裝 Nessus (續)

➤ 選"Nessus Essentials"，按Continue



安裝 Nessus (續)

- 輸入email獲取激活碼



The image shows a web form for obtaining a Nessus Essentials activation code. The form has a dark blue header with the Nessus logo and title. Below the header, there is a section titled 'Get an activation code' with instructions. The form includes input fields for 'First *', 'Last *', and 'Email *'. The 'First *' field contains 'John', the 'Last *' field contains 'Smith', and the 'Email *' field contains 'user@example.com'. At the bottom, there are three buttons: 'Skip', 'Back', and 'Email'.

nessus[®]
Essentials

Get an activation code

To receive an email with a free Nessus Essentials activation code, enter your information.

If you already have an activation code, skip this step.

First * Last *

John Smith

Email *

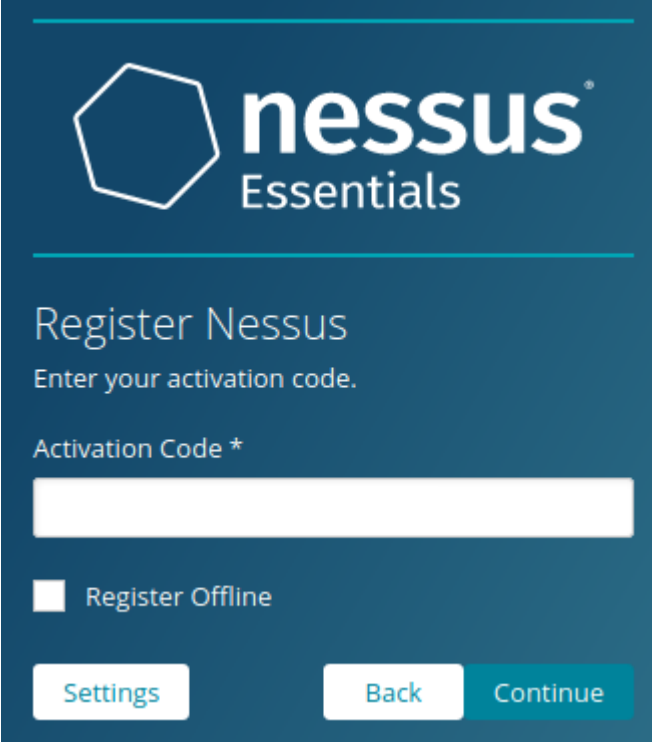
user@example.com

Skip Back Email

© 2022 Tenable[™], Inc.

安裝 Nessus (續)

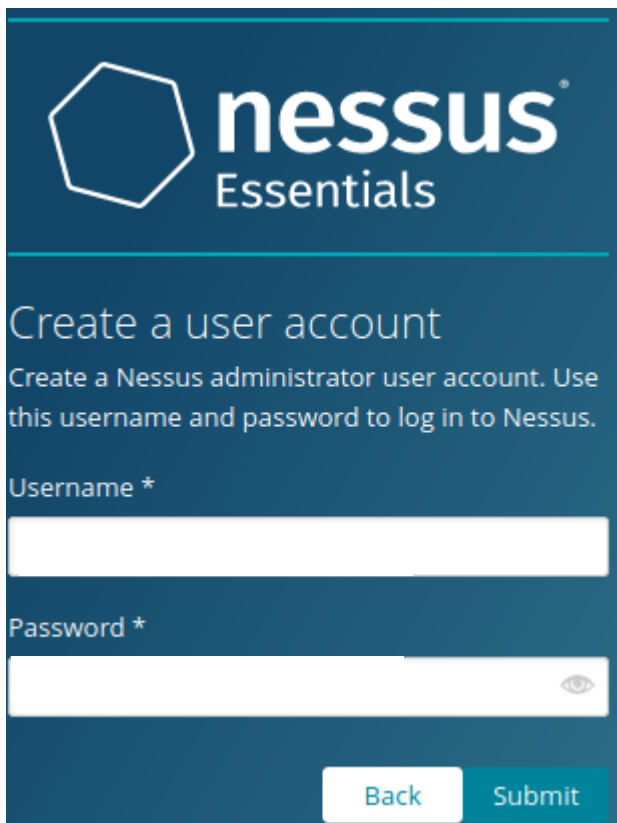
➤ 輸入激活碼



The image shows the Nessus Essentials registration interface. At the top, there is the Nessus logo (a blue hexagon) and the text "nessus Essentials". Below this, the heading "Register Nessus" is followed by the instruction "Enter your activation code." A label "Activation Code *" is positioned above a white text input field. Below the input field, there is a checkbox labeled "Register Offline". At the bottom, there are three buttons: "Settings" (white with blue text), "Back" (white with blue text), and "Continue" (blue with white text).

安裝 Nessus (續)

- 建立本機使用者帳號密碼



The image shows a web form for creating a user account in Nessus Essentials. The form has a dark blue header with the Nessus logo and the text "nessus Essentials". Below the header, the title "Create a user account" is displayed, followed by a subtitle: "Create a Nessus administrator user account. Use this username and password to log in to Nessus." The form contains two input fields: "Username *" and "Password *". The "Password *" field has a toggle icon (an eye) to the right of the input box. At the bottom of the form, there are two buttons: "Back" and "Submit".

nessus[®]
Essentials

Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

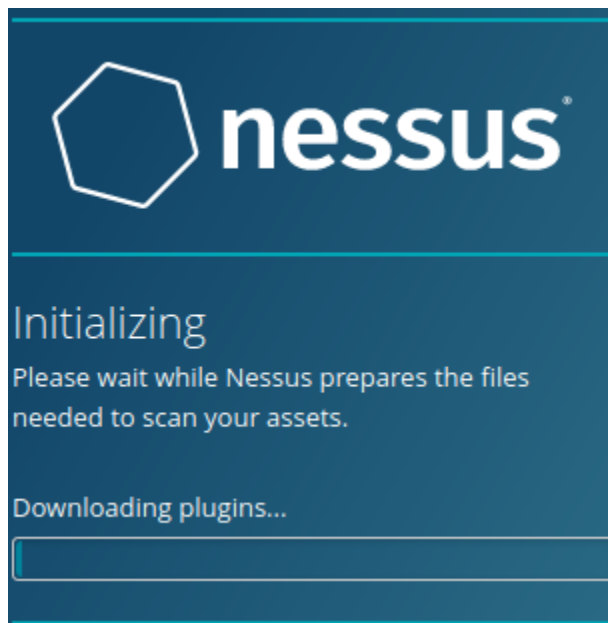
Username *

Password *

Back Submit

安裝 Nessus (續)

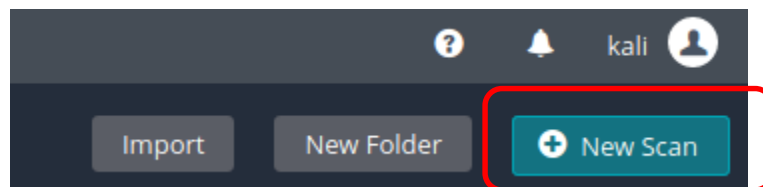
➤ 自動下載plugins



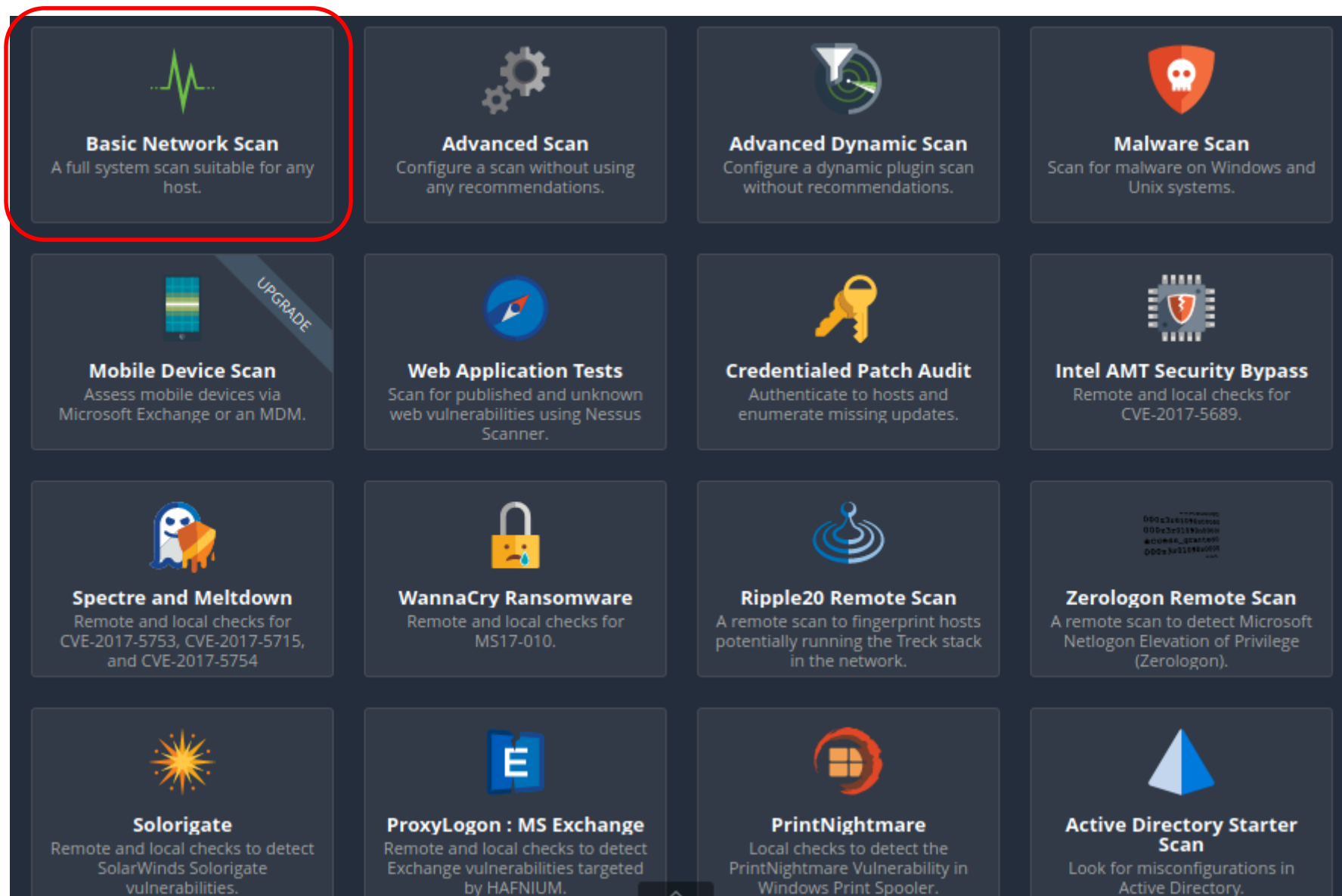
定義目標

- Nessus 支援多種掃描類型，包括：
 - ✓ Basic Network Scan (基本網路掃描)：適用於各種目標類型檢查的通用掃描。
 - ✓ Credentialed Patch Audit：經過身份驗證的掃描，列舉缺少的補丁。
 - ✓ Web Application Tests (Web 應用程式測試)：用來發現 Web 應用程式中已發布弱點的專門掃描。
 - ✓ Spectre and Meltdown：針對 Spectre 和 Meltdown 弱點的針對性掃描。
- 本單元主要介紹 Basic Network Scan

-
- Nessus安裝完成後就可以按“New Scan”開始第一次掃描：



Nessus支援的掃描類型: (選Basic Network Scan)



➤ 輸入掃描名稱和目標IP位址

New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name Metasploitable - Basic

Description

Folder My Scans

Targets 10.0.2.7

配置掃描定義

- 基本網路掃描模板(以及所有其他模板)，有預先配置的預設設置
- 但是，這些預設值可能不是我們所要的
- 我們必須考慮我們的環境、時間限制和將要掃描的目標
- 配置基本網路掃描模板時需要考慮的一些事項包括：
 - ✓ 目標是位於內部網路還是可以公開存取？
 - ✓ 掃描程序是否應該嘗試暴力破解用戶帳號密碼？
 - ✓ 掃描器應該掃描所有 TCP 和 UDP 通訊埠還是只掃描公開通訊埠？
 - ✓ 掃描器應該執行哪些檢查，應該避免哪些檢查？
 - ✓ 掃描器應該執行經過身份驗證的掃描還是未經身份驗證的掃描？

- 這次掃描，我們希望對所有通訊埠執行初始基本通訊埠掃描
- 預設情況下，基本網路掃描只會掃描公開通訊埠
- 要更改此設置，可按一下左側“Settings”標籤下的“Discovery”。

New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY (highlighted with a red box)

ASSESSMENT

REPORT

ADVANCED

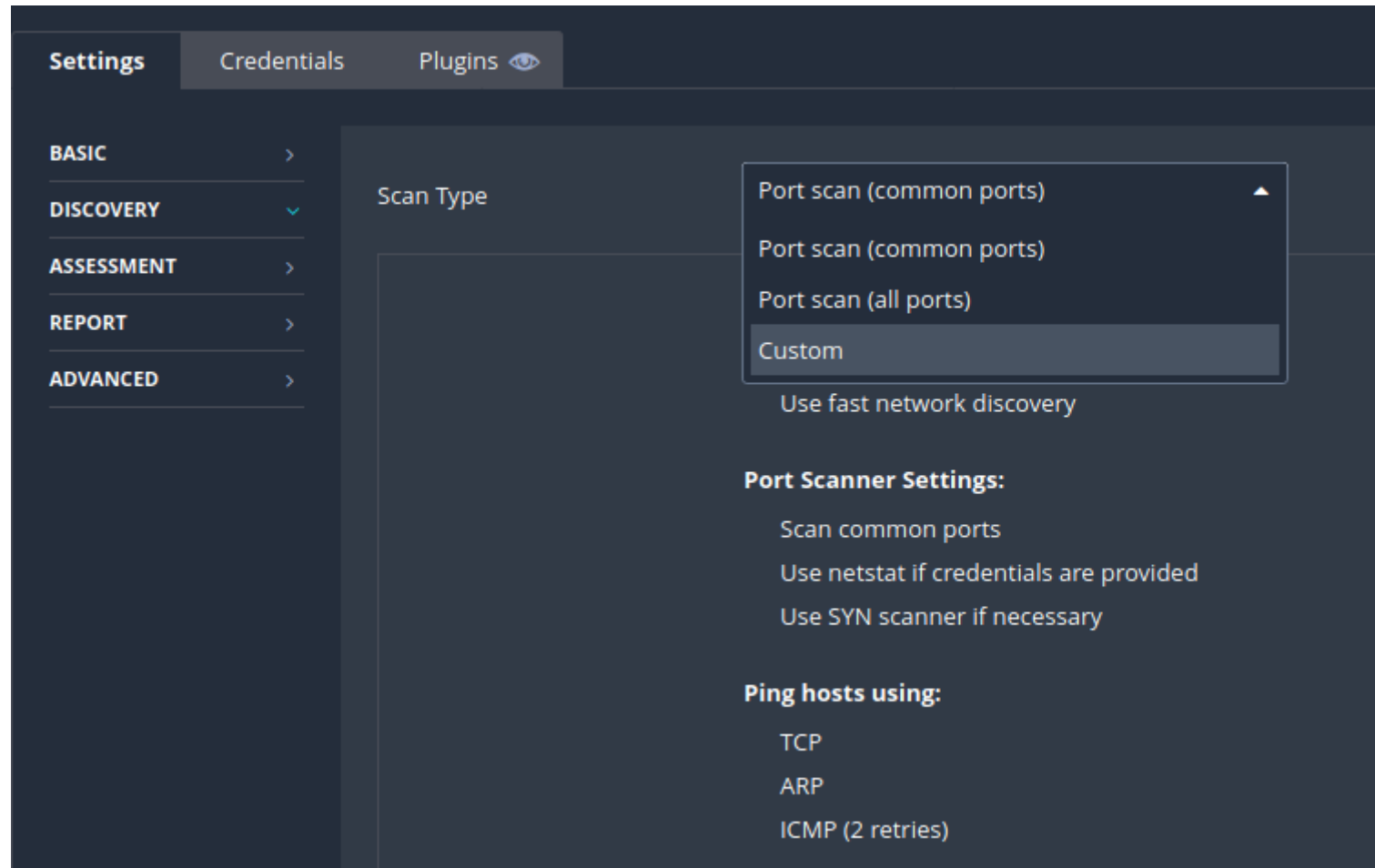
Name: Metasploitable - Basic

Description:

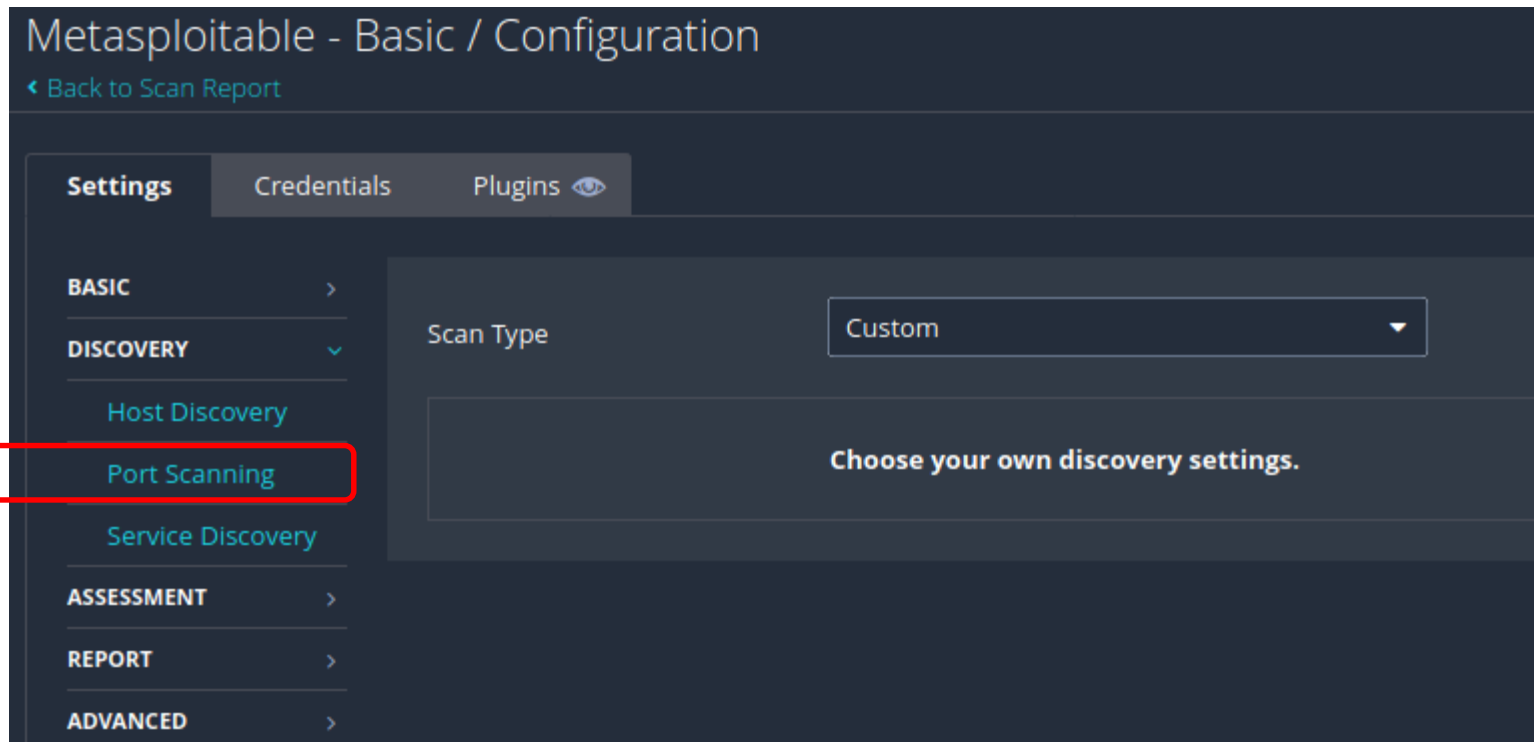
Folder: My Scans

Targets: 10.0.2.7

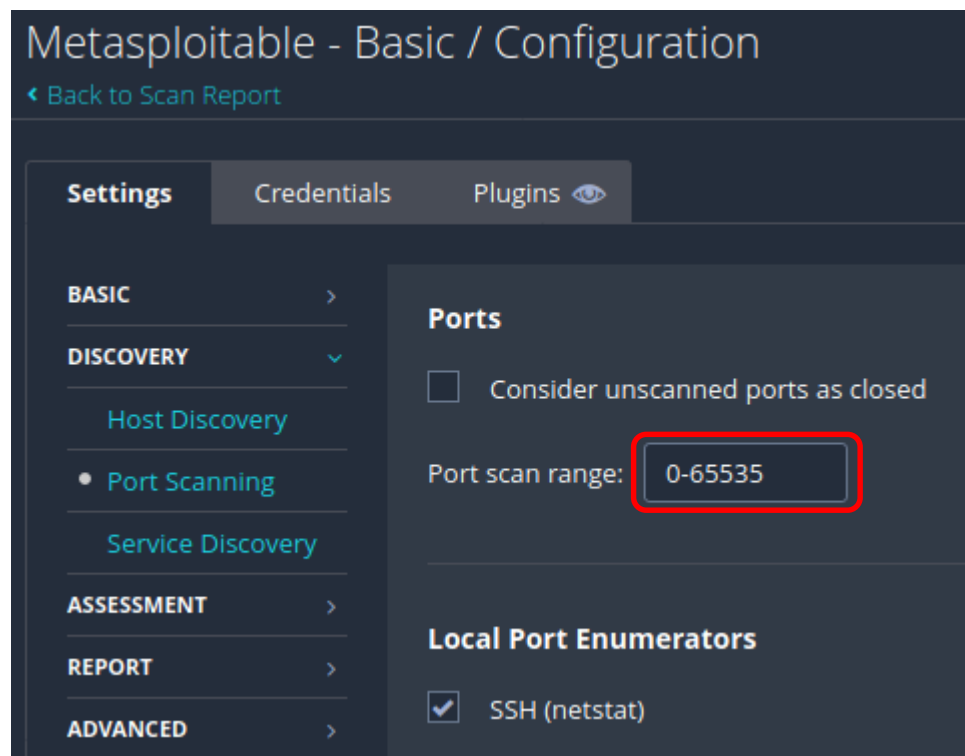
- 把Scan Type 的 Port scan (common ports) 改成 Custom



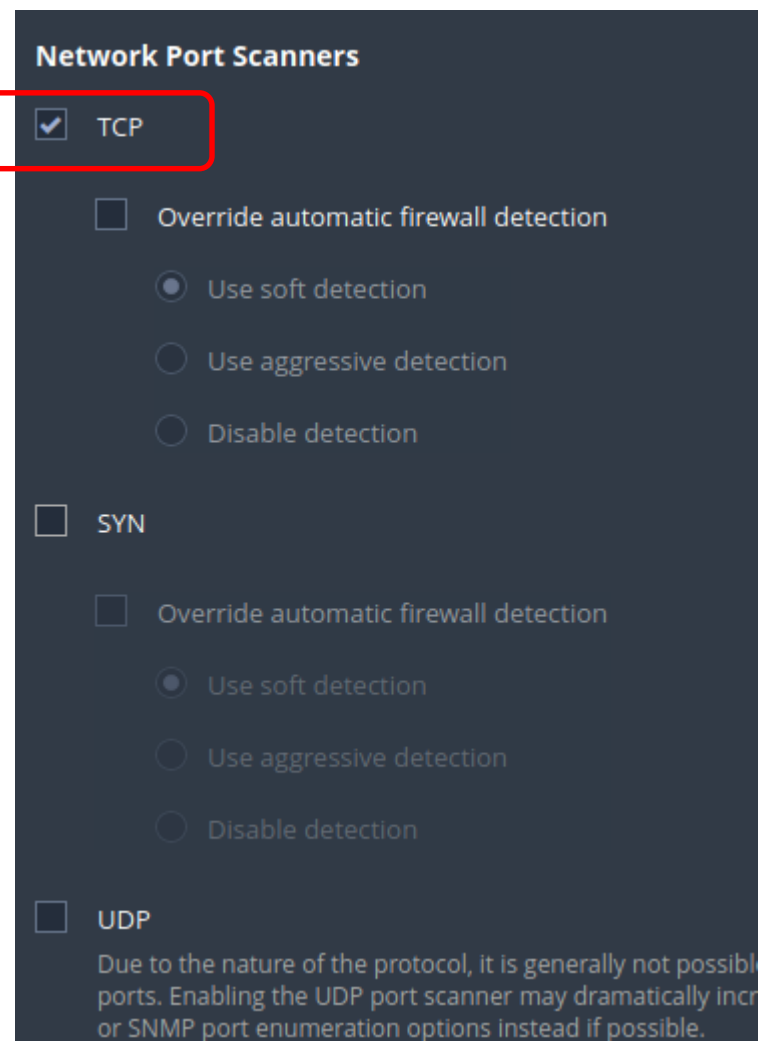
- 這會在DISCOVERY之下再加上Port Scanning 和 Service Discovery選項
- 按一下Port Scanning來配置通訊埠範圍：



- 把 Port scan range 改成 0-65535，以便掃描所有通訊埠：



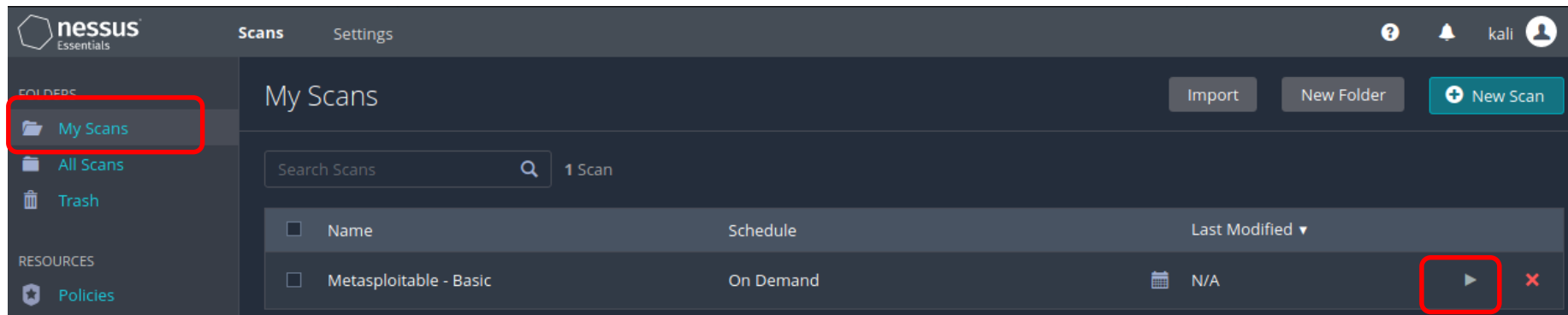
- 在本例中，我們選擇了一個掃描定義，會掃描所有 TCP 通訊埠，但不掃描 UDP 通訊埠
- 雖然這會提高掃描速度，但可能會錯過目標上運行的關鍵服務
- 在參與期間，我們必須在配置通訊埠掃描選項時權衡目標網路的穩定性、目標的範圍、參與的持續時間以及許多其他因素。



-
- 在掃描定義的配置過程中，我們沒有配置任何帳號密碼
 - 這意味著此掃描將在未經身份驗證的情況下運行
 - 此外，我們接受了基本網路掃描下的預設設置，這意味著不會啟用用戶帳密的暴力破解
 - 如果我們查看基本網路掃描下的其他選項，我們可以驗證掃描將針對目標運行通用檢查，而其他模板（如Spectre和Meltdown）則包括特定的弱點檢查
 - 請記住，像這樣配置的掃描所產生的網路流量將非常引人注目，因為它會掃描所有通訊埠並蒐集所有適用的弱點。

使用Nessus進行未經身份驗證的掃描

- 設置好Custom掃描後，可按Save儲存



- 按一下My Scan回到掃描頁面，再按一下右邊的三角形(Launch)
- 一開始會顯示狀態為Running
- 掃描結束會顯示狀態為Completed

- 掃描時間會因許多因素而異，例如掃描配置和網路速度
- 在“**My Scan**”頁面按一下掃描名稱 **Metasploitable - Basic**，可顯示在掃描過程中發現的主機清單以及潛在弱點的細項：

Metasploitable - Basic

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to My Scans](#)

Hosts 1 **Vulnerabilities** 71 **Remediations** 3 **VPR Top Threats** **History** 1


Filter Search Hosts 1 Host

Host	Vulnerabilities
<input type="checkbox"/> 10.0.2.7	11 5 30 6 136

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:09 AM
End: Today at 10:20 AM
Elapsed: 11 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

➤ 按一下 IP 地址或主機名可顯示針對該目標發現的弱點：

Metasploitable - Basic / 10.0.2.7

Configure Audit Trail Launch Report Export

Back to Hosts

Vulnerabilities 71

Filter Search Vulnerabilities 71 Vulnerabilities

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼	
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Ser...	Service detection	1	
<input type="checkbox"/>	CRITICAL	10.0	Unix Oper...	General	1	
<input type="checkbox"/>	CRITICAL	10.0 *	UnrealIRC...	Backdoors	1	
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Serve...	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell ...	Backdoors	1	
<input type="checkbox"/>	CRITICAL	...	2 SSL (...)	Gain a shell remotely	3	
<input type="checkbox"/>	MIXED	...	2 SSL (...)	Service detection	3	

Host Details

IP: 10.0.2.7
MAC: 08:00:27:4A:3F:E3
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 10:09 AM
End: Today at 10:20 AM
Elapsed: 11 minutes
KB: [Download](#)

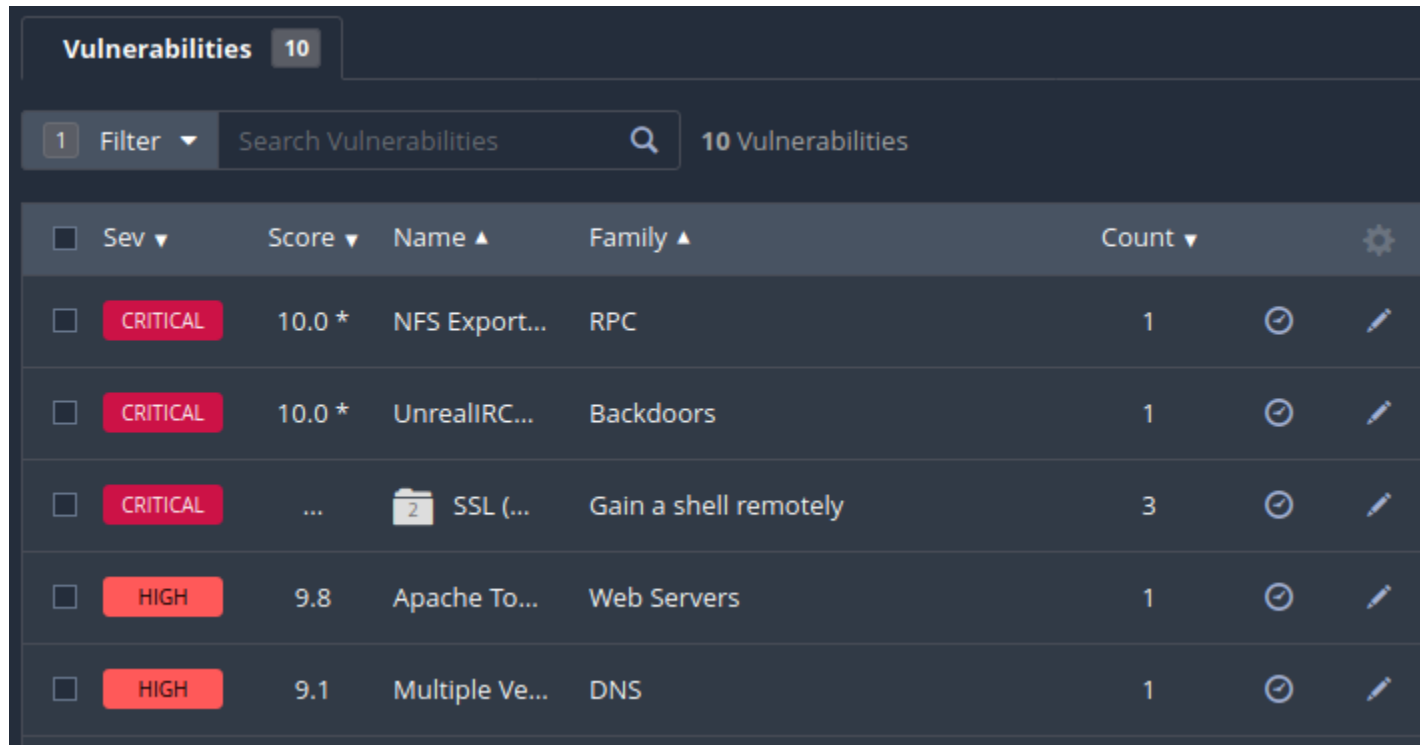
Vulnerabilities

Legend: Critical, High, Medium, Low, Info

- 可以按照嚴重性、可利用性、**CVE** 等過濾這些弱點
- 要顯示最有可能導致目標入侵的弱點，可以按一下**Filter**並將結果面板上的下拉列表改為"**Exploit Available**"(可利用弱點)，接受預設值"**is equal to**"(等於)"**true**"(真) 然後按"**Apply**"

The screenshot shows a 'Filters' dialog box with a dark background. At the top left is the title 'Filters' and a red close button 'X' at the top right. Below the title, there is a section 'Match' with a dropdown menu set to 'All', followed by the text 'of the following:'. Below this, there is a filter rule configuration area. It consists of three dropdown menus: the first is set to 'Exploit Available', the second is set to 'is equal to', and the third is set to 'true'. Each of these three dropdown menus is highlighted with a red rectangular box. To the right of the third dropdown is a plus sign icon '+'. At the bottom of the dialog, there are three buttons: 'Apply' (highlighted with a red box), 'Cancel', and 'Clear Filters'.

➤ 這將顯示 Nessus 所定義不同組別的弱點列表：



Vulnerabilities 10						
1	Filter	Search Vulnerabilities		10 Vulnerabilities		
<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	🕒 ✎
<input type="checkbox"/>	CRITICAL	10.0 *	UnrealIRC...	Backdoors	1	🕒 ✎
<input type="checkbox"/>	CRITICAL	...	2 SSL (...)	Gain a shell remotely	3	🕒 ✎
<input type="checkbox"/>	HIGH	9.8	Apache To...	Web Servers	1	🕒 ✎
<input type="checkbox"/>	HIGH	9.1	Multiple Ve...	DNS	1	🕒 ✎

- 按一下列表右上方的齒輪，選“Disable Groups”
會依嚴重程度列出弱點，顯示目標可能遭到攻擊
的風險，由大到小排列，而這正是我們所要的

1

Filter

Search Vulnerabilities

11 Vulnerabilities

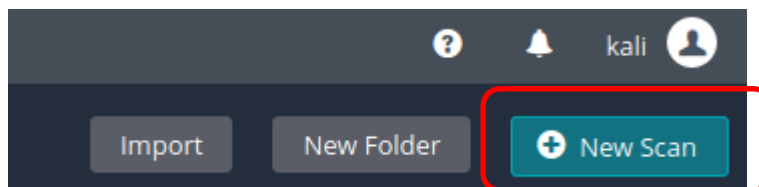
<input type="checkbox"/>	Sev	Score	Name	Family	Count	
<input type="checkbox"/>	CRITICAL	10.0 *	Debian Op...	Gain a shell remotely	2	
<input type="checkbox"/>	CRITICAL	10.0 *	Debian Op...	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	
<input type="checkbox"/>	CRITICAL	10.0 *	UnrealIRC...	Backdoors	1	
<input type="checkbox"/>	HIGH	9.8	Apache To...	Web Servers	1	
<input type="checkbox"/>	HIGH	9.1	Multiple Ve...	DNS	1	

Exercise 8-1

1. 按照上述步驟建立您自己的unauthenticated scan。
2. 在開啟 Wireshark 時執行掃描，並確認scanner為完成掃描所需執執行的步驟。
3. 查看掃描結果。

















Nessus認證掃描

- 執行經過身份驗證的掃描(authenticated scan)可產生更詳細的資訊並減少誤報(false positive)，這需要有效的目標帳密
- 為了證明經過身份驗證的掃描的價值，我們將對metasploitable執行authenticated scan
- 但請記住，大多數情況下，未經目標網路管理員的明確許可和明確溝通，不要任意執行經過身份驗證的掃描，因為production系統意外中斷的潛在風險更高
- 首先，按一下“New Scan”按鈕開始掃描。



-
- 這次改用 **Credentialed Patch Audit** 掃描模板
 - 該模板已預先配置為針對目標執行本機安全檢查
 - 此模板不僅會掃描操作系統缺少的補丁，還會掃描可能容易受到權限提升等攻擊向量影響的過時應用程式。

➤ 點選"Credentialed Patch Scan"

 Basic Network Scan A full system scan suitable for any host.	 Advanced Scan Configure a scan without using any recommendations.	 Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.	 Malware Scan Scan for malware on Windows and Unix systems.
 Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.	 Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner.	 Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	 Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.
 Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754	 WannaCry Ransomware Remote and local checks for MS17-010.	 Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.	 ZeroLogon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (ZeroLogon).
 Solorigate Remote and local checks to detect SolarWinds Solorigate vulnerabilities.	 ProxyLogon : MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.	 PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.	 Active Directory Starter Scan Look for misconfigurations in Active Directory.

➤ 輸入掃描名稱和IP位址

The screenshot shows the 'New Scan / Credentialed Patch Audit' interface. The 'Credentials' tab is selected and highlighted with a red box. The 'Name' field contains 'Metasploitable - Auth' and is also highlighted with a red box. The 'Targets' field contains '10.0.2.7' and is highlighted with a red box. The left sidebar shows a navigation menu with sections: BASIC (General, Schedule, Notifications), DISCOVERY, ASSESSMENT, REPORT, and ADVANCED.

New Scan / Credentialed Patch Audit

[Back to Scan Templates](#)

Settings **Credentials** Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Metasploitable - Auth

Description:

Folder: My Scans

Targets: 10.0.2.7

➤ 接下來，按一下 Credentials 選項標籤和 SSH 類別

- 在 Authentication method 下拉列表中，選擇 Password，將使用者名稱設為 “root” 並輸入密碼：

New Scan / Credentialed Patch Audit

[← Back to Scan Templates](#)

Settings **Credentials** Plugins

CATEGORIES Host ▼

Filter Credentials

SNMPv3

SSH

Windows

▼ SSH

Authentication method

Username

Password (unsafe!)

- 雖然在此只示範使用 SSH 配置，但我們可以按一下“Categories”下拉式選單，並選擇“All”查看其他 Nessus 支援的身份驗證機制

Metasploitable - Auth / Configuration

[← Back to Scan Report](#)


Settings Credentials Plugins

CATEGORIES **All** ▼

Filter Credentials

▶ SSH User: root, Auth method: password

- 按 Save 存檔，回到 My Scan 畫面，按下 Metasploitable - Auth 右邊的三角形即可啟動掃描：

<input type="checkbox"/>	Name	Schedule	Last Modified ▼	
<input type="checkbox"/>	Metasploitable - Auth	On Demand	✓ Today at 12:01 PM	

- 我們可以看到經過身份驗證的掃描是成功的，因為掃描程式可以找到更多受攻擊的非遠端公開的應用程式

Metasploitable - Auth

[Back to My Scans](#)

Configure

Audit Trail

Launch ▼

Report

Export ▼

Hosts 1

Vulnerabilities 50

Remediations 69

VPR Top Threats

History 1

Filter ▼

Search Hosts



1 Host



Host

Vulnerabilities ▼



10.0.2.7

30

93

122

12

150



Scan Details

Policy: Credentialed Patch Audit

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 11:55 AM

End: Today at 12:01 PM

Elapsed: 5 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Exercise 8-2

1. 按照上述步驟建立您自己的 Debian 客戶端 Authenticated Scan。
2. 查看掃描結果。

Nmap 弱點掃描

- 雖然 NSE 不是一個成熟的弱點掃描程式，但它確實有一個可用於檢測和驗證弱點的腳本引擎(Nmap Script Engine, NSE)
- NSE 腳本是用 Lua寫的，功能範圍從暴力破解和身份驗證到檢測和利用弱點。
- 我們將著重在“vuln”和“exploit”類別中的腳本，因為前者檢測到弱點，而後者嘗試利用它。
- 但是，這些類別之間存在重疊，並且某些“vuln”腳本可能本質上運行的是精簡弱點
- 因此，腳本也被進一步分類為“safe”或“intrusive”
- 執行後者時要格外小心，因為他們可能會導致遠端服務當機或關閉目標

NSE與script.db

- 在 Kali 上，NSE 腳本位於 `/usr/share/nmap/scripts/` 目錄
- *.nse檔可用任何文字編輯器閱覽
- 花點時間看一些 NSE 腳本，以熟悉這些腳本執行的格式和檢查類型。
- 此目錄中還有一個script.db檔，作為所有腳本的索引，並對每個 Nmap 腳本進行分類
- 例如，我們可以用grep來查找“vuln”和“exploit”類別的腳本：

```
(kali㉿kali)-[/usr/share/nmap/scripts]
$ cat script.db | grep '"vuln"|"exploit"'
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "broadcast-avahi-dos.nse", categories = { "broadcast", "dos", "intrusive", "v
Entry { filename = "clamav-exec.nse", categories = { "exploit", "vuln", } }
```

檢測“vuln”弱點

- 使用 `--script vuln` 針對目標運行 “vuln” 類別中的所有腳本來檢測弱點：

```
$ sudo nmap --script vuln 10.0.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-27 18:21 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
ftp-vsftpd-backdoor:
VULNERABLE:
vsFTPD version 2.3.4 backdoor
State: VULNERABLE (Exploitable)
IDs:  BID:48539  CVE:CVE-2011-2523
vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
Disclosure date: 2011-07-03
```

使用Nmap弱掃應注意事項

- 我們看到 `tp-vsftpd-backdoor.nse` 腳本成功檢測到目標上的 `vsFTPd version 2.3.4 backdoor` 弱點(CVE-2011-2523)，找到有興趣的弱點後，可進一步研究。
- Nmap 並不是傳統意義上的弱點掃描器，但是它對於類似的任務非常有用
- 使用 Nmap 可驗證弱點掃描器的結果，作為專用掃描器的備份，並幫助減少誤報
- 不過Nmap 也需要注意適用於傳統弱點掃描程式的相同警告
- 我們必須了解腳本將檢查和不檢查的內容、腳本將產生的流量以及每個腳本可能帶來的潛在危險^{P.55}

Exercise 8-3

1. 找到偵察SSL弱點的 NSE 腳本，並對 metasploitable機器執行該腳本。

Summary

- 弱點掃描工具可以提供大量資訊，並揭露一些嚴重且不可預見的弱點
- 這些弱點可能會在滲透測試過程中產生重大影響
- 話雖如此，重要的是我們要了解仍然需要手動審查，並且掃描程式只能發現已經用程式寫好的弱點
- 最後，我們應該始終牢記，弱點掃描工具可以執行可能對某些網路或目標有害的操作，因此我們在使用它們時必須謹慎

