臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

目錄

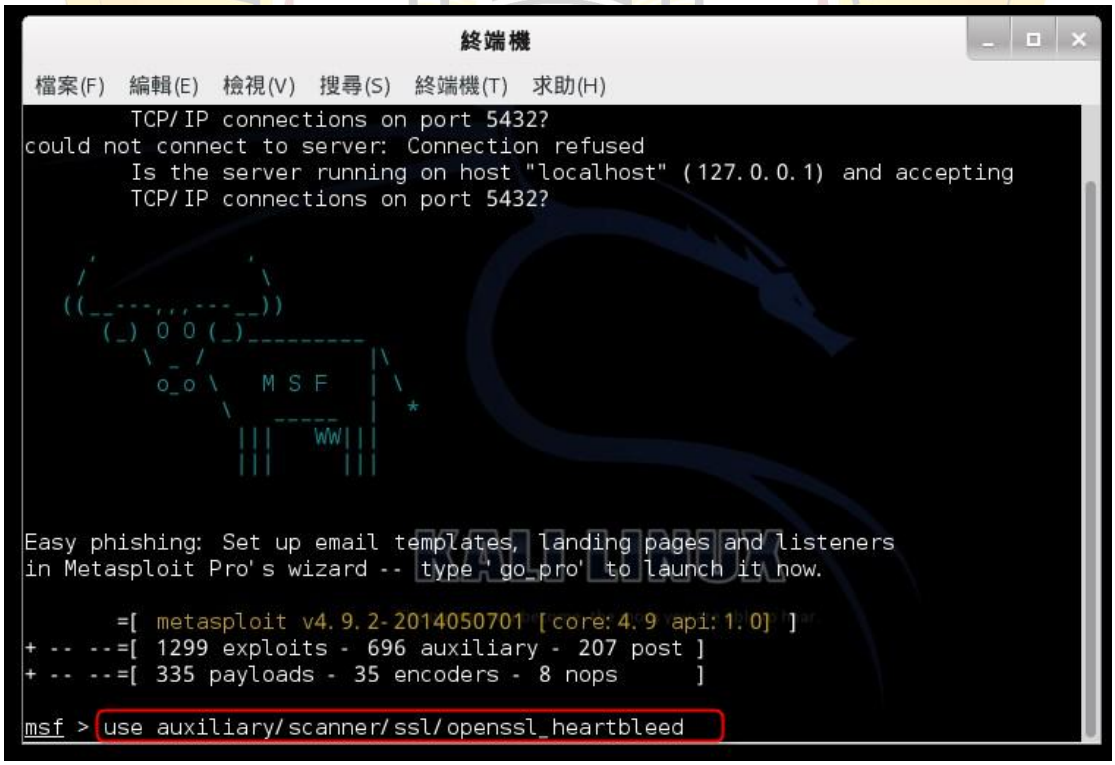
OPENSSL(CVE-2014-0160)漏洞分析與防禦方法簡介

本技術報告簡介

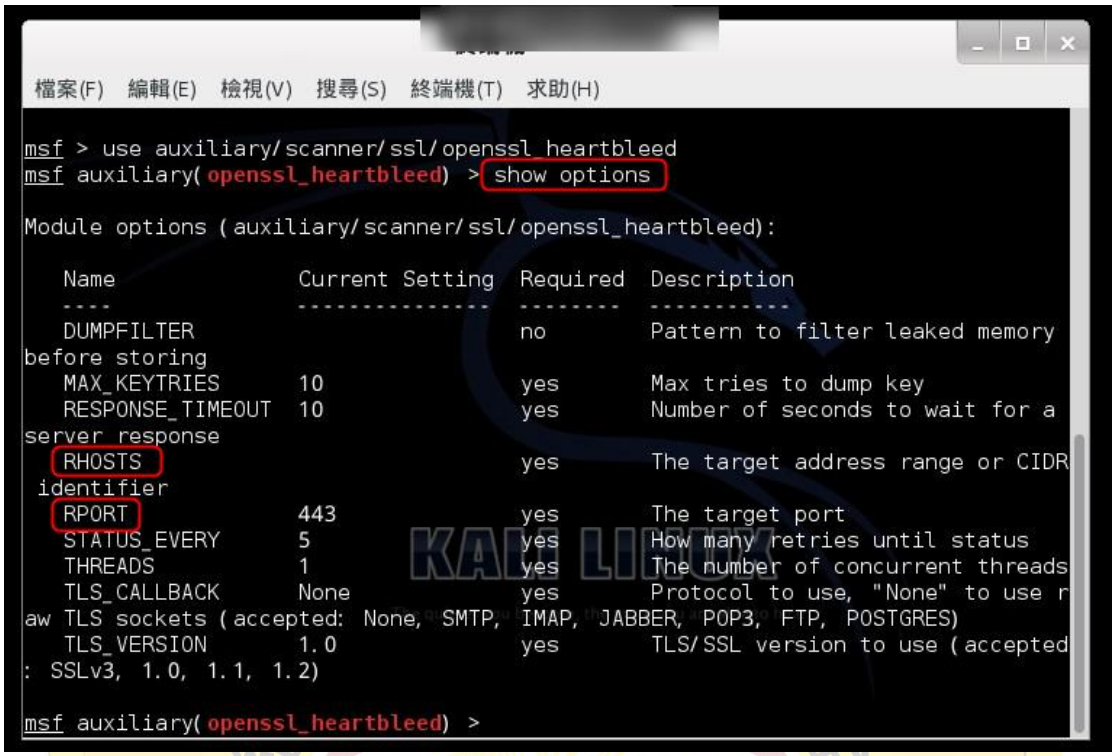
OPENSSL 漏洞(CVE-2014-0160)讓有心人士可透過 OpenSSL 技術竊取系統記憶體資料，取得使用者帳號與密碼等機敏資訊。本文將透過實作漏洞檢測、擷取系統資料、提供修補漏洞建議措施與結論等說明此漏洞，期望讀者能透過本分析報告確認管理及使用範圍內是否存在此漏洞，以進行漏洞的修補與防護。

使用 Metasploit 實做 OPENSSL 漏洞檢測

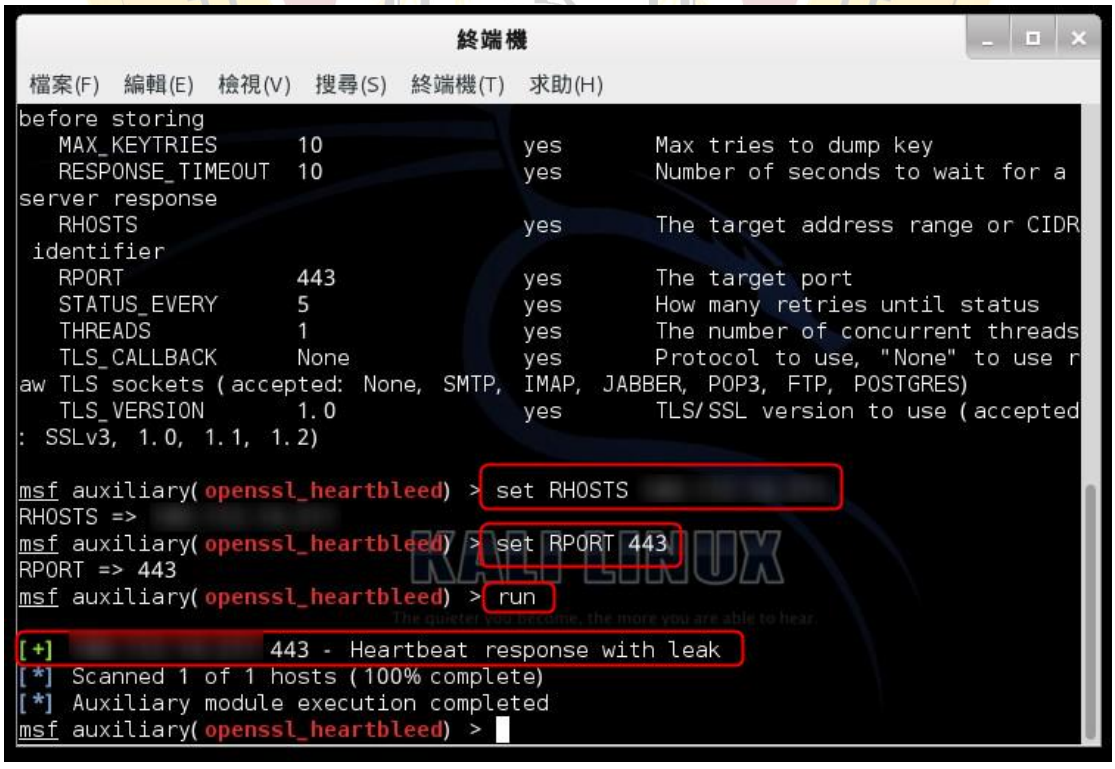
1.) 開啟 Metasploit msf 介面，並鍵入指令
"**use** auxiliary/scanner/ssl/openssl_heartbleed"



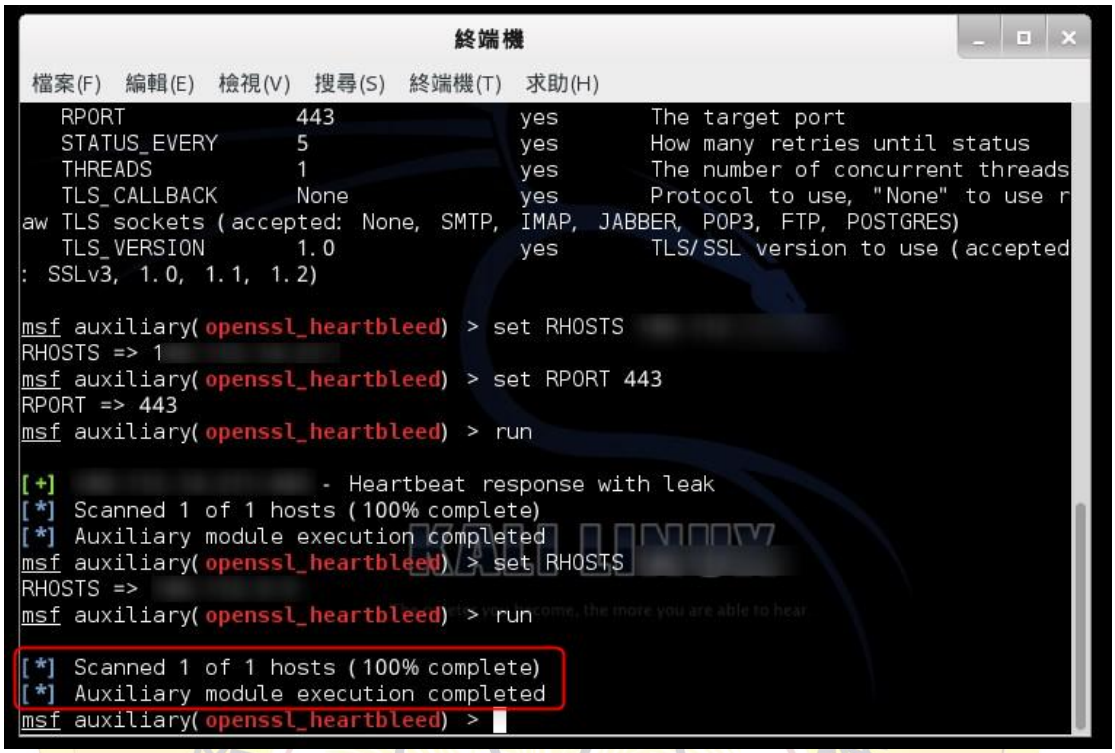
2.) 接著使用"show options"檢視有何參數須調整，此例中僅需設定"RHOSTS"(*目標 IP 位置*)以及"RPORT"(*目標 PORT*)



3.) 使用 set RHOSTS 及 set RPORT 等指令設定參數，設定完成後，鍵入"run"執行掃描，當顯示"**Heartbeat response with leak**"表示目標 IP 存有此弱點。



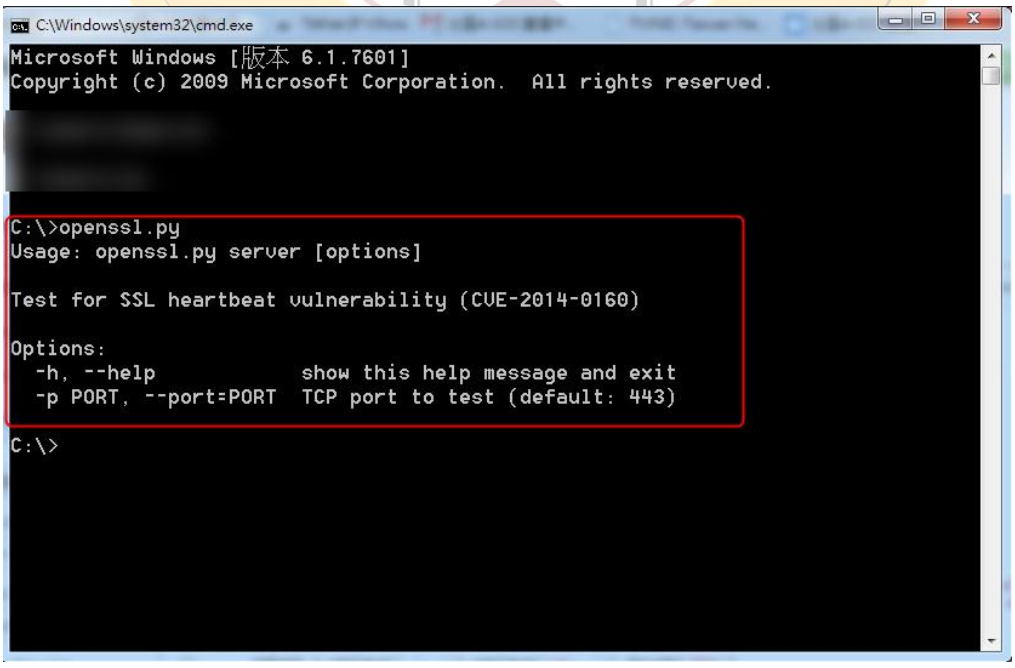
4.) 若目標 IP 無此此弱點，則會顯示如下圖資訊。



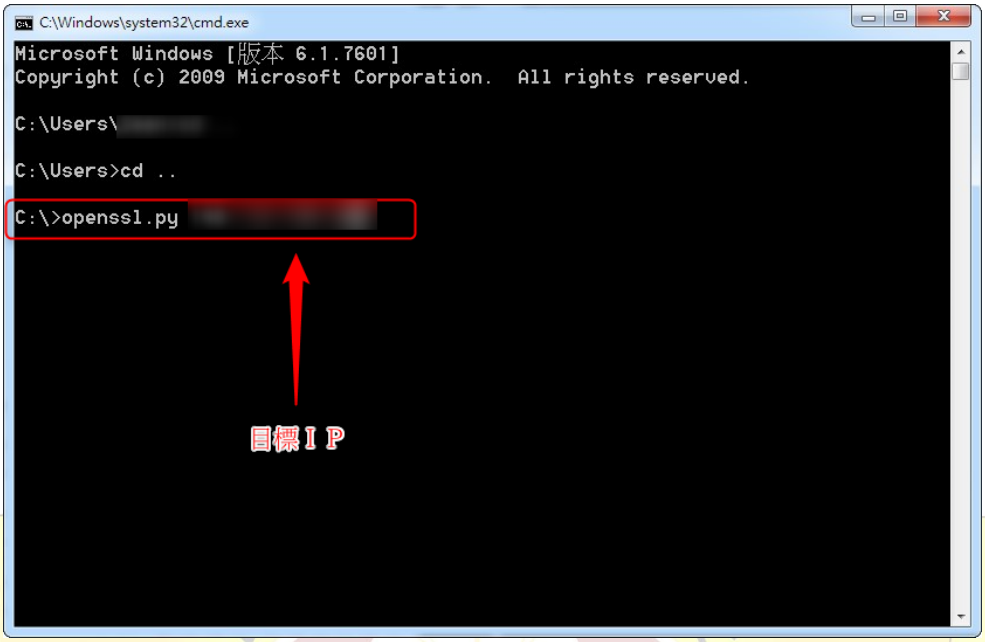
使用 Openssl.py 擷取 OPENSSL 漏洞資料

Openssl.py 為 Jared Stafford 利用 Python 所撰寫的檢測工具，為公開的原始碼，可至 *https://gist.github.com/sh1n0b1/10100394* 下載及使用。

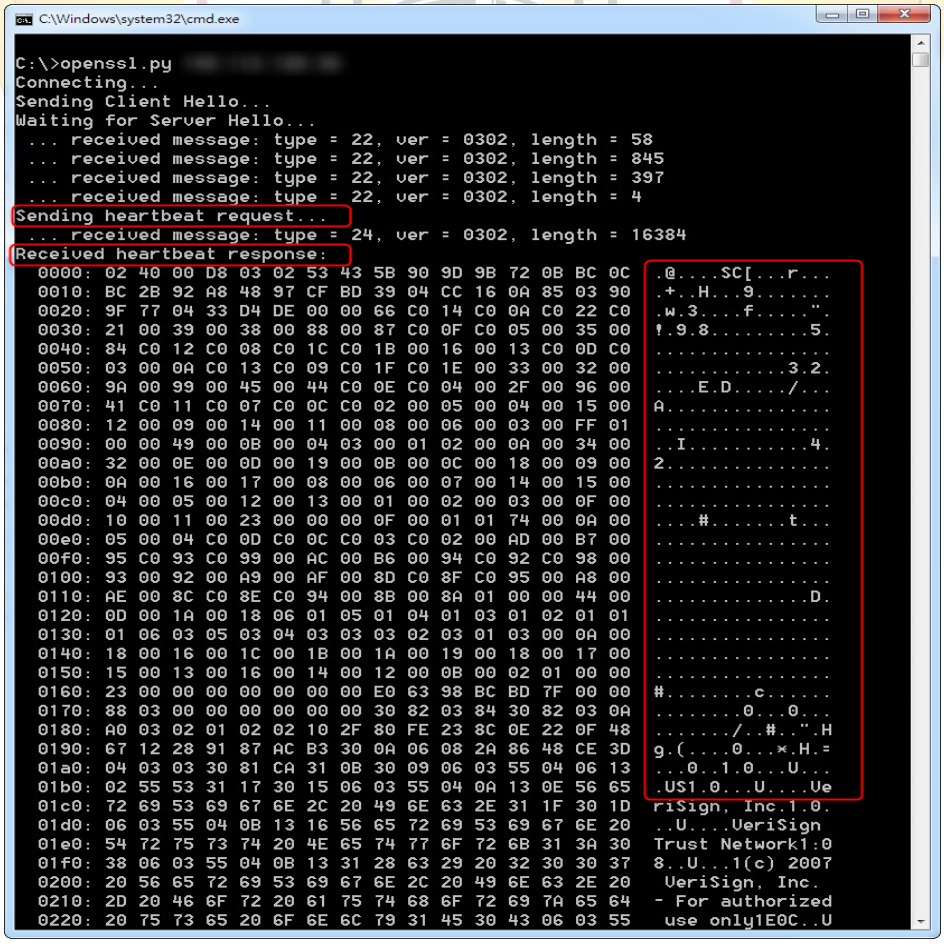
1.) 開啟檢測工具



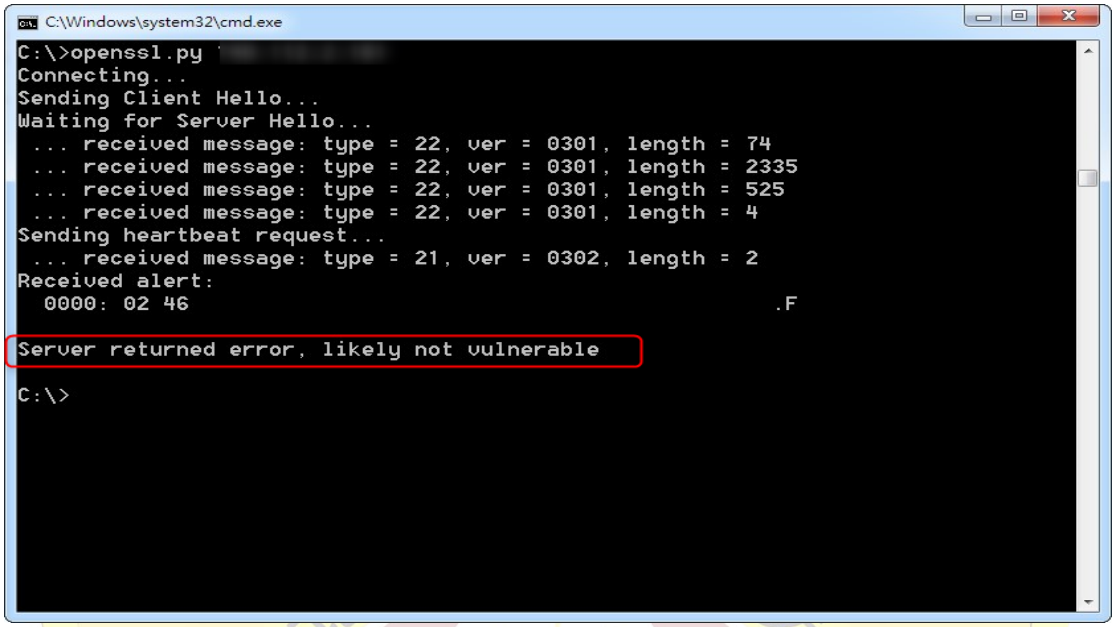
2.) 填入檢測時所需之參數(目標 IP 及 port，預設為 443)



3.) 目標 IP 存有此弱點，將可收到其記憶體中 64KB 的資料



4.) 若目標 IP 不存在此弱點，則會顯示如下圖資訊



修補 OPENSSL 漏洞

針對 OPENSSL 漏洞(CVE-2014-0160)，使用上述檢測工具可確認伺服器是否存在此漏洞。由於部份機敏資料可能已外洩，加上此弱點存取資料來源為記憶體，難以察覺是否已被外部使用者取得，故我們建議可參考下列幾點建議措施進行後續修補動作，避免重要機敏資料持續外洩。

1.) 立即更新 OpenSSL 套件至最新版本(1.0.1g or 1.0.2-beta2 以上之版本)
2.) 清除目前 Server 所有的 Session
3.) 重啟 OpenSSL 的服務
4.) 重新產生伺服器 SSL 私鑰
5.) 更新本機管理者帳號密碼
6.) 將原使用之憑證撤銷，並使用新產生之憑證

結論與建議

OPENSSL(CVE-2014-0160)漏洞影響範圍極廣，應盡速完成漏洞修補與損害管制，針對一般使用者與系統管理人員的建議如下；

一般使用者，若有使用 HTTPs 服務者，建議立刻進行密碼變更並留意自己的帳號是否有異常活動。

若您為系統管理人員，請確認系統之 OpenSSL 版本是否在受害範圍，若有，請進行修補，並使用 ssltest.py 檢測工具檢測確認洞已修補完成。若您暫時無法進行漏洞修補，可使用免費之 Snort IDS 進行攻擊偵測，Rule 編號分別為 sid: 30510 - 30517, 30520 - 30525, 30549, 30777 - 30788。

參考資料

1. http://www.icst.org.tw/Heartbleed.aspx?lang=zh://news.cnet.com/8301-1009_3-57591042-83/mobile-malware-grows-by-614-percent-in-last-year/
2. http://www.snort.org/snort-rules/#community
3. *https://gist.github.com/sh1n0b1/10100394*