

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., Wyszogrod, 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.