執行單位:郝力駭資安能力有限公司 滲透測試小組

版本日期:民國105 年1 月25日 版 號: V1.0

Metasploitable Ⅱ

滲透測試報告書

目錄

[1 前言 2](#_Toc453194420)

[2 聲明 2](#_Toc453194421)

[3 摘要 2](#_Toc453194422)

[4 測試說明 3](#_Toc453194423)

[4.1 測試方法論 3](#_Toc453194424)

[4.2 執行範圍 3](#_Toc453194425)

[4.3 執行期間 4](#_Toc453194426)

[4.4 預計使用工具 4](#_Toc453194427)

[4.5專案組織與成員 4](#_Toc453194428)

[4.6 專案工作項目 4](#_Toc453194429)

[5 執行過程說明 5](#_Toc453194430)

[5.1 檢測項目 5](#_Toc453194431)

[5.2 檢測過程及結果 6](#_Toc453194432)

[5.3 風險等級說明 6](#_Toc453194433)

[5.4風險等級說明 6](#_Toc453194434)

[6 發現事項與建議改善說明 7](#_Toc453194435)

[6.1 先天的防護機制發揮保護作用 7](#_Toc453194436)

[6.2 SQL Injection 7](#_Toc453194437)

[7 結論 8](#_Toc453194438)

[8附件：metasploitable II 滲透測試紀錄 8](#_Toc453194439)

# 1 前言

生大利資本無限公司(下稱甲方)為提高系統安全強度，委託郝力駭資安能力有限公司(下稱乙方)協助辦理metasploitable II 滲透測試作業，測試結果將提供甲方做為資訊安全強化參考。

# 聲明

本小組己盡最大努力挖掘漏洞，囿於小組的滲透測試技巧成熟度與涉獵的技術範疇，無法保證已窮舉測試各種漏洞。

本次滲透測試所發現的結果，並不保證系統已無其他漏洞存在，本報告書提供的補強建議為業界建議的修補方式，惟無法保證日後不會被發現存在其他弱點的。

# 摘要

本報告係為metasploitable II (下稱本系統)滲透測試報告書，執行結果發現之事項總結如下:

|  |  |
| --- | --- |
| 高風險事項 | 8項 |
| * A1 Injection * A2 Broken Authentication and Session Management * A3 Cross Site Scripting * A4 Insecure Direct Object References * A5 Security Misconfiguratin * A6 Sensitive Data Exposure * A7 Missing Function Level Access Control * A8 Cross-Site Request Forgery (CSRF) | |
| 中風險事項 | 2項 |
| * 低強度的機敏資料加密方式 * 不安全的驗證機制 | |
| 建議事項 | 1項 |
| * 不當的資訊揭露 | |

本次測試主要利用OWASP ZAP 及WebScarab 兩項工具(當然也使用其他掃描工具，但未獲得可利用的資訊)。

由於本系統揭露於外的網頁只有登錄頁面，在未取得帳號之前並無法做進一步的檢測，故基於下列二種假設，而進行：低權限使用者可能提權的測試方法進行。

**假設1：**透過社交工程手段取得一般使用者的帳號及密碼。

**假設2**：內部人員可能從事駭客行為。

基於上述假設，經甄友虔協助，開立一組info 帳號供用，本帳號僅具一般

使用者權限。

在以自動化工具(OWASP ZAP) 進行漏洞掃描無法取得有用資訊後，改採人工檢測模式，利用WebScarab 攔截要求/回應的資訊，從中分析可利用的漏洞，並利用SQLMap 對SQL Injection 進行攻擊，進而取得更多可用資訊。

# 4 測試說明

## 4.1 測試方法論

基於OSSTMM3 滲透測試類型，定義資安測試如下：

1. 測試的限制(即對象)一於105 年1 月25 日前完成對本系統之測試，測試範圍僅限系統主機及其直接相關的其他子系統，如網頁伺服器、應用伺服器、資料庫。
2. 作業區域一於甲方提供之4 樓作業區域內，並由甲方提供4 組IP供乙方人員使用(192.168.18.101~192.168.18.104 )。
3. 測試的範圍一有關攻擊前置作業之資料收集不限本系統之設備，唯實際可以攻擊目標僅限本系統之設備。
4. 測試範圖與外界的交互作用方式 -- 可以插入檔案、新增資料及/或讀取資料庫或系統保護的內容，但不得變更、刪除現存的資料，以免影響正常作業。且不得進行阻斷式攻擊。
5. 確認使用的工具(Utility) -- 如附件一所列。(請依實際使用之工具臚列清單，並做成附件一)
6. 界定測試的方式：依4.6.節所列工作項目，檢測系統弱點及漏洞。
7. 遵循事先議定的規則：若有未盡事宜，由雙方約定後做成書面紀錄。

## 4.2 執行範圍

1. 以甲方指定192.168.18.133 為測試標的，測試期間若疑似發現標的以外主機弱點時，應通報甲方，並經甲方同意後，方得做進一步測試。
2. 本次滲透測試探取灰箱測試方法，即就現行己知的系統架構(但不包含程式碼)資訊，以給定有限權限(一般使用者)的帳號進行測試。
3. 給定有限權限帳號合理性:基於「3 、摘要」的假設，駭客不一定是與本系統不相干的人員，亦有可能就是本系統現有的使用者或其周遭的人，因此事先假定一個低權限的帳號亦屬合理的測試方法。
4. 執行可控制的滲透測試行為，以便測試現有的應用系統是否具備適當的防護機制。

## 4.3 執行期間

自民國105 年1 月4 日至民國105 年1 月25 日止為之甲方上班時間內(含午休時間)。

## 4.4 預計使用工具

本專案將以Kali 2.x 之滲透測試整合環境為測試工具，並佐以業界常用之弱點評估工其，如nessus、neXpose，若使用其他工具應事先知會甲方，並獲得甲方同意後方得使用，有關工具清單如附件一。

## 4.5專案組織與成員

甲方之專案協調人員：倚定營。

乙方成員：

專案經理：畢成

測試技術員：高守、吳露棟

## 4.6 專案工作項目

本滲透測試專案應至少包含下列測試項目：

|  |  |
| --- | --- |
| 測試對象 | 測試類型 |
| 主機作業系統及服務平臺 | 作業系統提供之服務 |
| 資料庫平臺 |
| 網頁伺服器平臺 |
| 其他應用服務平臺 |
| 網頁應用程式 | OWASP TOP 10 2013 所列項目 |
| 密碼管理強度 | 包括線上暴力破解及離線雜湊破解 |
| 常見弱密碼檢測 |

# 5 執行過程說明

## 5.1 檢測項目

1. 網路探勘(Network Surveying) ：

模擬惡意攻擊者，進行網路探勘，蒐集目標主機資訊與網路資訊，包含主機位址、主機名稱、網域名稱、網址登記者及網路提供廠商等資訊。

1. 鑑別系統服務( System Services Identification)：

利用網路掃瞄工具(NMAP)找出目標所執行之程式或提供之服務，包含所開敵的網路端口、允許使用的網路協定、作業系統、應用服務程式及修補版號等資訊。

1. 檢測資訊洩漏(Information Leak Digging)：

包含主機回應之錯誤訊息、探索競爭情報(Competitive IntelligenceScouting) 及搜尋引擎所Cache 之資訊，確認是否具有任何資訊洩漏的問題。

嘗試人工輸入異常的資料，並收集相關異常回應資訊。

1. 弱點研究與驗證(Vulnerability Research and Verification)：

尋找具有安全漏洞的系統或應用程式執行入侵，包含利用SQL Injection、XSS、CSRF等各種方式。

嘗試以XSS或SQL Injection或HTML　Tag Injection進行攻擊，並收集攻擊成功之證據及使用方法或腳本。

1. 檢測網路應用( Internet Application Testing)：

檢測系統之網路元件與傳輸模式是否可直接或間接造成前述問題。於成功入侵之主機上繼續使用網路掃瞄工具，網路端口傳送程式及各種可供入侵用之攻擊程式等方式，尋找其他可滲透的網段主機以擴展戰果。

1. 檢測存取權限(Access Control Testing)：

測試是否可以避過驗證機制存取未授權的資料，並透過現有權限提升取得進一步資訊。本項測試包含信任關係測試(Trusted Systems Testing)，利用已佔領之系統或偽冒資訊，測試是否可進入具有存取限制的系統。

1. 權限提升與跳脫(Privilege Escalation and Abuse)：
2. 包含內容評估( Containment Measures Testing)、密碼破解(Password Cracking) 與特權程式測試(Privileged Service Testing) ，如於成功佔領主機上進行資料分析，尋找可茲利用的敏感資訊或機密資或破解高階使用者密碼，以進一步擴展戰果。對於需要長時間嘗試或對入侵極有用途的帳號密碼資訊，則選擇用窮舉猜測法工具嘗試破解。
3. 存活度解析( Survivability Review )：

檢視目標帳號、系統、應用程式是否可被惡意停用或關閉。

## 5.2 檢測過程及結果

1. 網路探勘(Network Surveying)：

本主機是登錄在甲方自有的DNS 伺服器，從外部Whois 收集到的資訊並無法進行相關識別。

1. 鑑別系統服務( System Services Identification)：

利用NMAP 得知系統開放端口，如工作紀錄所示，系統開放過多端口，已嚴重影響系統安全。

1. 檢測資訊洩露( Information Leak Digging)：

嘗試人工輸入異常的資料，在某些情形下，系統會回應詳細的錯誤訊息，造成機敏資料暴露。

1. 弱點研究與驗證( Vulnerability Research and Verification)：

經以測試帳號登入後，實際操作系統，發掘系統漏洞如「3 、摘要」所列，詳細步驟見「8 、附件： metasploitable II 滲透測試紀錄」。

1. 檢測網路應用( Internet Application Testing)：

同第(4)點所述。

1. 檢測存取權限(Access Control Testing)：

同第(4)點所述。

1. 權限提升與跳脫(Privilege Escalation and Abuse)：

利用SQL Injection、CSRF、Missing Function Level Access Control跳脫權限管制，成功取得管理員權限。

1. 存活度解析( Survivability Review )：

提權後，可以自行新增其他帳號及分配權限，以建立多重分身。

## 5.3 風險等級說明

請參閱附件: metasploitable II 滲透測試紀錄

## 5.4風險等級說明

* 測試完成後，滲透測試人員針對所有測試目標評定其風險等級，以該測試目標所造成的衝擊程度及發生的可能性做為因子，相乘得出風險等級；評定標準如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **衝擊程度** | **輕微** | **嚴重** | **非常嚴重** |
| **可能性** | 該弱點被利用之可能性高 | 中風險 | 高風險 | 高風險 |
| 該弱點被利用之可能性中 | 低風險 | 中風險 | 高風險 |
| 該弱點不易被利用 | 低風險 | 低風險 | 中風險 |

# 6 發現事項與建議改善說明

## 6.1 先天的防護機制發揮保護作用

雖然本系統有許多漏洞，但因系統硬體架構上的防護:

* 1. 本機限制可存取IP 。
  2. 防火牆已關閉不必要的服務端口。

故一般駭客不易攻擊成功。

## 6.2 SQL Injection

1. 弱點1：
   1. 測試目標： <http://192.168.18.133/dvwa/vu1nerabi1ities/sq1i/>
   2. 發現事項：

本網頁的「User ID」欄存在SQL Injection弱點，利用此弱點可以取得資料庫內相關資訊及使用者帳號、密碼。

* 1. 詳如附件之步驟三弱點一。

1. 弱點2：
2. 測試目標：<http://192.168.18.133/dvwa/vu1nerabi1ities/sq1i_b1ind/>
3. 發現事項：

本網頁的「User ID」欄存在SQL Injection 弱點，利用此弱點可以取得資料庫內相關資訊及使用者帳號、密碼。

1. 詳如附件之步驟三弱點二。
2. 弱點3：
3. 測試目標：http://192.168.18.133/mutil1idae/index.php?page=register.php/
4. 發現事項：
5. 本網頁的「Username」欄存在SQL Injection弱點，利用此弱點可以取得資料庫內相關資訊及使用者帳號、密碼。
6. 詳如附件之步驟三弱點三。
7. 建議解決方案

修正程式的查詢語法，建議採用Prepared Command之查詢方式。

1. OWASP Reference：OWASP 2013 A1
2. 風險等級：高

(這裡只列出兩項代表，實際上應按滲透測試結果逐項列出。)

# 7 結論

本次滲透測試結果主要得到以下結論:

1. 本系統測試發現高風險15 項、中風險31 項、低風險6 項及建議資訊84 項，詳如附件8 之滲透測試紀錄。在駭客取得一般權限之帳號後，可能對系統進行各式攻擊。
2. 建議系統程式應予改寫，並將前端的檢核機制於後端程式實做，以達到實質檢核的效果。

# 8附件：metasploitable II 滲透測試紀錄

執行單位：郝力駭資安能力有限公司 滲透測試小組

版本日期：民國105 年1 月25日 版 號: V1.0

Metasploitable Ⅱ

滲透測試紀錄

|  |  |  |  |
| --- | --- | --- | --- |
| 測試人員 | 高守 (請親簽以示負責) | 執行日期 | 2016/01/05 |
| 檢測標的 | (填入目標的IP或Hostname或URL) | | |
| 使用工具 | Nslookup, Google Hacking (請依實際使用的工具填寫) | | |
| 測試端IP | (填入執行測試的工作站之IP) | | |
| 檢測項目： | | | |
| (這裡填寫今日檢測的項目) | | | |
| 輸出畫面或訊息 | | | |
| (這裡放入載圖及執行步驟或指令，如果截圖或說明太多，也可以利用附件方式呈現，這一段通常會有最多資料) | | | |
| 發現事項說明 | | | |
| (執行過程中所取得有用資訊或現象的摘要紀錄。) | | | |
| 專案經理 | 畢成 (請親簽以示負責) | 復閱時間 | 2016/01/05 18：43 |
| 審核人員 | 倚定營 (請親簽以示負責) | 審閱時間 | 2016/01/06 10：21 |