基於誘捕技術之無線區域網路入侵偵測機制研究

許仲穎、曹偉駿

E-mail: 9708167@mail.dyu.edu.tw

摘 要

現行無線區域網路(Wireless Local Area Networks, WLAN)的確是帶給使用者許多的便利性，如：建置容易、設定簡單等。也因此人們已經對這些技術產生了很大的依賴性，但無線區域網路在安全性上卻遠比傳統有線的環境需要更多的考量，由於無線網路是透過空氣當介質傳遞，因此使用者在傳輸資料時，很容易被駭客所竊取。現今的技術大多是利用入侵偵測系統(Intrusion De-tection System, IDS)作為防禦入侵的方法，但現行的入侵偵測系統都有兩大缺失：(1)只能偵測已知型的攻擊;(2)經常發生無效的偵測。本研究提出並測試各種不同無線誘捕系統(Wireless Honeypot)的架構，包括低互動、高互動、混合式等，以提出具高誘捕率之架構，同時也利用資料收集模組，以Honeyd偽冒成無線基地台，詳盡的收集、擷取入侵者的惡意行為，並再以資料分析模組完整的分析所有可能的入侵行為，降低入侵偵測的誤判率且做更精確的入侵行為研判。此外，本系統產生的報表則能提供管理者在日後做為更新系統依據。最後本研究亦製作Linux Live CD供系統管理者能快速建置此無線誘捕系統。

關鍵詞 : 網路安全 ; 無線區域網路 ; 無線誘捕系統

目錄

中文摘要 . . . . . iii 英文摘要 . . . . . iv 誌謝辭 . . . . . v 內容目錄 . . . . . vi 表目錄 . . . . . viii 圖目錄 . . . . . ix 第一章 緒論. . . . . 1 第一節 研究背景. . . . . 1 第二節 研究動機與目的. . . . . 1 第三節 研究流程. . . . . 3 第四節 論文架構. . . . . 5 第二章 文獻探討. . . . . 6 第一節 現行無線區域網路安全議題. . . . . 6 第二節 入侵偵測系統探討. . . . . 10 第三節 誘捕系統技術. . . . . 13 第三章 高偵測率之無線入侵偵測機制. . . . . 19 第一節 建置無線誘捕系統系統. . . . . 20 第二節 資料分析模組. . . . . 22 第三節 系統測試階段. . . . . 26 第四章 系統建置與測試. . . . . 28 第一節 實驗環境. . . . . 28 第二節 實驗流程說明. . . . . 30 第三節 系統測試結果. . . . . 34 第四節 實驗結果分析. . . . . 36 第五章 結論與未來發展方向. . . . . 41 第一節 結論. . . . . 41 第二節 未來發展方向. . . . . 42 參考文獻 43

參考文獻

Artail, H., Safa, H., Sraj, M., Kuwatly, I., & Al-Masri, Z. (2006). A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks. Computers & Security 25(4), 274-288. Badra, M., Urien, P., & Hajjeh, I. (2007). Flexible and fast security solution for wireless lan. Ervasive and Mobile Computing 3(1), 1-14. Beheshti, M., & Wasniowski, R. (2007). Data fusion support for intrusion detection and prevention. Proceedings of the International Conference on Information Technology (p966). Beyah, R., Corbett, C., & Copeland, J. (2006). The case for collaborative distributed wireless intrusion detection systems. Proceedings of the IEEE International Conference on Granular Computing (pp. 782-787). USA: Atlanta. Chuvakin, A. (2003). Honeynets: high value security data analysis of real attacks launched at a honeypot. Network Security 2003(8), 11-15. Fake AP Project, Available: http://www.blackalchemy.to/project/fakeap/ [2008, June 23]. Hilley, S. (2002). At last, a wireless honeypot. Proceedings of the Incorporating E-Commerce, Internet and Telecommunications Security, (pp. 1-2). Honeynet, Available: http://project.honeynet.org/ [2008, June 23]. Iheagwara, C., Blyth, A., Bennett, M. (2005). Architectural and functional issues in systems requirements specifications for wireless intrusion detection systems implementation. Proceedings of the 2005 Systems Communications (pp. 434-441). Canada: Montreal. Jiang, X., Xu, D., & Wang, Y. (2006). Collapsar: a vm-based honeyfarm and reverse honeyfarm architecture for network attack capture and detention. Journal of Parallel and Distributed Computing 66(9), 1165-1180. Kim, D., Koh, S., & Kim, S. (2006). An integrated scheme for intrusion detection in wlan. Proceedings of the International Conference on Information Networking, Advances in Data Communications and Wireless Networks (pp. 723-732). Japan: Sendai. Kreibich, C., Crowcroft, J. (2004). Honeycomb - creating intrusion detection signatures using honeypot. ACM SIGCOMM Computer Communication Review 34(1), 51-56. Lei, J., Fu, X., Hogrefe, D., & Tan, J.

(2007). Comparative studies on authentication and key exchange methods for 802.11 wireless lan. Computers & Security 26(5), 401-409. Lim, Y., Schmoyer, Y., Levine, J., & Owen, H. (2003). Wireless intrusion detection and response. Proceedings of the IEEE Workshop on Information Assurance (pp. 68-75). USA: New York. Nessus, Available: http://www.nessus.org/nessus/ [2008, June 23]. Netstumbler, Available: http://www.netstumbler.com/ [2008, June 23]. Ning, P., Cui, Y., Reeves, D., & Xu, D. (2004). Tools and techniques for analyzing intrusion alerts. ACM Transactions on Information and System Security 7(2), 273-318. NMAP, Available: http://nmap.org/ [2008, June 23]. Ouyang, Y. C., Chang, R. L., & Chiu, J. H. (2003). A new security key exchange channel for 802.11 wlans. Proceedings of the 37th Annual International Carnahan Conference on Security Technology (pp. 216-225). Taiwan: Taipei. Portokalidis, G., & Bos, H. (2007). SweetBait: zero-hour worm detection and containment using low and high-interaction honeypots. Computer Networks 51(5), 1256-1274. Potter, B. (2004). Wireless intrusion detection. Network Security 2004(4), 4-5. R. Siles. (2007). HoneySpot: the wireless honeypot. Spanish Honeynet Project. Samer, F., Salim. H., Youssif, A., (2007) Anomaly-based behavior analysis of wireless network security. Proceedings of the Mobile and Ubiquitous Systems: Networking & Services (pp. 1-8). USA: Philadelphia. Sobh, T. (2006). Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces 28(6), 670-694. Sorman, M., Kovac, T., & Maurovic, D. (2004) Implementing improved wlan security. Proceedings of the 46th International Symposium Electronics (pp. 229-234). Croatia: Zadar. Spitzner, L. Honeypots : definitions and value of honeypots. Available: http://www.tracking-hackers.com/papers/honeypots.html [2008, June 23]. Tang, Y., Hu, H., Lu, X., & Wang, J. (2006). HonIDS: enhancing honeypot system with intrusion detection models. Proceedings of the Fourth IEEE International Workshop on Information Assurance (pp. 135-143). UK: Royal Holloway. Thakar, U., Varma, S., & Ramani, A. (2005). HoneyAnalyzer analysis and extraction of intrusion detection patterns & signatures using honeypot. Proceedings of the the Second International Conference on Innovations in Information Technology. UAE: Dubai. Tsakountakis, A., Kambourakis, G., & Gritzalis, S. (2007). Towards effective wireless intrusion detection in ieee 802.11i. Proceedings of the Third International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing (pp. 37-42). Turkey: Istanbul. Viecco, C. (2007). Improving honeynet data analysis. Proceedings of the IEEE Workshop on Information Assurance and Security (pp. 30-37). USE: New York. Wall, D., Kanclirz, Jr., Jing, Y., Faircloth J., & Barrett, J. (2004). Managing and securing a cisco swan, SYNGRESS. Wang, S., Tao, R., Wang, Y., & Zhang, J. (2003). WLAN and It's security problems. Proceedings of the Fourth International Conference on Parallel and Distributed Computing (pp. 241-244). China: Chengdu. Yek, S. (2003). Measuring the effectiveness of deception in a wireless honeypot. Proceedings of the 1st Australian Computer, Network & Information Forensics Conference. Australia: Perth. Yek, S. (2004). Implementing network defence using deception in a wireless honeypot. Proceedings of the 2nd Australian Computer, Network & Information Forensics Conference, (pp. 4-15). Australia: Perth.