



## 在 Black Hat® 大會中，沒有一個駭客能夠破解 Symantec™ Critical System Protection

2011 年 8 月 12 日

賽門鐵克威力強大的虛擬和實體伺服器安全解決方案 — Symantec™ Critical System Protection 近日在 Black Hat® 技術安全大會中通過考驗。來自全球各個知名團體的老練駭客試圖破解一台受到 Symantec Critical System Protection 保護、但卻未安裝修補程式的脆弱伺服器，不過他們全都功敗垂成，無法擷取到隱藏在該伺服器當中的「旗標」。

Critical System Protection 技術團隊在 Black Hat 大會中安排了一項測試，讓所有人都來試試手氣，想辦法叫出隱藏在一台未安裝修補程式的伺服器當中的「旗標」。目的就在於讓安全專業人員和駭客找出產品中存在的落差，協助我們改善產品。我們在一台未安裝修補程式的 Windows XP 伺服器上，利用 Critical System Protection 強大的預防政策來保障該旗標。該伺服器擁有 Rapid 7 所提報的 10 個已知漏洞，十分容易受到駭客攻擊，同時還有能讓外部存取的開放性網路共享。

一位攻擊開發人員/安全漏洞網路掃描工具決定試試看，將他的工具組當中能夠找得到的所有攻擊全都丟向該系統。在攻擊該系統之前，他先掃描系統以找出哪些程式在監聽，然後才設計他的攻擊行動。他試了包含緩衝區溢位 (Buffer Overflow) 和執行緒注入 (Thread Injection) 等攻擊，想破壞好幾項服務，包括 SMB、NetBIOS 和 RPC。他也試圖開啟 remote shell，不過並沒有成功。此外，他也嘗試讓服務執行指令，不過全都被 Critical System Protection 攔截下來。他使用了幾種不同的密碼猜測攻擊工具，試圖入侵系統，不過，在猜測密碼方面也是全軍覆沒。該系統的防護十分強大，最後他還是無法入侵。

同一時間至少都有 10 組不同的 IP 在攻擊這台電腦，其中某些 IP 位址源自其他的國家，因此也包括屬於不同駭客集團的人，他們一直在嘗試以社交工程技巧取得該系統的資料。這些被 Critical System Protection 偵測到的攻擊想要對系統上的漏洞發動攻擊，並且取得 remote shell 或執行指令。

其中有一個很有趣的狀況，有一位駭客老手要求做一項愚蠢的使用者攻擊，他希望賽門鐵克技術團隊開啟瀏覽器，然後指出該機器上隱藏旗標的網頁位址。他試著在該系統上執行瀏覽器攻擊，以便安裝後門程式，不過，安裝後門程式的作業也被 Critical System Protection 攔截了。接著他又要求直接存取，不過賽門鐵克團隊解釋，在真實的世界中是不可能發生這種狀況的。於是他建立了一個可執行檔，希望賽門鐵克在該系統上啟動它，不過，Critical System Protection 也阻止了該檔案的執行。他製作了一個內嵌 Netcat (一種後門程式) 的文件，然後要求賽門鐵克人員在指令列開啟該檔案。他給了賽門鐵克團隊希望要開啟的指令列，然後 Netcat 就啟動了。最後他得以進入自己的系統，並且建立一個 remote shell。唯有 Critical System Protection 的防火牆元件允許所有系統之間的流量通過時，才有可能做到這一點。他以為他成功了，不過他還是沒辦法擷取到旗標。在 Black Hat 大會結束之前，大約共有 20 個人嘗試過，但都無法擷取到旗標，因此沒有人贏得大獎。

因此，Critical System Protection 在 Black Hat 大會中證明了它是一套保障虛擬與實體伺服器的強大解決方案。它的安全政策能保護未安裝修補程式和老舊的系統，避免外部威脅，例如零時差攻擊、先進的頑強攻擊以及惡意內部人員所造成的漏洞。

欲知更多有關 Symantec™ Critical System Protection 的資訊，  
歡迎造訪我們的網站：<http://www.symantec.com/business/critical-system-protection>  
或撥打免付費電話：1 (800) 745 6054 與我們的產品專員聊聊。