

# 基於 Tripwire 檢測工具以偵測變形 Rootkit 之研究

林明孝、曹偉駿

E-mail: 9510752@mail.dyu.edu.tw

## 摘要

現今的網際網路發展迅速且成熟，駭客的人數不斷的快速成長，而入侵行為也漸趨變化與複雜，駭客得以針對Linux或Windows作業系統的漏洞與弱點來發展出多樣化的攻擊技術，如病毒、蠕蟲、特洛依木馬、後門程式與Rootkit等惡意軟體。要如何維護系統安全，避免遭受到駭客的入侵，成了當下相當重要的議題。一般的主機型入侵偵測系統大多以過濾Syslog或稽核追蹤，來找出可能被攻擊的證據，但駭客可經由植入Rootkit來取得root權限或留下後門，以使其再次地入侵系統並竄改系統程式，而系統管理者卻難以發現其蹤跡。因此，本研究從Linux系統管理者的角度進行探討，找出作業系統是否已被植入User Mode Rootkit。在所設計的偵測機制中，首先使用Chkrootkit工具偵測目前已知的Rootkit，再針對此已知Rootkit入侵特性藉由Tripwire來檢測系統檔案的完整性，以從資料庫中找出被變形Rootkit所異動的項目，再與已知型Rootkit所會異動的項目做比對，因而找出變形Rootkit，藉此提昇變形Rootkit惡意軟體之偵測能力。本論文最後亦實際模擬測試，以驗證所提偵測機制之高效益。

關鍵詞：惡意軟體；入侵偵測系統；Rootkit；Linux

## 目錄

封面內頁 簽名頁 授權書.....	iii	中文摘要.....	iv	英文摘要.....	v	誌
謝.....	vi	目錄.....	vii	圖目錄.....	x	表目
錄.....	xiii	第一章 緒論 1.1 研究背景與動機.....	1	1.2 研究目的.....	1	1.3 論文
架構.....	6	第二章 文獻探討 2.1 入侵偵測系統.....	8	2.1.1 入侵的類型.....	8	2.1.2
入侵偵測系統的種類.....	10	2.2 Rootkit惡意軟體.....	11	2.2.1 電腦病毒種類.....	11	2.2.2
Rootkit原理與應用.....	19	2.2.3 比較分析.....	22	2.3 主機型入侵偵測分析的資料來源.....	24	
2.3.1 系統呼叫(system call).....	24	2.3.2 使用者的歷史指令記錄檔.....	25	2.3.3 主機端的網路流量.....	25	
25 2.3.4 主機端的記錄檔.....	25	2.3.5 檔案的雜湊(hash)值.....	26	2.3.6 相似度.....	27	
2.3.7 比較分析.....	28	2.4 Rootkit現有的偵測技術探討.....	29	2.4.1 交叉察看偵測.....	30	
2.4.2 硬體式偵測.....	31	2.4.3 行為偵測.....	32	2.4.4 特徵偵測.....	33	2.4.5 完整性
偵測.....	35	2.4.6 比較分析.....	38	第三章 基於Tripwire檢測工具以偵測變形Rootkit 3.1 研究流		
程.....	40	3.2 偵測工具分析.....	41	3.2.1 Chkrootkit工具.....	42	3.2.2 Tripwire工
具.....	43	3.3 Rootkit偵測機制設計.....	45	3.3.1 User mode Rootkit入侵於Linux系統之分析..	45	3.3.2 偵
測流程之設計.....	47	3.3.3 記錄檔特徵比對演算法.....	54	第四章 系統實作與模擬測試 4.1 實驗環		
境.....	56	4.2 系統前置處理.....	57	4.3 系統介面與各功能說明.....	66	4.4 系統模擬與
測試.....	71	4.5 實驗結果與分析比較.....	93	第五章 結論與未來展望 參考文獻.....		
	98					

## 參考文獻

- Abraham, A., Grosan C., & Chen, Y. (2005). Cyber Security and the Evolution of Intrusion Detection Systems. Retrieved March 28, 2006, from <http://www.cs.ubbcluj.ro/~cgrosan/kerala.pdf>. Andreas, B. (2004). UNIX and Linux based Rootkits Techniques and Countermeasures. Retrieved May 10, 2006, from [https://www.dfn-cert.de/team/bunten/rootkits\\_first2004.pdf](https://www.dfn-cert.de/team/bunten/rootkits_first2004.pdf). F-SECURE (2006). F-Secure BlackLight. Retrieved April 25, 2006, from <http://www.f-secure.com/blacklight>. Butler, J., & Hoglund, G. (2005). VICE-Catch the hookers. Retrieved March 22, 2005, from <http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-butler/bh-us-04-butler.pdf>. Butler, J., Undercoffer, J. L., & Pinkston, J. (2003). HIDDEN PROCESS:The Implication for Intrusion Detection. Proceedings of the 2003 IEEE Workshop on Information Assurance.(pp. 116-121). Chkrootkit(2005). Locally checks for signs of a rootkit. Retrieved December 5, 2005, from <http://www.chkrootkit.org>. CERT/CC Statistics (1988-2006). Retrieved May 19, 2006, from [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html). Cohen, F.(1987). Computer viruses-theory and experiments. Computers & Security, 6(1), 22-35. Chen, S., & Ranka, S. (2005). Detecting Internet Worms at Early Stage. IEEE Journal on Selected Areas in Communications, 23(10), 2003-2012. Chebrolu, S., Abraham A., & Thomas, J. (2005). Feature Deduction and Ensemble Design of Intrusion Detection Systems. Computers & Security, 24(4), 295-307. Daniels, T., & Spafford, E. H. (1999). Identification of Host Audit Data to

Detect Attacks on Low-level IP Vulnerabilities. ACM Journal of Computer Security, 7(1), 3-35. DeMara, R. F., & Rocke, A. J. (2004). Mitigation of network tampering using dynamic dispatch of mobile agents. Computers & Security, 23(1), 31-42. Feng, Li., Guan, X., Guo, S., Gao, Y., & Liu, P. (2004). Prediction the intrusion intentions by observing system call sequences. Computers and Security, 23(3), 241-252. F-SECURE (2006).

F-Secure. Retrieved May 15, 2006, from <http://www.f-secure.com/>. Forrest, S., Hofmeyr, A. S. A., Somayaji, A., & Longstaff, T. A. (1996). A Sense of Self for Unix Process. IEEE Symposium on Security & Privacy, 120-128. Felten, E. W., & Halderman, J. A. (2006). Digital Rights Management, Spyware, and Security. IEEE Security & Privacy, 4(1), 18-23. Hawkins, S. (2002). Understanding the Attackers Toolkit. Retrieved May 25, 2006, from [http://www.giac.org/practical/gsec/Sunnie\\_Hawkins\\_GSEC.pdf](http://www.giac.org/practical/gsec/Sunnie_Hawkins_GSEC.pdf). Jha, S., & Hassan, M. (2002). Building Agents for rule-based intrusion detection system. Computer Communications, 25(15), 1366-1373. Kim, G. H. & Spafford, E. H. (1994). The Design and Implementation of Tripwire: A File System Integrity Checker. Proceedings of the 2nd ACM Conference on Computer and Communications Security. (pp.18-29). Kuhnhauser, W. E. (2004). Root kits: An operating systems viewpoint. ACM SIGOPS Operating Systems Review, 38(1), 12-23. King, S. T. & Chen, P. M. (2005). Backtracking Intrusions. ACM Transactions on Computer Systems(TOCS), 23(1), 51-76. Kim, G. H. & Spafford, E. H. (1994). Experiences with Tripwire:Using Integrity Checkers for Intrusion Detection. Proceeding of 2nd ACM Conference on Computer and Communications Security. Kruegel, C., Robertson, W., & Vigna, G. (2004). Detection Kernel-Level Rootkits Through Binary Analysis. Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC). Lee, W., Fan, W., Miller, M., Stolfo, S., & Zadok, E. (2002). Toward Cost-Sensitive Modeling for Intrusion Detection and Response. Journal of Computer Security, 10(1-2), 5-22. Leu, F. Y. & Yang, T. Y. (2003). A Host-based Real-Time Intrusion Detection System with Data Mining and Forensic Techniques. Proceedings of the 37th IEEE Annual International Carnahan Conference on Security Technology, (pp. 580-586). Levine, J., Culver, B., & Owen, H. (2003). A Methodology for Detecting New Binary Rootkit Exploits. Proceedings IEEE SouthEastC on 2003. Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., Weber, D., Webster, S. E., Wyschogrod, D., Cunningham, R. K., & Zissman, M. A. (2000). Evaluating Intrusion Detection System: the 1998 DARPA Off-Line Intrusion Detection Evaluation. Proceedings of the 2000 DARPA Information Survivability Conference and Exposition. Maxion, R. A. (2003). Masquerade Detection Using Enriched Command Lines. Proceedings of International Conference on Dependable Systems and Networks, (pp. 5-14). Mao J., & Jain, A. (1996). A Self-Organizing Network for HyperEllipsoidal Clustering. IEEE Transactions on Neural Networks, 7(1), 16-29. CSI/FBI. (2006). New FBI Computer Crime Survey. Retrieved April 19, 2006, from [http://www.fbi.gov/page2/jan06/computer\\_crime\\_survey011806.htm](http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm), 2006. Nachenberg, C. (1999). Computer Parasitology. Proceedings of the Ninth International Virus Bulletin Conference. Oh S. J., & Kim, J.Y. (2004). A Hierarchical Clustering Algorithm for Categorical Sequence Data. Information Processing Letters, 91(3), 135-140. Petroni, N., Fraser, T., Molina, J., & Arbaugh, W. (2004). Copilot-a Coprocessor-based Kernel Runtime Integrity Monitor. Proceedings of the Usenix Security Symposium. Rootkit Revealer. Retrieved May 27, 2006, from <http://www.sysinternals.com/Files/RootkitRevealer.zip>. Red database security. <http://www.red-database-security.com/>. Rkhunter. Retrieved February 20, 2006, from <http://www.rootkit.nl/>. Rootcheck. Retrieved February 22, 2006, from <http://www.ossec.net/en/rootcheck.html>. Rutkowska, J. (2005). Thoughts about Cross-View based Rootkit Detection. Retrieved May 10, 2006, from [http://www.invisiblethings.org/papers/crossview\\_detection\\_thoughts.pdf](http://www.invisiblethings.org/papers/crossview_detection_thoughts.pdf). Somayaji, A., & Forrest, S. (2000). Automated Response Using System-Call Delays. Proceedings of the 9th Usenix Security Symposium. (pp. 185-197). Stearley, J. (2004). Towards Informatic Analysis of Syslogs. Proceedings of the IEEE International Conference on Cluster Computing. (pp. 309-318). Security Focus. Retrieved May 21, 2006, from <http://www.securityfocus.com/infocus/1854>. Symantec Caught in Norton ' Rootkit ' Flap. Retrieved June 12, 2006, from <http://www.eweek.com/article2/0,1895,1910077,00.asp>. Sysinternals Freeware. Retrieved June 18, 2006, from <http://www.sysinternals.com/>. Spaffod, E. H.(1991). The Internet Worm Incident. Technical Report. Thimbleby, H., Anderson, S., & Cairns, P. (1998). A framework for Modelling trojans and computer virus infection. Computer Journal, 41(7), 444-458. Tripwire. Retrieved March 17, 2006, from <http://www.tripwire.com>. Tripwire Security Inc. Retrieved June 22, 2006, from <http://www.tripwiresecurity.com>. TRENDMICRO. Retrieved May 9, 2006, from <http://www.trendmicro.com/la/home/enterprise.htm>. Wang, Y. M., Beck, D., Vo, B., Roussev, R., Verbowski, C. (2005). Detecting Stealth Software with Strider GhostBuster. Proceedings of the 2005 International Conference on Dependable Systems and Networks. (pp. 368-377). Zovi, D. D. (2004). Kernel Rootkits. Retrieved May 14, 2006, from <http://www.sans.org/rr/papers/60/449.pdf>, 2004.