整合誘捕與弱點檢測技術之入侵偵測機制

孫學智、曹偉駿

E-mail: 9707370@mail.dyu.edu.tw

摘 要

為了保護系統與通訊的安全，在傳遞過程中透過一些通訊的加密機制，如：SSH、SSL。為了保護網路不受到惡意的攻擊，亦發展出不同的防禦系統，如：防火牆、弱點掃瞄、誘捕系統和入侵偵測系統。雖然可由弱點檢測了解網路潛在威脅，但實際遭遇攻擊時，防火牆與入侵偵測系統卻常因為樣本(Patterns)老舊或不足，造成誤報或誤判，無法有效發揮預警功能。若能搭配誘捕系統，取得駭客攻擊或病毒發起之特徵，即可協助管理者加強網路與系統之安全。 目前文獻大多指出，誘捕系統多為單獨的高互動或低互動環境，有經驗的入侵者透過連結服務時，可經由主機回應(ICMP)的時間或下達進階指令(如FTP的 hash指令)，辨識是否為誘捕環境，進而選擇繼續攻擊或離開。就管理者而言，誘捕系統所捕獲的資料有時太繁雜，無法有效的進行入侵分析。因此，本研究基於混合式誘捕環境，將誘捕系統所收集的攻擊特徵資料與系統弱點掃描檢測之結果，分別透過前置處理後進行比對，若比對符合，則以電子郵件通知管理者，讓管理人員能更快了解攻擊的發生。

關鍵詞 : 誘捕系統;入侵偵測系統;網路安全;區域網路

目錄

參考文獻

一、中文部份 資策會FIND/經濟部技術處(2008)，創新資訊應用研究計劃[線上資料]，來源: http://www.iii.org.tw/[2008, January 2] 賴溪松(2004)，網路攻防實驗教材，資通安全:系列14，資通安全專輯，台北:財團法人國家實驗研究院科技政策研究與資訊中心。 二、英文部份 Arkin, O. (2001). ICMP Usage in Scanning, The complete Know-How [Online]. Available: http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf [2001, June 1]. Artaila, H., Safab, H., Sraja, M., Kuwatlya, I., & Al-Masria, Z. (2006). A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks. Computers & Security, 25(4), 274-288. Balas, E. (2003). Know your enemy: Sebek [Online]. Available: http://www.honeynet.org/papers/sebek.pdf [2003, November 17]. Balas, E., Travis, G., & Viecco, C. (2006). A Dynamic Filtering Technique for Sebek System Monitoring. Proceedings of the Information Assurance Workshop (pp. 275 – 282), USA: Military Academy of New York. Biermann, E., Cloete, E., & Venter, L. M. (2001). A comparison of intrusion detection system. Computer and Security, 20(8), 676-683. CERT, (2008). Publications about vulnerabilities [Online], Available: http://www.cert.org/stats/cert_stats.html [2008, Apr 14]. Cliff, S. (1990). The Cuckoo ’ s Egg:Tracking a Spy through the Maze of Computer Espionage. New York:Pocket Books. Cukier, M., & Panjwani, S. (2007). A Comparison between Internal and External Malicious Traffic. Proceedings of the 18th IEEE International Symposium on Software Reliability (pp. 109-114), Sweden: University West of Trollha"ttan. Dacier, M., Pouget, F., & Debar, H. (2004). Honeypots: practical means to validate malicious fault assumptions. Proceedings of the 10th Pacific Rim International Symposium on Dependable Computing (pp. 383-388), French Polynesia: Tahiti of Papeete. David, W. (2007). Honeynets: a tool for counterintelligence in online security. Network Security, 2007(1), 4-8. Denning, D. E. (1987). An Intrusion Detection Model. IEEE Transactions on Software Engineering, 13(2), 222-232. FBI/CSI, (2007). Computer crime and security survey [Online]. Available: http://gocsi.com/forms/csi_survey.jhtml [2007, August 27]. Fu, X., Yu, W., Cheng, D., Tan, X., Streff, K., & Graham, S. (2006). On Recognizing Virtual Honeypots and Countermeasures. Proceedings of the 2nd IEEE International

Symposium on Dependable, Autonomic and Secure Computing (pp. 211-218), USA: University of Indianapolis. Gordon, L. (2006). Top 100 Network Security Tools [Online]. Available: http://sectools.org [2006, December 1]. Grundshober, S. (1998). Sniffer Detector Report [Online]. Available: http://www.eurecom.fr/~nsteam/Papers/grundschober98.ps [1998, June 26]. Han, H., Lu, X. L., Lu, J., Bo, C., & Yong, R. L. (2002). Data Mining Aided Signature Discovery in Network-based Intrusion Detection System. Operating Systems Review, 36(4), 7-13. Hart, R., Morgan, D., & Tran, H. (1999). An introduction to automated intrusion detection approaches. Information Management & Computer Security, 1999(7), 76-82. Helmer, G., Wong, J., Honavar, V., & Miller, L. (2002). Automated discovery of concise predictive rules for intrusion detection. Journal of Systems and Software, 60(3), 165-175. Hilley, S. (2002). At last, a wireless honeypot. Network Security 2002(8), 1-2. Illgun, K., Kemmerer, R., & Philips, A. (1995). State Transition Analysis: A Rule-based Intrusion Detection Approach. IEEE Transaction on Software Engineering, 14(2), 181-199. Innella, P., & McMillan O. (2001). An Introduction to IDS [Online]. Available: http://www.securityfocus.com/infocus/1520 [2001, December 6]. ITU. (1991). X.800:Security architecture for Open Systems Interconnection for CCITT applications [Online]. Available: http://www.itu.int/rec/T-REC-X.800-199103-I/e [1991, August 30]. Jostein, J. (2008). A Novel Testbed for Detection of Malicious Software Functionality. Proceedings of the Third International Conference on the Availability, Reliability and Security (pp. 292-301), Spain: Technical University of Catalonia. Khosravifar, B., & Bentahar, J. (2008). An Experience Improving Intrusion Detection Systems False Alarm Ratio by Using Honeypot. Proceedings of the 22nd International Conference on Advanced Information Networking and Applications (pp. 997-1004), Japan: Okinawa of GinoWan. Krawetz, N. (2004). Anti-honeypot technology. Security & Privacy, 2(1), 76-79. Kreibich, C., & Crowcroft, J. (2004). Honeycomb: creating intrusion detection signatures using honeypots. ACM SIGCOMM Computer Communication, 34(1), 51-56. Maheswari, V., & Sankaranarayanan, P. E. (2007). Honeypots: Deployment and Data Forensic Analysis. Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (pp. 129-131), Sweden: University West of Trollha"ttan. Matthias, B., Thomas, D., & Bernhard, P. (2007). Enhanced Internet security by a distributed traffic control service based on traffic ownership. Journal of Network and Computer Applications, 30(3), 841-857. Mukkamala, S., Yendrapalli, K., Basnet R., Shankarapani, M. K., & Sung, A. H. (2007). Detection of virtual environments and low interaction honeypots. Proceedings of the Information Assurance and Security Workshop (pp. 92-98), USA: Military Academy of New York. Pejovic, V., Kovacevic, I., Bojanic, S., Leita, C., Popovic, J., & Nieto, T. O. (2007). Migrating a HoneyDepot to Hardware. Proceedings of the International Conference on Emerging Security Information, Systems, and Technologies (pp. 151-156), Spain: Valencia. Provos, N. (2004). A virtual honeypot framework. Proceedings of the 13th USENIX Security Symposium (pp. 1-14), USA: San Diego. Provos, N. (2007). The Honeyd [Online]. Available: http://www.honeyd.org [2007, March 27]. Rathgeb, E. P., & Hoffstadt, D. (2008). The E-Mail Honeypot System Concept, Implementation and Field Test Results. Proceedings of the 2nd International Conference on the Digital Society (pp. 1-6), Martinique: Sainte Luce. Ray, P. (2007). Host Based Intrusion Detection Architecture for Mobile Ad Hoc Networks. Proceedings of the 9th International Conference on Advanced Communication Technology (pp. 1942-1946). Korea: Phoenix Park. Roesch, M. (1999). Snort: Lightweight Intrusion Detection for Networks. Proceedings of the 13th Conference on Systems Administration (pp. 229-238), USA: Washington of Seattle. Sadasivam, K., Samudrala, B. & Yang A. T. (2005). Design of network security projects using honeypots. Journal of Computing Sciences in Colleges, 20(4), 282-293. Serpanos, D. N., & Lipton, R. J. (2001). Defense agisnt man-in-the-middle attack in client-server systems. Proceedings of the Sixth IEEE Symposium on Computers and Communications (pp. 9-14), Tunisia: Hammamet. Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Schwartz, B., Kent, S. T., & Strayer, W. T. (2002). Single-packet IP traceback. IEEE/ACM Transactions on Networking, 10(6), 721-734. Spitzner, L. (2002). Honeypot: tracking hackers, Addison Wesley. Spitzner, L. (2003). Honeypots-Definitions and Value of Honeypots [Online]. Available: Dec 1, (2003), Available: http://www.trackin g -hackers.com/papers/honeypots.html [2007, August 17]. Spitzner, L. (2005). Know Your Enemy:Honeywall CDROM Roo [Online]. Available: http://www.honeynet.org/papers/cdrom /roo/index.html [2005, August 17]. Spitzner, L. (2008). The Honeywall CDROM Roo [Online]. Available: http://www.honeynet.org/tools/index.html [2008, June 6]. Verwoerd, T., & Hunt, R. (2002). Intrusion detection techniques and approaches. Computer Communication, 2002(25), 1356-1365. Watson, D. (2007). Honeynets: a tool for counterintelligence in online security. Network Security, 2007(1), 4-8. William, S. (2004). Network security essentials:Applications and standards. Pearson. Withall, M., de Silva, M. S., Parish, D., & Phillips, I. (2007). Honey Plotter and the Web of Terror. Proceedings of the 16th International Conference on Computer Communications and Networks (pp. 1262-1266), USA: Hawaii of Honolulu. Xie, M., Wu, Z., & Wang H. (2007). HoneyIM: Fast Detection and Suppression of Instant Messaging Malware in Enterprise-Like Networks, Proceedings of the 23rd Annual Computer Security Applications (pp. 64-73), USA: Florida of Miami Beach. Zhang, Y. F., Xiong, Z. Y., & Wang, X. Q. (2005). Distributed intrusion detection based on clustering. Proceedings of the Fourth International Conference on Machine Learning and Cybernetics (pp.2379-2383), China: Guangzhou.