

誘捕系統（HONEYPOT）的保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 什麼是誘捕系統?	3
誘捕系統的分類	3
II. 誘捕系統的部署策略	6
III. 誘捕系統的例子	7
IV. 總結	9

摘要

誘捕系統（Honeypot）是用來引誘攻擊者入侵機構資訊系統的陷阱。誘捕系統若部署得宜，便能夠作為預警及先進的保安監察工具，減低資訊科技系統及網絡遭攻擊的風險。當攻擊者試圖入侵資訊系統時，誘捕系統能對入侵方法加以分析，為系統的潛在漏洞提供寶貴資訊。

本文將對誘捕系統作出簡單介紹，以及如何部署誘捕系統以加強機構及企業的重要系統及網絡保安。

I. 什麼是誘捕系統？

根據誘捕系統計劃創始人 Lance Spitzner，誘捕系統的目的，是為了得悉攻擊者如何刺探及利用資訊科技系統的弱點¹。誘捕系統亦可以被定義為：「*an information system resource whose value lies in unauthorised or illicit use of that resource*」²，換句話說，誘捕系統便是佈置在網絡上引誘攻擊者的誘餌。誘捕系統是典型的虛擬電腦系統，偽裝執行完整服務及應用程式，並一如網絡上典型系統或伺服器開啟連接埠，模擬真實電腦系統。

誘捕系統之所以起作用，是因為它令攻擊者誤以為它是真實的系統。他們攻擊系統時並不知道正被秘密觀察。當攻擊者嘗試攻擊誘捕系統時，誘捕系統便會收集施襲的相關資訊，例如攻擊者的互聯網規約位址（IP address）。攻擊者的活動對攻擊技術提供了寶貴資料及分析，讓系統管理員可以在需要時追尋攻擊來源。

誘捕系統可以作生產或研究的用途。生產誘捕系統（production honeypot）是用來減低保安風險的，因大部份生產誘捕系統模擬特定的操作系統或服務，誘使攻擊者利用自動化工具隨意尋找含有保安漏洞的系統加以攻擊，故生產誘捕系統能夠保護網絡或系統免受這類攻擊。設置生產誘捕系統可以減慢攻擊工具的掃描過程，浪費攻擊者時間。一些生產誘捕系統更可以令攻擊完全停止，例如向攻擊者傳送 window size 網路參數為零的確認小包，這會令攻擊維持在「等待」狀態，而它只能當網路參數增加時才可以傳送數據³，因此，生產誘捕系統經常被視為偵察及威懾的工具。

用作研究的誘捕系統是真實的操作系統及服務，風險因此亦較高。這種誘捕系統對新的攻擊技術及手法提供詳盡資料，各類攻擊的狀況亦因而較準確。誘捕系統的記錄檔案及其它在攻擊過程中收集到的資料，促使對攻擊的防範、偵測以及應變措施得以改良。一般來說，大學及軍事部門會設置用作研究的誘捕系統來收集新攻擊手法的資料，其中部份研究成果更會公開，惠及整個社群。

誘捕系統的分類

誘捕系統可分為低互動及高互動兩大類。低互動誘捕系統（low-interaction honeypots）通常用作生產；高互動誘捕系統（high interaction honeypots）則往往用於研究。

低互動誘捕系統

¹ <http://rootprompt.org/article.php3?article=210>

² <http://www.spitzner.net/honeypots.html>

³ <http://safari.oreilly.com/0321321286/ch09lev1sec12>

低互動誘捕系統的互動程度是有限的，它在操作時一般會模擬有限度的服務和操作系統。因為模擬操作和服務的有限，攻擊者的活動也相對地受到限制。舉例來說，在模擬連接埠監聽檔案傳送規約（FTP）的服務時，可能只須簡單地模擬 FTP 登入或支援一些額外的 FTP 指令即可。

低互動誘捕系統的好處是較為簡單，因而易於設立和維修。再者，由於所模擬的操作有限，誘捕系統被利用的潛在風險亦較低。但低互動誘捕系統只能收集有限的資料，而且富有經驗的攻擊者遇上此誘捕系統時很容易便能辨認出來。

例子：偽裝系統（Façades）

偽裝系統是透過模擬服務或應用程式，以提供目標主機虛假表象的系統，當偽裝系統被攻擊時，系統會收集攻擊者的資訊。有些偽裝系統只會提供部份應用程式層面的行為（例如 banner presentation），有些則會模擬出特定服務甚至網絡堆疊行為（network stack behaviour）。偽裝系統的價值主要視乎系統能夠模擬的服務和應用程式，以及設立和管理的容易程度而定。

偽裝系統的部署簡單容易，只需簡單的安裝及工具便能模擬各種系統。偽裝系統並非真實的系統，亦沒有真實的保安漏洞，所以攻擊者不能用作跳板來攻擊系統之用。然而，因為這些系統只能提供潛在威脅的基本資訊，所以通常只為中小型企業使用，大企業往往要配合其它保安技術使用。

高互動誘捕系統

高互動誘捕系統因涉及真實的操作系統及應用程式，例如設置真實的 FTP 伺服器用以收集針對特定 FTP 伺服器或服務的攻擊資料，所以系統較為複雜。

提供真實系統讓攻擊者攻擊，對攻擊行為不加規範，這能讓管理員收集有關攻擊方法的詳盡及完整資料。不過，攻擊者卻有可能利用高互動誘捕系統作跳板來襲擊機構內其它系統，因此足夠的保護措施是必須的。在最壞情況下，可能要截斷誘捕系統的網絡連接，以阻止攻擊者進一步入侵網絡及其它電腦。

示例一：待宰羔羊（Sacrificial Lambs）

待宰羔羊是刻意方便攻擊者攻擊的現成系統。管理員須定期檢查系統，以判斷系統是否已被破解，如果已破解，則需判斷系統遭受到哪些攻擊。至於傳送至誘捕系統的指令及其它額外數據，則可以為部署在誘捕系統附近的網絡監聽裝置（network sniffer）收集。然而，由於這些誘捕系統是在運作中（live），所以可成為攻擊者的跳板作進一步攻擊。

因此部署時要額外考慮如何隔離及控制誘捕系統，例如設置防火牆或其它網路控制裝置，又或將誘捕系統從內部網絡截斷。

因為待宰羔羊是真實的系統，所有產生的結果都跟真實無差別。但待宰羔羊需要較多管理的工作負擔，例如管理員須親自安裝操作系統，人手進行應用程式配置或系統安全強化及分析工作，並有可能需要額外工具。如上所述，部署這類誘捕系統需要額外考量，亦需要由專門從事有關保安工作的專業人員提供管理和支援，對誘捕系統收集的數據加以分析。

示例二：傀儡系統（Instrumented Systems）

傀儡系統是現成的系統，對預載操作系統及核心層級作出改良，因而能夠提供更多的資料，也能夠實施更嚴密的封鎖或監控。跟待宰羔羊不同，該操作系統及核心已經保安專業人員修改。當操作系統及核心被修改過後，系統會像真實目標一樣在網絡運作。傀儡系統結合了待宰羔羊及偽裝系統的優點。跟待宰羔羊一樣，傀儡系統會提供真實系統的完整複本，供攻擊者入侵；與此同時，又像偽裝系統般容易接達但難以入侵。此外，對操作系統及核心的修改也足以阻止攻擊者用作攻擊網絡其它部份的踏腳石。

示例三：誘捕濫發電郵系統（Spam Honeypots）

誘捕系統技術可以用來研究濫發電郵及收集他人電郵地址的行為。部署誘捕系統可以研究電郵濫發者如何偵測公開郵件傳遞。電腦可以模擬電郵伺服器、代理伺服器及網絡伺服器的運作，接收濫發電郵並加以分析，以確定收到濫發電郵的原因⁴。此外亦可以設置電郵捕捉器（email trap），開設一個用來專門接收濫發電郵的電郵地址。

⁴ <http://www.honeyd.org/spam.php>

II. 誘捕系統的部署策略

為了使誘捕系統發揮最大的效用，同時將誘捕系統帶來的風險減到最低，必須精心規劃及部署誘捕系統。以下是關於一些常見的誘捕系統部署策略：

1. 把誘捕系統與生產伺服器並排地一起安裝，並需要映照生產伺服器的一些真實資料及服務，藉此吸引攻擊者。為了增加系統遭入侵的機會，誘捕系統的保安可以稍為鬆懈，以收集攻擊的有關資料。然而，如果攻擊者成功入侵網絡內的誘捕系統，遭入侵的誘捕系統可以用來掃描網絡內其它潛在目標。這亦是在生產系統內安裝誘捕系統的主要缺點。使用其它部署方法（包括下文所介紹的）並不會出現這情況，因為整個誘捕系統本身便是虛構出來的網絡。
2. 為每個伺服器配對一個誘捕系統，任何指向伺服器的可疑通訊都會被導向到誘捕系統。指向傳輸控制規約（TCP）埠 80 的通訊如常轉到伺服器的互聯網規約位址（IP address），但所有其它指向互聯網伺服器的通訊則會導向至誘捕系統。與此同時，為了偽裝誘捕系統，伺服器的網頁內容等部份數據可能要複製至誘捕系統。
3. 建立誘捕系統網絡（honeynet）：利用誘捕系統組成的網絡，模擬及複製真實或虛構的網絡。誘捕系統網路在攻擊者看來，就像在幾個不同的平台運行各種應用程式。誘捕系統網路能夠針對攻擊作預警，而透過觀察哪類電腦及服務遭攻擊，以及攻擊者做過什麼，為了解及分析攻擊者的意圖提供了極佳的方法。誘捕系統網路計劃（The Honeynet Project）⁵是研究誘捕系統網路的最佳例子。

⁵ <http://www.honeynet.org/>

III. 誘捕系統的例子

以下是一些誘捕系統免費軟件的例子：

1. **Deception Toolkit**⁶：這是首個以開放源碼建立的誘捕系統，於 1997 年面世。軟件由 Perl 手稿程式及 C 源碼組成，能模擬各種不同的監聽服務，其主要目的在於欺騙人類攻擊者。
2. **LaBrea**⁷：這誘捕系統能起圍困作用，目的在於拖延甚或阻止攻擊，能偵測出蠕蟲及其它惡意程式碼，並加以圍困。該軟件可在視窗及 Unix 操作系統運作。
3. **Honeywall CDROM**⁸：這是一隻存有開放源碼程式集的可啟動光碟，它會自動部署一個名為 **Honeywall** 的誘捕系統網路通訊閘，令誘捕系統網路的部署變得簡單及有效。它能截取、控制及分析誘捕系統網路對外及對內的活動。
4. **Honeyd**⁹：這是一個功能強勁的開放源碼低互動誘捕系統，可在視窗及類似 Unix 的操作系統上運作。這系統能夠監察未使用的互聯網規約 (IP)，及在傳輸控制規約／互聯網規約 (TCP/IP) 的層疊級別 (stack level) 上模擬操作系統；亦可以同時模擬數以千計的虛擬主機，並監察所有基於 UDP 及 TCP 的連接埠。
5. **Honeytrap**¹⁰：這是一個用來觀察針對網絡服務攻擊的低互動誘捕系統，能為管理員收集有關已知及未知的網絡攻擊資訊。
6. **HoneyC**¹¹：這是一種客戶誘捕系統的例子，它會接達伺服器，目的是找出網絡上的惡意伺服器。它使用模擬客戶找出伺服器回應的種類，以分析是否屬惡意網頁內容，藉此辨認出惡意伺服器。
7. **HoneyMole**¹²：這工具是用來部署「誘捕農場」(honeypot farms) 或分佈式誘捕系統的，它會將網絡通訊轉向至誘捕系統的中央，對收集得來的數據加以分析。

適用於企業使用的商用產品的例子如下：

1. **Symantec Decoy Server**：這是誘捕系統式入侵偵測系統 (intrusion detection system, (IDS))，能實時偵察未經准許的接達及系統濫用，並加以遏制及監察¹³。

⁶ <http://www.all.net/dtk/index.html>

⁷ <http://labrea.sourceforge.net/labrea-info.html>

⁸ <http://www.honeynet.org/tools/cdrom/>

⁹ <http://www.honeyd.org/>

¹⁰ <http://honeytrap.mwcollect.org/>

¹¹ <https://www.client-honeynet.org/honeyc.html>

¹² <http://www.honeynet.org.pt/index.php/HoneyMole>

¹³

<http://www.symantec.com/business/support/documentation.jsp?language=english&view=manuals&pid>

2. Specter¹⁴：這是建基於誘捕系統的智能入侵偵測系統。它能夠模擬 14 種操作系統，監察 14 個不同網絡服務及捕捉器，並有多樣配置及通報功能。

=51899

¹⁴ <http://www.specter.com/default50.htm>

IV. 總結

誘捕系統有其優點及不足處。誘捕系統引誘及圍困攻擊者，當有人與之互動時，誘捕系統會收集資訊及發出警報，無疑是很有用的工具。攻擊者的活動為攻擊技術及方法分析提供了可貴的資料。因為誘捕系統只截取及存檔數據及向其發出要求，所以不會為網絡帶寬增加額外負擔。

不過，誘捕系統亦有其不足處。因為誘捕系統只能追蹤及截取那些直接與之互動的活動，卻不能偵測針對網絡內其它系統的攻擊。再者，若部署誘捕系統欠缺計劃及考慮，對現有的網絡可能帶來更多的風險。因為誘捕系統的設計是讓人入侵的，所以總有可能被攻擊者攻佔並用來作踏腳石，通往網絡內其它系統，這可能便是誘捕系統最具爭議性的缺點。