A Study on Detecting Metamorphic Rootkits Based on Tripwire Tool

林明孝、曹偉駿

E-mail: 9510752@mail.dyu.edu.tw

ABSTRACT

With the rapid development and prevalence of Internet, more and more hackers rampant on the cyberspace invent out much more diverse and complex intrusion techniques. According to the bugs or defects of Linux and Windows operating systems, hackers can develop a great diversity of malicious software such as virus, worm, Trojan horse, backdoor, and rootkit. How to maintain a secure computing platform and avoid intrusion from hackers becomes a very crucial issue nowadays. Most host-based intrusion detection systems (HIDS) find out attacking evidences by filtering or auditing the operating system logs. However, hackers can place rootkits to get the root access right or leave backdoors, which let hackers intrude the system and change the system programs again. In such a way, administrators usually have little clue to detect it out. Consequently, this thesis focuses on the Linux system administrator ‘ s point of view to check out if the operating system has been placed a user mode rootkit. The proposed detecting mechanism is to employ the Chkrootkit tool to detect out the known rootkits, and then in terms of its intrusion characteristics, examine the integrity of system files by the Tripwire tool. From the database, we can first find out the abnormal items caused by the metamorphic rootkits, and then compare with the previously gained abnormal items generated by the known rootkits to find out metamorphic rootkits. Finally we also simulate the proposed detecting scheme to validate its feasibity.

Keywords : Malicious Software ; Intrusion Detection System ; Rootkit ; Linux

Table of Contents

REFERENCES

Abraham, A., Grosan C., & Chen, Y. (2005). Cyber Security and the Evolution of Intrusion Detection Systems. Retrieved March 28, 2006, from http://www.cs.ubbcluj.ro/~cgrosan/kerala.pdf. Andreas, B. (2004). UNIX and Linux based Rootkits Techniques and Countermeasures. Retrieved May 10, 2006, from https://www.dfn-cert.de/team/bunten/rootkits_first2004.pdf. F-SECURE (2006). F-Secure BlackLight. Retrieved April 25, 2006, from http://www.f-secure.com/blacklight. Butler, J., & Hoglund, G. (2005). VICE-Catch the hookers. Retrieved March 22, 2005, from http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-butler/bh-us-04-butler.pdf. Butler, J., Undercoffer, J. L., & Pinkston, J. (2003). HIDDEN PROCESS:The Implication for Intrusion Detection. Proceedings of the 2003 IEEE Workshop on Information Assurance.(pp. 116-121). Chkrootkit(2005). Locally checks for signs of a rootkit. Retrieved December 5, 2005, from http://www.chkrootkit.org. CERT/CC Statistics (1988-2006). Retrieved May 19, 2006, from http://www.cert.org/stats/cert_stats.html. Cohen, F.(1987). Computer viruses-theory and

experiments. Computers & Security, 6(1), 22-35. Chen, S., & Ranka, S. (2005). Detecting Internet Worms at Early Stage. IEEE Journal on Selected Areas in Communications, 23(10), 2003-2012. Chebrolu, S., Abraham A., & Thomas, J. (2005). Feature Deduction and Ensemble Design of Intrusion Detection Systems. Computers & Security, 24(4), 295-307. Daniels, T., & Spafford, E. H. (1999). Identification of Host Audit Data to Detect Attacks on Low-level IP Vulnerabilities. ACM Journal of Computer Security, 7(1), 3-35. DeMara, R. F., & Rocke, A. J. (2004). Mitigation of network tampering using dynamic dispatch of mobile agents. Computers & Security, 23(1), 31-42. Feng, Li., Guan, X., Guo, S., Gao, Y., & Liu, P. (2004). Prediction the intrusion intentions by observing system call sequences. Computers and Security, 23(3), 241-252. F-SECURE (2006). F-Secure. Retrieved May 15, 2006, from http://www.f-secure.com/. Forrrest, S., Hofmeyr, A. S. A., Somayaji, A., & Longstaff, T. A. (1996). A Sense of Self for Unix Process. IEEE Symposium on Security & Privacy, 120-128. Felten, E. W., & Halderman, J. A. (2006). Digital Rights Management, Spyware, and Security. IEEE Security & Privacy, 4(1), 18-23. Hawkins, S. (2002). Understanding the Attackers Toolkit. Retrieved May 25, 2006, from http://www.giac.org/practical/gsec/Sunnie_Hawkins_GSEC.pdf. Jha, S., & Hassan, M. (2002). Building Agents for rule-based intrusion detection system. Computer Communications, 25(15), 1366-1373. Kim, G. H. & Spafford, E. H. (1994). The Design and Implementation of Tripwire: A File System Integrity Checker. Proceedings of the 2nd ACM Conference on Computer and Communications Security. (pp.18-29). Kuhnhauser, W. E. (2004). Root kits: An operating systems viewpoint. ACM SIGOPS Operating Systems Review, 38(1), 12-23. King, S. T. & Chen, P. M. (2005). Backtracking Intrusions. ACM Transactions on Computer Systems(TOCS), 23(1), 51-76. Kim, G. H. & Spafford, E. H. (1994). Experiences with Tripwire:Using Integrity Checkers for Intrusion Detection. Proceeding of 2nd ACM Conference on Computer and Communications Security. Kruegel, C., Robertson, W., & Vigna, G. (2004). Detection Kernel-Level Rootkits Through Binary Analysis. Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC). Lee, W., Fan, W., Miller, M., Stolfo, S., & Zadok, E. (2002). Toward Cost-Sensitive Modeling for Intrusion Detection and Response. Journal of Computer Security, 10(1-2), 5-22. Leu, F. Y. & Yang, T. Y. (2003). A Host-based Real-Time Intrusion Detection System with Data Mining and Forensic Techniques. Proceedings of the 37th IEEE Annual International Carnahan Conference on Security Technology, (pp. 580-586). Levine, J., Culver, B., & Owen, H. (2003). A Methodology for Detecting New Binary Rootkit Exploits. Proceedings IEEE SouthEastC on 2003. Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., Weber, D., Webster, S. E., Wyschogrod, D., Cunningham, R. K., & Zissman, M. A. (2000). Evaluating Intrusion Detection System: the 1998 DARPA Off-Line Intrusion Detection Evaluation. Proceedings of the 2000 DARPA Information Survivability Conference and Exposition. Maxion, R. A. (2003). Masquerade Detection Using Enriched Command Lines. Proceedings of International Conference on Dependable Systems and Networks, (pp. 5-14). Mao J., & Jain, A. (1996). A Self-Organizing Network for HyperEllipsoidal Clustering. IEEE Transactions on Neural Networks, 7(1), 16-29. CSI/FBI. (2006). New FBI Computer Crime Survey. Retrieved April 19, 2006, from http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm, 2006. Nachenberg, C. (1999). Computer Parasitology. Proceedings of the Ninth International Virus Bulletin Conference. Oh S. J., & Kim, J.Y. (2004). A Hierarchical Clustering Algorithm for Categorical Sequence Data. Information Processing Letters, 91(3), 135-140. Petroni, N., Fraser, T., Molina, J., & Arbaugh, W. (2004). Copilot-a Coprocessor-based Kernel Runtime Integrity Monitor. Proceedings of the Usenix Security Symposium. Rootkit Revealer. Retrieved May 27, 2006, from http://www.sysinternals.com/Files/RootkitRevealer.zip. Red database security. http://www.red-database-security.com/. Rkhunter. Retrieved February 20, 2006, from http://www.rootkit.nl/. Rootcheck. Retrieved February 22, 2006, from http://www.ossec.net/en/rootcheck.html. Rutkowska, J. (2005). Thoughts about Cross-View based Rootkit Detection. Retrieved May 10, 2006, from http://www.invisiblethings.org/papers/ crossview_detection_thoughts.pdf. Somayaji, A., & Forrest, S. (2000). Automated Response Using System-Call Delays. Proceedings of the 9th Usenix Security Symposium. (pp. 185-197). Stearley, J. (2004). Towards Informatic Analysis of Syslogs. Proceedings of the IEEE International Conference on Cluster Computing. (pp. 309-318). Security Focus. Retrieved May 21, 2006, from http://www.securityfocus.com/infocus/1854. Symantec Caught in Norton ‘ Rootkit ’ Flap. Retrieved June 12, 2006, from http://www.eweek.com/article2/0,1895,1910077,00.asp. Sysinternals Freeware. Retrieved June 18, 2006, from http://www.sysinternals.com/. Spaffod, E. H.(1991). The Internet Worm Incident. Technical Report. Thimbleby, H., Anderson, S., & Cairns, P. (1998). A framework for Modelling trojans and computer virus infection. Computer Journal, 41(7), 444-458. Tripwire. Retrieved March 17, 2006, from http://www.tripwire.com. Tripwire Security Inc. Retrieved June 22, 2006, from http://www.tripwiresecurity.com. TRENDMICRO. Retrieved May 9, 2006, from http://www.trendmicro.com/la/home/enterprise.htm. Wang, Y. M., Beck, D., Vo, B., Roussev, R., Verbowski, C. (2005). Detecting Stealth Software with Strider GhostBuster. Proceedings of the 2005 International Conference on Dependable Systems and Networks. (pp. 368-377). Zovi, D. D. (2004). Kernel Rootkits. Retrieved May 14, 2006, from http://www.sans.org/rr/papers/60/449.pdf, 2004.