基於資料挖掘之Linux無線區域網路入侵偵測系統

梁成揚、曹偉駿

E-mail: 9608084@mail.dyu.edu.tw

摘 要

隨著無線區域網路的蓬勃發展，以及Linux 的使用者日益增加，因此無線區域網路環境下Linux 的安全也越來越受重視。本研究針對無線區域網路下的Linux 多種系統記錄檔，進行入侵偵測研究。我們首先發展高準確度的階層式群集分析機制，使得可以自行產生適當群集數，也可自行判斷正、異常群集。而所得的正、異常群集再透過關聯法則探勘技術，以建立入侵偵測法則。除了關聯法則探勘外，在法則探勘的階段，本研究亦結合了情境法則探勘技術，如此作法可以一併找出單一攻擊事件並且亦能於各群集中找出多重序列間的相互關係，以發掘出攻擊事件的組成及發生次序，並將上述這些具備正常或異常行為判斷能力之法則，分別建構於正常或異常的法則資料庫中。另外，為後續不斷增加的系統記錄檔，我們使用漸增式法則探勘技術，來更新法則庫，使得藉由漸增式模糊關聯法則與情境法則的比對，讓系統管理者對駭客入侵攻擊手法有更深入的了解。綜合上述，我們所建構的系統實為一功能完整之Linux-based無線區域網路入侵偵測系統，因此是非常適用於現行的系統環境中。

關鍵詞：入侵偵測系統(Intrusion Detection System)，分群演算法(Clustering Algorithm)，關聯法則(Association Rules)，情境法則(Episode Rules)，無線區域網路(WLAN)

目錄

參考文獻

一、中文部份 台灣電腦網路危機處理?協調中心，802.11無線網路安全白皮書[線上資料]，來源: http://www.cert.org.tw/. [2003, February]。 二、英文部分 Anderson, J. P. (1980). Computer security threat monitoring and sur-veillance. Technical Report Contract 79F26400, Fort Washington. Balazinska, M. & Castro, P. (2003). Characterizing mobility and net-work usage in a corporate wireless local-area network. In J. Pieprzyk & H. Ghodosi (Eds.), Proceedings of the 1st international conference on Mobile systems, applications and services, (pp. 303 – 316), New York: Springer-Verlag. Boudriga, N. & Obaidat, M. S. (2006). Mobility, sensing, and security management in wireless ad hoc sensor systems. Computers & Elec-trical Engineering, 32(1-3), 266-276. CERT/CC, Incidents reported[Online]. Available : http://www.cert.org/stats/ [2007, April 30] Chien, B. C., Lin, Z. L. & Hong, T. P. (2002). An efficient algorithm for clustering categorical data. Journal of Computer Science and Technology Archive, 17(5), 611-624. Daniels, T. & Spafford, E. H. (1999). Identification of host audit data to detect attacks on low-level IP vulnerabilities. Journal of Computer Security, 7(1), 3-35. Dobrowiecki, T. (2003). Episode Mining to Automatically Filter False Alarms. In N.H. Vaidya, M.S. Corson, & S.R. Das (Eds.), Proceedings of the 10th PhD Mini-Symposium on IEEE Hungary Section (pp. 44-45), Long Beach: IEEE. Feng, L., Guan, X., Guo, S., Gao, Y. & Liu, P. (2004). Prediction the intrusion intentions by observing system call sequences. Computers &

Security, 23(3), 241-252. Florez, G., Bridges, S. A. & Vaughn, R. B. (2002). An improved algo-rithm for fuzzy data mining for intrusion detection. In L. Xu & L. Korba (Eds.), Proceedings of the North American Fuzzy Information Processing Society Conference, (pp. 457-462) , New York: Springer-Verlag. Forrest, S. & Somayaji, A. (2000). Automated response using system-call delays. In S. Cui, P. Duan, & C.W. Chan (Eds.), Proceedings of the 9th Usenix Security Symposium, (pp. 185-197) , New York: Springer-Verlag. Forrrest, S. A., Hofmeyr, S., Somayaji, A. A. & Longstaff, T. A. (1996). A sense of self for unix process. In J. Forlizzi, J. Lee, & S. Hudson (Eds.), Proceedings of the IEEE Symposium on Security & Privacy (pp. 120-128), New York: IEEE. Guan, Y., Ghorbani, A. A. & Belacel, N. (2003). Y-means: A clustering method for intrusion detection. In D.T. Lee & B.S. Lin (Eds.), Proceedings of Canadian Conference on Electrical and Com-puter Engineering, (pp. 1-4), New Jersey: IEEE. Heady, R., Luger, G., Maccabe, A. & Servilla, M. (1990). The archi-tecture of a network level intrusion detection system. Technical report CS90-20, University of New Mexico: Department of Computer Sci-ence. Hirano, S., Sun, X. & Tsumoto, S. (2004). Comparison of clustering methods for clinical databases. Information Sciences, 159(3-4), 155-165. Hossain, M. (2002). Integrating association rule mining and decision tree learning for network intrusion detection: a preliminary investiga-tion. In I.F. Akyildiz, J.Y.B. Lin, & R. Jain (Eds.), Proceedings of the International Conference on Information Systems, Analysis and Syn-thesis, (pp. 65-70), New Orleans: IEEE. Jain, A. K., Murty, M. N. & Flynn, P. J. (1999). Data clustering: a re-view. ACM Computing Surveys, 31(3), 264-323. Jha, S. & Hassan, M. (2002). Building agents for rule-based intrusion detection system. Computer Communications, 25(15), 1366-1373. Jiang, M. F., Tseng, S. S. & Su, C. M. (2001). Two-phase clustering process for outliers detection. Pattern Recognition Letters, 22(6-7), 351-382. Khoshgoftaar, T.M., Nath, S.V., Zhong, S. & Seliya, N. (2005). A clus-tering approach to wireless network intrusion detection. In J. Crow-croft (Ed.), Proceedings of International Conference on Tools with Ar-tificial Intelligence, (pp. 190-196), London: ACM. Lee, W., Stolfo, S. J. & Mok, K. W. (1999). A data mining framework for building intrusion detection models. In P. Druschel & M.F. Kaashoek (Eds.), Proceedings of the 1999 IEEE Symposium on Secu-rity and Privacy, (pp. 120-132), New York: IEEE. Leu, F. Y. & Yang, T. Y. (2003). A host-based real-time intrusion de-tection system with data miningand forensic techniques. In D.B. John-son & Z. Haas (Eds.), Proceedings of the 37th IEEE Annual Interna-tional Carnahan Conference on Security Technology, (pp. 580-586), New York: IEEE. Liu, Y., Chen, K., Liao, X. & Zhang, W. (2004). A genetic clustering method for intrusion detection. Pattern Recognition, 37(5), 927-942. Luo, J. & Bridges, S. M. (2000). Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection. International Jour-nal of Intelligent Systems, 15(8), 687-703. Luo, J., Bridges, S. & Vaugham, R. B. (2001). Fuzzy frequent epi-sodes for real-time intrusion detection. In D. Maughan & N.H. Vaidya (Eds.), Proceddings of IEEE International Conference on Fuzzy Sys-tems, (pp. 368-371), Atlanta: IEEE. Mannila, H., Toivonen, H. & Verkamo, A.I. (1997). Discovery of fre-quent episodes in event sequences. Data Mining and Knowledge Dis-covery, 1(3), 1-47. Maxion, R. A. (2003). Masquerade detection using enriched command lines. In J. Vitter (Eds.), Proceedings of International Conference on Dependable Systems and Networks, (pp. 5-14), Dallas: ACM. Oh, S. J. & Kim, J. Y. (2004). A hierarchical clustering algorithm for categorical sequence data. Information Processing Letters, 91(3), 135-140. Qin, M. & Hwang, K. (2004). Frequent Episode Rules for Internet Anomaly Detection. In D. Naccache (Eds.), Proceedings of the Third IEEE International Symposium on Network Computing and Applica-tions, (pp.161-168), New York: IEEE. Sobh, T. S. (2006). Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces, 28(6), 670-694. Spitizner, L. (2003). The honeynet project: trapping the hackers. IEEE Security & Privacy, 1(2), 15-23. Stearley, J. (2004). Towards informatic analysis of syslogs. In H. Krawczyk (Eds.), Proceedings of the IEEE International Conference on Cluster Computing, (pp. 309-318), San Francisco: IEEE. Tsaur, W. J. & Shieh, Y. C. (2003). Constructing fuzzy association rules for intrusion detection systems. In N. Koblitz (Eds.), Proceed-ings of the 2003 National Computer Symposium, (pp. 1256-1263), New York: Springer-Verlag.