網際網路惡意網站偵測機制之研究

鄭進興　吳永彬
國立高雄第一科技大學資訊管理系
jscheng@ccms.nkfust.edu.tw

摘要

近年來網路快速蓬勃發展，使得惡意網站潛伏的安全陷阱不勝枚舉，促使網路安全事件不斷發生，故能提供使用者偵測或防範的方法來避免遭受攻擊及降低所造成的傷害是相當重要的議題，目前誘捕系統(Honeypots)是屬於安全防護防禦機制之一。傳統的誘捕系統屬於被動式的偵測，往往只能在攻擊事件發生後，才對管理者發出警告以進行應變處理，這樣在時效性已顯不足，本研究以 Client 端誘捕系統的概念，又稱做 Client Honeypot ，來探討有別於傳統的入侵偵測系統被動式偵測模式，讓使用者可以採用主動式偵測方式以保障網路存取的安全。本文採用 Open Source 工具 HoneyC 來進行研究，能主動式的判別網際網路的網頁是否屬於惡意網站，因此能讓使用者在瀏覽網頁時，降低網路可能存在的威脅，確保本身的安全。

關鍵詞:惡意網站、誘捕系統、HoneyC

Abstract

The network grows fast rising and flourishing in recent years, there are too numerous security traps making malicious websites lurk, impel the network security incident to happen constantly. Therefore, it is quite important topic that can offer user detect or method of protect that avoid being attacked and reduce the injury caused. At present, Honypots is belonging to one of security defense against mechanisms. The traditional Honypots belong to the detecting and examining of passive form that can only be after the attack happened, it just sends out the warning to deal with emergency by administrator, make efficiency already show insufficiently. The research is in accordance with Honypots concept in client, also called Client Honeypot, to discuss it different form traditional intrusion detection system passive form to the way of detect that enable users to adopt actively way of detect in order to ensure network access security .This article adopt HonyeC of open source tool carry on research enable active to determine Web sites whether is good or malicious. Therefore, make user reduce the possible threat of the network to ensue one's own security while browsing through the webpage.

Keywords: Malicious websites, Honeypot, HoneyC

1. 前言

網路科技的發展帶來無數便利及拉近了人們之間的距離，然而現在網路已由過去單純簡單，演化到目前龐大複雜，許多問題也因應而生。資訊安全問題由於網路的快速蓬勃發展，延伸至網路安全議題，其中顯而易見的便是各式各樣的系統弱點遭到挖掘，導致電腦駭客、病毒等影響網路安全問題日漸突顯，造成企業與個人資料的外漏，引發財物損失、曝露商業機密及私人隱私。根據近來實例(刑事局，2007)[2]，刑事警察局科技犯罪防制中心發現，兩岸駭客設置俗稱「釣魚網站」的假網頁，誘使民眾登入，伺機植入木馬程式，竊取網路銀行帳號密碼等個人資料，再轉帳盜領存款，已知有五名網路銀行用戶遭轉帳盜領合計近千萬元。由此可知網路攻擊事件一直圍

繞在我們生活週遭不勝枚舉，可以在短短的時間內蔓延整個網路，造成網路使用者的受害，特別是近年來，高危險惡意攻擊事件不斷出現，使世界經濟蒙受了輕則幾十億，重則幾百億美元的巨大損失，使得大家特別重視網路安全的維護。

網路的發展使得 Web 服務所能提供的服務應用變的更多，如 FTP、HTTP 等，但這些服務本身都有設計上的缺失，導致被電腦駭客所利用變成更多不同弱點的型式存在，一但被網路駭客發現，就會利用這些弱點進行攻擊。而一般使用者又缺乏相關知識，更不了解防護方法，所以很容易的掉入陷井裡，蒙受巨大的損失。為了避免攻擊事件發生，除了靠使用者的認知、判斷外，還需額外的工具或防護技巧來避免安全事件的發生。

在網路安全問題已經被大家所重視，網管人員常會使用入侵偵測系統(IDS, Intrusion Detection System)或誘捕系統(Honeypot)來建構網路防護系統，被設計來引誘擷取惡意活動的程序進而產生警告訊息，以提升防護能力。因為隨著網路的安全不確定因素增加，入侵檢測系統的日誌內容也日益龐大，甚至有些系統每天的日誌量就達 1GB。在這個少花錢多辦事的世界裏，企業再也沒有過多的人力用來每天處理如此大量的日誌內容，IDS 本質上是屬於被動式的偵測，往往等到有攻擊事件發生，才有進一步的防護作為，這種的防護措施，時效性似乎不是那麼的高。

上面所描述是偏向 Server 端的防護，因此近幾年有提出新的概念叫做 Client Honeypot，它與傳統的 Server Honeypot 差別在於它是屬於主動式的偵測，被設計從惡意主機當中能主動偵測攻擊行為，然而 Server Honeypot 不能主動偵測。就因如此，Client Honeypot 能主動偵測網路上所提供的 Web 服務是否含有惡意的攻擊行為存在，能大大的降低網路使用者的威脅。

2. 文獻探討

本節先談到 Web 所帶來的威脅，再簡述相關現有的 Client Honeypot 技術偵測機制研究。

2.1. Web 威脅的崛起

現今網路的普及化，各式各樣建構在網路上的應用服務也逐漸的增多，也帶來了無數的便利，人們也利用這些網路服務來提升工作效率，如網路購物、網路報稅等等。這些服務無時無刻都與 Web 習習相關，但伴隨著網路安全問題的出現日益已成為社會大眾所關心的焦點。根據網路安全方案供應商趨勢科技(Trend Micro)研究報告，於 2006 年 12 月公佈之『2006 年資安威脅綜合報告與 2007 年趨勢預測』指出[5]，在 2006 年中，資安威脅已從廣泛散播轉變為針對特定目標與區域，除了電子郵件與即時訊息資安威脅之外，Web 也已成為資安威脅的有力散播工具，如圖 1 所示。尤其預測在 2007 年使用者將可目睹 Web 的崛起，成為蔓延極廣的資安威脅而且通常是結合多種檔案與資安威脅的混合式威脅。其所遭受的危害，可能包括機密資訊外洩、身分驗證資訊遭竊、感染傀儡程式、被安裝廣告程式/間諜程式等等。

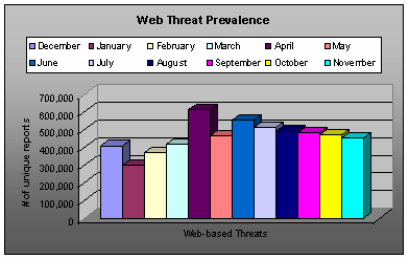

圖 1. Web 資安威脅散播情形

然而 web 應用逐漸在網際網路上被廣泛使用，如 Aparch、ASP、PHP 等，再加上開發者對其所擅長之開發語言所掌握的安全認知不足及本身語言上設計的缺陷存在，都有可能引起攻擊者的注意成為他們攻擊目標，因此這也是新的攻擊事件不斷上演主要原因。

由此可知，在未來 Web 資安威脅趨勢仍延續下去。因為電腦駭客會持續尋找 Web 服務上的弱點將與惡意程式結合在一起，並極有可能運用人性弱點，也就是社交工程(Social Engineering)來進行攻擊，如網路釣魚(Phishing)、垃圾郵件(Spam Mail)

等等。綜觀上述，web application 已嚴然成為駭客攻擊的最佳管道，尤其利用 web 的弱點開啟企業資訊大門的技巧更是日新月異、層出不窮。綜觀上述，如何修補 Web 這方面的漏洞來對抗網路攻擊是個關鍵議題之一。

2.2. 誘捕系統 (Honeypots)

隨著網路攻擊行為的日增成熟，要去學習如何防範一直困擾著系統管理人員；同時，要如何去從攻擊中找出犯罪證據更是關鍵挑戰之一。現今資訊安全防護策略大都注重在已知的威脅上，根本無法因應未知攻擊，在阻擋入侵的同時，也無法真正偵測出入侵者的面貌。如今，隨著資訊科技的進步，開啟運用另一種思維來對抗，將以往被動的防禦，轉為積極學習。這項方法是所謂的誘捕系統(Honeypot)。

根據"Hpoeypots: Tracking Hacker"的定義[8]: 所謂的誘捕系統(Honeypots)是一種資訊系統資源(resourece)，其價值在於未經授權或非法用此資源。Honeypot 一般被認為是放在網路上可以被探測與攻擊的系統，因為 Honeypot 沒有營運的價值(production value)，因此沒有使用的正當性，此意味著任何 Honeypot 的互動，例如：探測或掃描，就其定義而言都是可疑的。

誘捕系統便是一個成功反制的措施，實質上可以拖延攻擊者，同時能提供防禦者足夠的資訊來瞭解對方，避免攻擊造成的損失。而誘捕系統可當作入侵偵測系統來監控，蒐集入侵的證據，瞭解分析攻擊者入侵的手法，可降低攻擊者隨機試探或攻擊的機率，提高主機系統防護安全性。

2.3 Client Honeypot

從早期 honeypot 發展至今大都屬於傳統(server)Honeypot 類型防禦偵測攻擊，主要目的是讓它被駭客偵測、被攻擊以及被惡意程式(exploit code)所危害，概念如圖 2 所示。因此是屬於被動式等待攻擊，如果攻擊者沒有進行攻擊就無法揮發誘捕系統功用，例如 Honeynet[10]採用多台的誘捕系統集合成一個整個誘捕網路，模仿實際或虛擬的網路運作等待入侵者攻擊。

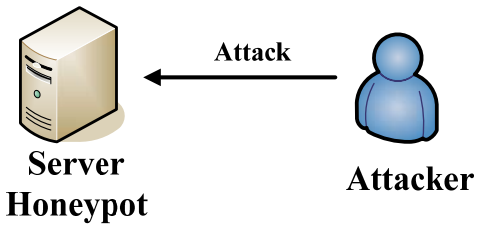

圖 2. Server Honeypot 概念架構

近年來，根據 Lance Spizner (June,2004)所提出新的概念叫做 Client Honeypot 如圖 3 所示，它與傳統的 Server Honeypot 差別在於它是屬於主動式的偵測能與目標主機產生互動性，被設計從惡意主機當中能主動偵測攻擊行為，然而 Server Honeypot 不能主動偵測。就因如此，Client Honeypot 能主動偵測網路上所提供的 Web 服務是否含有惡意的攻擊行為存在。

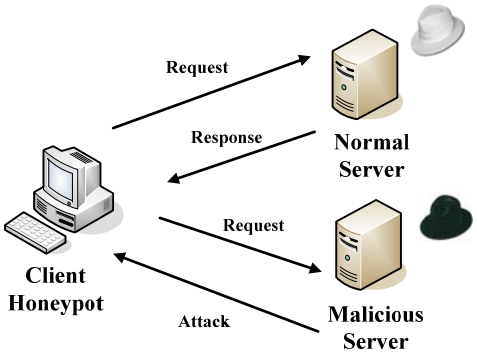

圖 3. Client Honeypot 架構

2.3 現有 Client Honeypot 工具分析

在現有常見 Client Honeypot 中有幾種相似功能的工具，都能判別主機是否為惡意程式，而在下述中將逐一介紹探討。

2.3.1 Honeymonkey

由於有越來越多的網路駭客在研究如何透過瀏覽器(Web Browser)侵犯使用者，然而由軟體服務商微軟(Microsoft)所提出的概念能專門分析某個網站是否存在惡意程式的計畫-HoneyMonkey [12]。而 HoneyMonkey 是一個虛擬系統，該系統

上運行一個 Windows XP 作業系統，它模擬使用者對網際網路上網頁的查詢，查看是否會對 Windows 發動攻擊的網站，及記錄駭客的入侵行為或者蠕蟲病毒攻擊行為，希望以此來保護 window XP 系統不受到攻擊。

其運作方式先執行一個 StriderFlight Data Recorder (FDR)程式來監視目錄中的每一個檔案以及註冊機碼(Registry)的讀寫行為。然後，再執行瀏覽器去瀏覽某一個網站上的網頁資料，並在瀏覽每一個網頁時都會等待數分鐘，且 HoneyMonkey 不接受任何提出安裝要求對話框的請求。在瀏覽網頁時，任何不是建立在瀏覽器暫存目錄中的執行檔都會被 FDR 給記錄下來。HoneyMonkey 就是利用這樣的測試方法來判斷某個網站是否存在惡意的程式碼。但是這種方式需要較好硬體環境來執行，所以建置成本較高且較不容易佈署。

2.3.2 Honeyclient

Honeyclient 是一個 web-based 高互動性 Honeypot，由 Kathy Wang 在 2004 年所提出[11]，它是第一個開放原始碼(open source)client Honypot 由 perl 語法撰寫而成，Honeyclient 是狀態基礎(event-based)並且在 client 端能偵測到攻擊，透過監視特定目錄和註冊鍵。利用密碼雜湊 MD5，在與 server 產生互動之後對目錄和註冊鍵比對這些進行密碼雜湊演算。如果發現跟原本的 Checksum 結果碼不一樣的話，可能判斷為惡意的，而 Honeyclient 缺點是執行速度較慢去 crawl web 和偵測惡意主機。但缺點跟 HoneyMonkey 一樣需要較好的建置硬體成本。

2.3.3 Capture

Capture[9] 是一個高互動性的 Client Honeypot，具有較多的完整功能與潛在的惡意主機互相影響後能辨識出是否為惡意的主機，使用虛擬機器來模擬系統環境以觀察系統狀態的變化，如果系統的狀態變化被偵測判別出來與 Capture 互相影響的主機則會被分類為隱藏有惡意程式的主機。而缺點跟上述的 HoneyMonkey、Honeyclient 相似都需要較好的硬體資源才能有較好的執行效率，且本身操作佈署環境是複雜的。

3. 研究架構方法

本文根據 Client Honeypot 概念，透過修改 HoneyC 開放原始碼[16]，來達到對網路上可能潛在的惡意主機做主動偵測判別，並新增 Snort 規則提升判斷的準確率，產生可能含有惡意攻擊警告訊息讓使用者或管理者提早得知可能為惡意網頁，以利安全防護。

3.1 採用之研究方法與原因

在網路環境不確定因素增加及 Web 資安威脅的快速崛起，本研究是從 Client Honeypot 概念能夠主動對網路上的任何可能潛在的惡意 Web 服務去做偵測，在上述幾個例子都是屬於高互動性功能的 Client Honeypot，主要缺點是硬體成本高，執行效率慢以及不易建置佈署。而 HoneyC 是 Freeware，屬於低互動性的 Client Honeypot，優點為低成本、執行效率快、容易佈署，其本身會模擬 Client 端代替真實系統與 Server 互動，避免真正遭受到攻擊事件的發生，提高網路使者用者自我的防護。

3.2 HoneyC 架構概念

HoneyC 為獨立跨平臺架構[14]，延續低互動性 Client Honeypot 概念為基礎，可分成三個模組分別為 Queuer 模組、Visitor 模組及 Analysis Engine 模組，如圖 4 所示。Queuer 模組使用由網際網路內容提供者(ICP)-Yahoo 所提供的 YahooSearchAPI 進行網址搜尋找到目標主機動作、Visitor 模組模擬 Web 瀏覽器(使用 wget 替代真實瀏覽器)向目標主機進行互動、Analysis Engine 模組採用 Snort Rule[15]為基礎進行演算法分析如特徵比對，比對傳回來的訊息是否有違反安全政策規則。

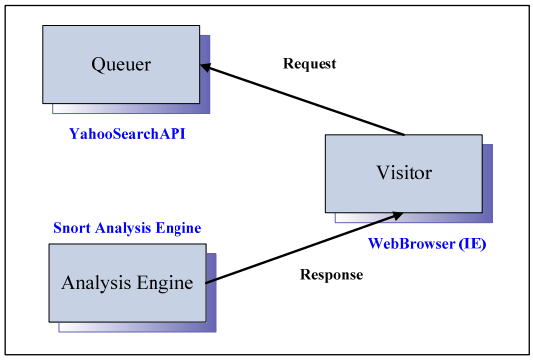

圖 4. HoneyC 模組概念

HoneyC 向目標主機的互動是基於在 HTTP 協定上[7]，提出 HTTP 要求透過 Queuer 模組產生及接受 HTTP 回應訊息透過 Visitor 模組產生，在每個模組之間的訊息處理方式採用 XML(可延伸性標記語言)進行資料間交換傳遞、處理。HoneyC 整體架構，如圖 5 所示。而圖 6 為 HoneyC 運作流程概念。

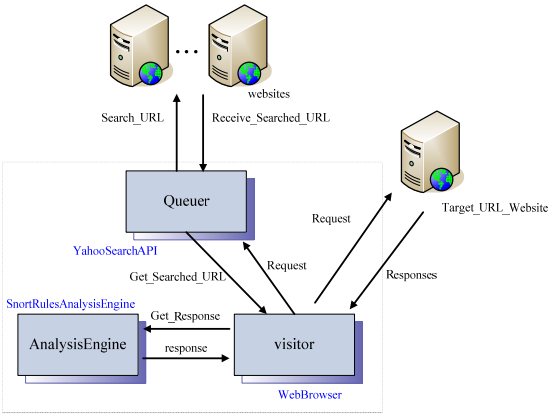

圖 5.HoneyC 架構圖

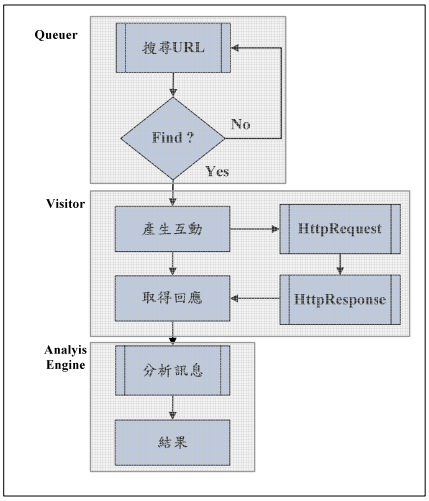

圖 6. HoneyC 運作流程概念

3.3. 系統架構流程

本研究系統架構如圖 7 所示，在此圖左邊是一般網路使用者 Internet 請求 Web 服務，其中可能包含正常 Website 服務或有惡意 Website 服務存在。如果使用者不小心點選到惡意網頁，極有可能遭到包括木馬程式、病毒等攻擊，導致網路威脅性提高。而此圖右邊是模擬 Web 瀏覽器，先代替網路使用者向網際網路上的 Website 請求回應動作，將對方主機所回傳回來的訊息經過本系統分析後，判斷是否為 Positive 或 Negative 網頁，再顯示警告訊息給使用者知道此網頁可能為惡意網頁，避免進入遭受危害。

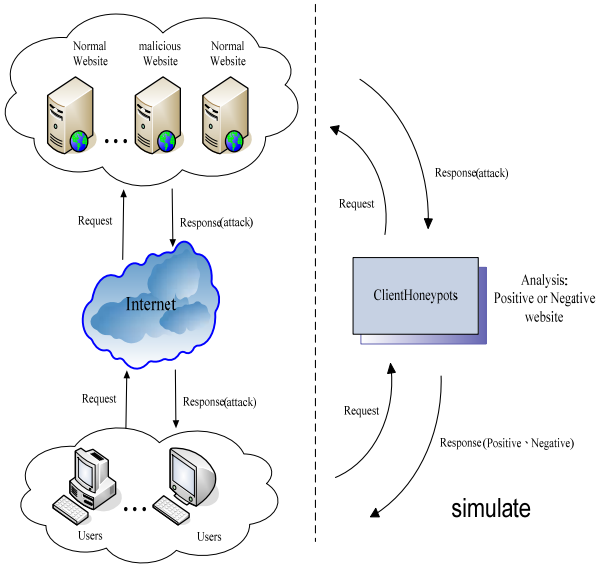

圖 7.系統架構

4. 系統實測結果

本系統實測結果以最近相當熱門的網路釣魚為例，建置一個假網頁利用 Javascript 語法嵌入在網頁中，做一個假網址列圖片覆蓋到真正的瀏覽器中的網址列上，形成看似真實的網址列，而假網頁則以中華電信為例進行測試。以上純屬實驗性質，沒有任何意圖。

4.1 系統實驗環境架構

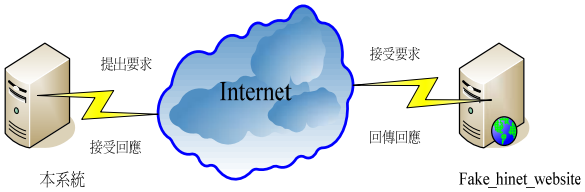

圖 8.實驗環境架構

在此實驗環境中如圖 8 所示，使用兩台主機進行測試，分別為本系統主機與假的 Web 服務主機，而在假的 Web 服務主機中架設偽造中華電信網頁如圖 9 所示。本研究在進行實測部份，會向假的 Web 服務主機提出要求回應訊息，而在假 Web 服務則會回傳訊息給本系統，在接受回應訊息後進行分析是否能正常運作於真實網路上。

圖 9.偽造網頁

4.2 系統實驗結果

在 SnortAnalysisEngine 模組中增加一條防護 Phishing 的 Snort Rules[6]，以增加判斷準確率，下述為它的規則範例:

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"BLEEDING-EDGEMSIEHidden AddressBar(Phish)";flow:to_client,established; content:"window.createpopup";nocase; content:"innerhtml";nocase;content:"vuln_"; nocase;reference:url,www.guninski.com/popspoof.html;reference:url,securityresponse.symantec.com/avcenter/venc/data/js.trojan.blinder.html; classtype:trojan-activity; sid:2001813; rev:3;)

圖 10 為未增加 Anti-Phishing rules 時，我們對偽造的網頁進行測試時，並無偵測出假的網址列，只有偵測出一般的網頁內容回應。

圖 10. 未增加 snort rules 的分析訊息

圖 11 為增加 Anti-Phishing rules 後，即可偵測出偽造網頁裡含有假的網址列，如圖中的紅色框所示，且被歸類為網路木馬攻擊，主機位址為 http://abin.mis.nkfust.edu.tw 跟原本中華電信網址不一樣，由此可知經過分析後認為此網頁可能是偽造的 Phishing 網頁。

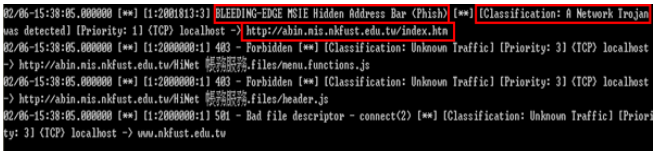

圖 11. 增加 snort rules 的分析訊息

5. 結論

在現今網路快速普及的時代，使的提供 Web 服務也越來越多樣化，但這也是最常被忽略的網路威脅之一。一般網路使用者在網際網路上瀏覽網頁時，很可能一個不注意即遭受到網路駭客所設下的陷阱而遭受損害。本研究探討 Client Honeypot 概念，以防護網際網路上惡意網站的攻擊，並利用修改 HoneyC 開放原始碼，增加 Snort 規則檔來提升判斷惡意網站的準確率，並進行實際測試是否能有效達到所要偵測的功能。

HoneyC 具有低互動性的特質，與現有其它 Client Honeypots 工具相比較仍擁有許多優點，然而如何更提高其偵測判斷的準確度，在未來仍有值得改善及發展的地方，我們預期增加更多精確

的規則檔及縮短判斷時間，可考慮結合異常偵測技術與誤用偵測的技術進行雙重檢核或許可以更精確改進其準確度，以降低日益嚴重的惡意 Web 服務所引起的網路威脅。

ACKNOWLEDGEMENT

This work was supported in part by TWISC@NCKU, National Science Council under the Grants NSC 94-3114-P-006-001-Y.

參考文獻

1. 王茂吉(2003)。適用於網頁伺器之應用型入侵偵測系統。私立中原大學資訊工程研究所碩士學位論文。桃園縣。
2. 刑事局(2007)。假網頁釣密碼 駭客盜領千萬。刑事警察局科技犯罪防制中心。 2007 年 02 月 08 日。取自 http://www.cib.gov.tw/index.aspx
3. 薛宇盛(民 95)。入侵偵測系統實務-WinSnort For Windows 2003 Server。台北市：松崗
4. 賴榮滄（2004）。以入侵偵測系統為基礎之主動式網頁過濾及阻擋機制。私立逢甲大學資訊工程研究所碩士學位論文。台中市。
5. 趨勢科技(2007)。2006 年資安威脅綜合報告與 2007 年趨勢預測。2007 年 12 月 15 日，取自 :http://www.trendmicro.com.tw/pr/report/2006_Annual_Threat_Roundup.doc。
6. bleedingsnort(2003), Retrieved February 2007, form World Wide Web http://www.bleedingsnort.Com/.
7. Fielding, R., Gettys, J., Mogul, J. C., Frystyk, H., Leach, P., and Berners-Lee, T.(1999) ,Hypertext Transfer Protocol – HTTP/1.1, Retrieved DecembEr(2006), form World Wide Web http://tools.ieft.org/html/.
8. Lance Spitzner (1999), Honypot: To Build A HonEypot, Retrieved February,2007, from World WidE Web http://www.spitzner.net/honeypot.html
9. mara, F., Tang, Y., Steenson, R., and Seifert, C. (2006)Capture - Honeypot Client, Retrieved December 2006, from World Wide Web http://capture-hpc.source/.
10. The Honeynet PROJECT, Retrieved April 25, 2007, from the World Wide Web: http://www.honeynet.org./
11. Wang, K. Honeyclient, Version 0.1.1, Retrieved January 2007, from the World Wide Web: http://www.honeyclient/.
12. Microsoft(2005), The Strider Honeymonkey Proj Ect, Retrieved February 2007, from the World Wid E Web : http://research.microsoft.com/MoneyMonkey/.
13. M. Roesh.(1999), Snort-Lightweight Instrusion Detection for Netwrok, In Proceedings of LISA 1999:13th System Admininstration Conference, Nov. 7-12
14. Seifert, C.(2006), HoneyC - The Low-Interaction Client Honeypot, 2006. Retrieved .October 2006 from the World Wide Web : http://honeyc.sourceforge.net/.
15. Snort (1998), The Open Source Network Intrusion Detection System Retrieved November, 2007 from World Wide Web: http://www.snort.org/
16 Sourceforge (2004), Open Source Software Development projects, Retrieved August,2006 , from World Wide Web: http://sourceforge.net