A Study on Intrusion Detection System in WLAN Using Honeypot Techniques

許仲穎、曹偉駿

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

ABSTRACT

With the popularity of WLAN (Wireless Local Area Networks) they provide users with a lot of convenience such as ease of integration and setup. These properties make people rely on WLAN. But the security of WLAN needs more considerations than traditional networks, because of WLAN transmission is easy to be intercepted by hackers. The common method of defending WLAN is to use an intrusion detection system, but in such a way there are two defects: (1) it is unable to detect unknown attacks; (2) its false positive is too high. This study constructs and then tests several wireless honeypot, including the modes of low-interaction, high-interaction and hybrid. We also develop a data analysis module to analyze all possible intrusions completely, and use the honeyd tool to act fake AP to capture the malicious behavior of intruders, in order to reduce the false alert rate. Besides, the proposed system can generate reports for reference to administrators. Fi-nally, we develop a Linux Live CD for constructing the wireless honeypot quickly.

Keywords : Network Security ; Wireless Local Area Networks ; Wireless Honeypot

Table of Contents

REFERENCES

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.