植基於連線分析之入侵警訊關聯機制

蕭克勤、曹偉駿

E-mail: 9511208@mail.dyu.edu.tw

摘 要

網際網路的導入，不僅增加了資訊的價值，但也使得企業組織與普羅大眾在享受其便利時， 必須更注重安全的議題。我們會使用防火牆、防毒軟體以及入侵偵測系統，以確保網路環境的安 全性。然而隨著網路流量的增加，經由入侵偵測系統產生的警訊也隨之暴增。面對這麼大量的警 訊，要如何瞭解、管理與採取適 當的對策，實在不是一件容易的事。 本研究提出了一個基於使用者行為之入侵警訊關聯方法，藉由改良過的相似度函數處理警訊，使得網管人員可以得到更有意義的資訊。因此可以更容易地分析入侵警訊，並降低管理上的負 擔。此外，本論文亦開發出實際系統，以驗證系統遭受攻擊時，的確可以提供更具關聯性的警訊，以供管理者進行分析與瞭解。

關鍵詞 : 入侵偵測系統 ; 網路安全 ; 警訊分析 ; 關聯

目錄

參考文獻

1.陳培德、賴溪松 (2002)。 入侵偵測系統簡介與實現。資訊安全通訊，8(2)，21-37。 2.Anderson, J. P. (1980). Computer security threat monitoring and surveillance. 3.Bace, R. G. (1999). Intrusion Detection: Sams Publishing. 4.Biermanna, E., Cloeteb, E., & Venterc, L. M. (2001). A comparison of Intrusion Detection systems. Computers & Security, 20(8), 676-683. 5.BLADE Software IDS Informer. from http://www.bladesoftware.net/prod_ids.html 6.Botha, M., & Solms, R. v. (2003). Utilising fuzzy logic and trend analysis for effective intrusion detection. Computers & Security, 22(5), 423-434. 7.Burbeck, K. (2005). Current research and use of anomaly detection. The 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise. 8.CERT/CC. (2006). CERT/CC Statistics 1988-2006. from http://www.cert.org/stats/ 9.Cuppens, F. (2001a). Cooperative intrusion detection. Proceeding of International Sysmposium on Information superiority: tools for crisis and conflict-management. 10.Cuppens, F. (2001b). Managing alerts in a multi intrusion detection environment. Proceeding of 17th Annual Computer Security Applications Conference. 11.Cuppens, F., Autrel, F., Miege, A., & Benferhat, S. (2002). Correlation in an intrusion detection process. Procedeeing of Internet Security Communication Worksho. 12.Denning, D. (1987). An intrusion Detection Model. IEEE Transactions on Software Engineering, 13(2), 222-232. 13.Forte, D. V. (2004). The “ Art ” of log correlation: Tools and Techniques for Correlating Events and Log Files. Computer Fraud & Security, 2004(8), 15-18. 14.Graham, R. (2001). FAQ: Network Intrusion Detection Systems. 15.Hypersonic SQL Group. from http://www.hsqldb.org/ 16.IP-to-Country.com. from http://ip-to-country.webhosting.info/ 17.IPCop Firewall. from http://www.ipcop.org/ 18.Koziol, J. (2004). Intrusion Detection with Snort: Sams Publishing. 19.Lee, S., Chung, B., Kim, H., Lee, Y., Park, C., & Yoon, H. (2006). Real-time analysis of intrusion detection alerts via correlation. Computers & Security, 25(3), 169-183. 20.Metasploit Project. from http://www.metasploit.com/ 21.Nmap. from http://www.insecure.org/nmap/ 22.Northcutt, S., & Novak, J. (2003). Network Intrusion Detection (3 ed.): Sams Publishing. 23.p0f. from http://lcamtuf.coredump.cx/p0f.shtml 24.Perdisci, R., Giacinto, G., & Roli, F. (2006). Alarm clustering for intrusion detection systems in computer networks. Engineering Applications of Artificial Intelligence, 19(4), 429-438. 25.Perrochon, L., Jang, E., Kasriel, S., & Luckham, D. C. (2000). Enlisting event patterns for cyber battlefield awareness. DARPA Information Survivability Conference & Exposition. 26.Snort Offical Website. from http://www.snort.org/ 27.Subhadrabandhu, D., Sarkar, S., & Anjum, F. (2004). Efficacy of misuse detection in ad hoc networks. IEEE International Conference on Sensor and Ad hoc Communications and Networks. 28.Thottanand, M., & Ji, C. (2003). Anomaly detection in IP networks. IEEE Transactions on Signal Processing, 51(8), 2191-2204. 29.Valdes, A., & Skinner, K. (2001). Probabilistic Alert Correlation.

Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection. 30.Yu, D., & Frincke, D. (2006). Improving the quality of alerts and predicting intruder's next goal with Hidden Colored Petri-Net. Computer Networks, Accepted.