運用網路誘捕系統對入侵行為之分析與實作

楊景隆、曹偉駿

E-mail: 9314333@mail.dyu.edu.tw

摘 要

現今大部份的資訊安全專家分析網路資料，找出入侵者的行為模式，並發展新的偵測規則給入侵偵測系統(Intrusion Detection Systsem, IDS)使用，但是這工作是依靠專家的能力和知識，總是辛苦和耗時，而且有時不能保證完成可以偵測出入侵行為。　　本研究描述在應用Honeynet架構下分析發覺網路入侵和攻擊行為，本研究運用了一個網路誘捕系統收集、擷取入侵者的惡意行為，因此收集到的資料是惡意的行為，並詳盡的紀錄入侵者活動的行為，資料量當然是比完全在網路上擷取所有封包還要少的很多，而且有意義。　　本研究認為一個入侵行為是由一連串的有次序的警報事件所組成，所以在資料的分析上，採取情節法則的探勘方式，可以解析出更具有代表性的惡意網路行為特徵。

關鍵詞 : 網路安全、入侵偵測系統、網路誘捕系統、情節法則

目錄

目錄 封面內頁 簽名頁 授權書………………………………………………………………iii 中文摘要…………………………………………………………………..v 英文摘要…………………………………………………………........vi 誌謝…………………………………………………………………...…vii 目錄……………………………………………………………………..…viii 圖目錄………………………………………………………………………..x 表目錄………………………………………………………………………xi 第一章　緒論 1 1.1　研究背景與動機 1 1.2　研究目的 1 1.3　研究流程 2 第二章　文獻探討 5 2.1　入侵偵測系統 5 2.1.1　入侵偵測系統的簡介 5 2.1.2　現行入侵偵測技術的限制 9 2.1.3　免費的小型入侵偵測系統-SNORT 10 2.2　入侵行為的探討 12 2.3　誘捕系統 14 2.3.1　誘捕系統的簡介 14 2.3.2　誘捕系統的分類 18 2.3.3　誘捕系統所面臨的法律問題 22 2.4　資料探勘 24 2.4.1　行為模式探勘 24 2.4.2　關聯法則 25 2.4.3　情節法則 27 第三章　系統設計與研究方法 30 3.1　系統網路架構 30 3.2　紀錄模組 31 3.2　實作模式 33 3.3　分析方法 36 第四章　研究實作 41 4.1　系統使用平台架構設備 41 4.2　程序設計 44 4.2.1　產生候選情節 45 4.2.2　辨識序列中情節 47 4.3　實作過程 50 第五章　結論與未來研究方向 56 5.1　結論 56 5.2　未來研究方向 57 參考文獻 58 附錄一 62 附錄二 66

參考文獻

參考文獻 [1] R. Agrawal and R. Srikant. "Mining Sequential Patterns," Proceedings of the Eleventh International Conference on Data Engineering, pp. 3-14, 1995.

[2] B. Caswell, "Snort 2.0 Intrusion Detection," Syngress Publishing, Inc., 2003.

[3] W. W. Cohen, "Fast Effective Rule Induction," Proceedings of the 12th International Conference on Machine Learning, 1995.

[4] J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," Fuzzy Information Processing Society, NAFIPS 19th International Conference of the North American, pp. 301-306, 2000.

[5] J. E. Dickerson, J. Juslin, O. Koukousoula and J.A. Dickerson, "Fuzzy intrusion detection," IFSA World Congress and 20th NAFIPS International Conference, vol. 3 , pp. 1506-1510, 2001.

[6] T. Dobrowiecki, "Episode Mining to Automatically Filter False Alarms," Proceedings of the 10th PhD Mini-Symposium on IEEE Hungary Section, pp. 44-45, 2003.

[7] H. Han, X. L. Lu, J. Lu, C. Bo and R. L. Yong, "Data mining aided signature discovery in network-based intrusion detection system," Source ACM SIGOPS Operating Systems Review, vol.36 , Issue 4, pp. 7-13, 2002.

[8] W. Lee, S.J. Stolfo and K.W. Mok, "A data mining framework for building intrusion detection models" Proceedings of the 1999 IEEE Symposium on Security and Privacy, pp. 120-132, 1999.

[9] J. Levine, R. Labella, H. Owen, D. Contis and B. Culver, "The use of Honeynets to detect exploited systems across large enterprise networks," Information Assurance Workshop on IEEE Systems, Man and Cybernetics Society, pp. 92-99, 2003.

[10] J. Luo, S. Bridges, and R. B. Vaugham, "Fuzzy Frequent Episodes for Real-time Intrusion Detection," IEEE International Conference on Fuzzy Systems, pp. 368-371, 2001.

[11] H. Mannila and H. Toivonen. "Discovering Generalized Episodes using Minimal Occurrences," Proceedings of the Second Int'l Conf. on knowledge discovery and data mining, 1996.

[12] H. Mannila, H. Toivonen, and A. I. Verkamo. "Discovery of Frequent Episodes in Event Sequences," Data Mining and Knowledge Discovery, 1997.

[13] N. Provos, "A Virtual Honeypot Framework," Center for Information Technology Integration of University of Michigan Technical Report 03-1, 2003, http://www.citi.umich.edu/techreports/ [14] R. Rehman, "Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID, " Prentice Hall PTR; 1st edition, 2003.

[15] L. Spitzner, "Honeypots: Tracking Hackers," Addison-Wesley Pub Co., 2003.

[16] L. Spitizner, "The Honeynet Project:Trapping the Hackers," IEEE Security & Privacy, vol. 1, No. 2, pp. 15-23, 2003.

[17] L. Spitzner, "Honeypots: Definitions and Value of Honeypots," http://www.tracking-hackers.com/papers/honeypots.html [18] R. Srikant, and R. Agrawal, "Mining Generalized Association Rules," Proceedings of the 21st Int'l Conference on Very Large Databases, 1995.

[19] L. C. Wu, and S. F. Chen, "Building Intrusion Pattern Miner for Snort Network Intrusion Detection System," The IEEE International Carnahan Conference on Security Technology, ICCST2003, pp. 477-484, 2003.

[20] S. Yeldi, S. Gupta, T. Ganacharya, S. Doshi and D. Bahirat, "Enhancing network intrusion detection system with honeypot," TENCON 2003. Conference on Convergent Technologies for Asia-Pacific Region, vol. 4, pp. 1521-1526, 2003.

[21] J. Yin, G. Zhang and Y. Chen, "Intrusion discovery with data mining on honeynet," International Conference on Machine Learning and Cybernetics, pp. 41-45, 2003.

[22] F. Zhang, S. Zhou, Z. Qin and J. Liu, "Honeypot: a Supplemented Active Defense System for Network Security," Proceedings of the Fourth International Conference on Parallel and Distributed Computing Applications and Technologies, pp. 231-235, 2003.

[23] Analysis Console for Intrusion Databases (ACID), http://acidlab.sourceforge.net/ [24] The Honeynet Project Whitepapers, http://project.honeynet.org/papers/index.html [25] The Honeynet Project Tools for Honeynets, http://project.honeynet.org/tools/index.html [26] Snort, http://www.snort.org [27] Snort_inline, http://snort-inline.sourceforge.net [28] Zone-H.org Stats & graphs, http://www.zone-h.org/en/stats