References

[1] R.P. Lippmann, et al., "Evaluating Intrusion Detection Systems: The 1998 DARPA off-line Intrusion Detection Evaluation," In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, May 1998.

[2] R. Lippmann, J. Haines, D. Fried, J. Korba, and K. Das, "The 1999 DARPA Off-Line Intrusion Detection Evaluation," In *Proceedings of the Symposium on Recent Advances in Intrusion Detection (RAID)*, Toulouse, France, October 2000.

[3] S. Northcutt, J. Novak, and D. McLachlan, *Network Intrusion Detection: An Anlyst's Handbook*, 2nd ed. Indianapolis, Indiana, New Riders Publishing, 2000.

[4] M. D. Schiffman, *Building Open Source Network Security Tools: Components and Techniques*, Indianapolis, Indiana, Wiley Publishing Inc., 2003.

[5] R. Alder, J. Babbin, A, Doxtater, J.C. Foster, T. Kohlenberg and M. Rash, *Snort 2.1: Intrusion Detection*, 2nd ed. Rockland, MA, Symgress Publishing, Inc., 2004.

[6] K.K. Frederick, "Evaluating Network Intrusion Detection signatures, Part One, Two, Three," [Online]. Available: http://www.securityfocus.com/print/infocus/1623, 1630, 1651. [Accessed: January 05, 2007].

[7] J. Zhou, A.J. Carlson, and M. Bishop, "Verify results of network intrusion alerts using lightweight protocol analysis," in *Proceedings of the 21st Annual Computer Security Applications Conference*, 2005.

[8] R. Sommer, and V. Paxon, "Enhancing Byte-Level Network Intrusion Detection Signatures with Context," in *Computer and Communications Security conference*, Washington, DC, USA, October 2003.

[9] S. Lodin, "Intrusion Detection Product Evaluation Criteria," Ernst & Young LLP, October 1998.

[10] M. Smith, S. Durkin and K. Tan, "A Design for Building an IPS using open source products," SANS Institute, 2006.

[11] L. Wang, "NITS: Network Infrastructure Testing Suite," The University of Memphis, 2006.

[12] N.J. Puketza, K. Zhang, M. Chung, B. mukherjee and R.A. Olsson, “A Methodology for Testing Intrusion Detection Systems,” IEEE Transactions on Software Engineering, vol. 22, pp. 719-729, October 1996.

[13] M. Tvenge, “Using benchmarking to improve IDS configurations,” M.Sc. thesis, NISlab, Gjøvik University College, Høgskolen i Gjøvik, 2004

[14] T.H. Ptacek, T.M. Newsham, “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection,” Secure Networks, Inc., January 1998.

[15] N. Athanasiades, R. Abler, J. Levine, H. Owen, and G. Riley, “Intrusion Detection Testing and Benchmarking Methodologies,” in *Proceedings of the First International Workshop on Information Assurance*, 2003.

[16] F. Massicotte, F. Gagnon and Y. Labiche, “Automatic Evaluation of Intrusion Detection Systems,” in *Proc. Annual Computer Security Applications Conference*, 2006.

[17] R. Marty, “THOR: A Tool to Test Intrusion Detection Systems by Variation of Attacks,” Diploma Thesis, Swiss Federal Institute of Technology, Zurich, March 2002.

[18] “IDS Evaluation,” [Online]. Available: http://www.blackknife.com/Archive/Deaddrop/Papers/IDSeval.html. [Accessed: February 03, 2007].

[19] “Evaluating Intrusion Detection Systems,” [Online]. Available: http://www.cs.ucsb.edu/~kemm/courses/CS595/TestingIDSs/. [Accessed: April 18, 2007].

[20] “Snort - the de facto standard for intrusion detection-prevention,” [Online]. Available: http://www.snort.org.

[21] “Intrusion Detection Solutions from Internet Security Systems,” [Online]. Available: http://www.iss.net/products/product_sections/Intrusion_Detection_.html.

[22] “Shoki,” [Online]. Available: http://shoki.sourceforge.net/.

[23] “Bro Intrusion Detection System - Bro Overview,” [Online]. Available: http://www.bro-ids.org].

[24] “SANS Institute – Network, Security, Computer, Audit Information and Training,” [Online]. Available: www2.sans.org. [Accessed: October 28, 2007].

[25] “Neohapsis OSEC,” [Online]. Available: http://osec.neohapsis.com.

[26] "ISECOM - Making Sense of Security," [Online]. Available: http://www.isecom.org.

[27] S. Staniford-Chen, "Common Intrusion Detection Framework," [Online]. Available: http://gost.isi.edu /cidf/. [Accessed: July 20, 2007].

[28] "Welcome to the Home of OSSEC," [Online]. Available: http://www.ossec.net/. [Accessed: September 29, 2007].

[29] "CVE – Common Vulnerabilities and Exposures (CVE)," [Online]. Available: http://cve.mitre.org/. [Accessed: October 10, 2007].

[30] "SecurityFocus," [Online]. Available: http://www.securityfocus.com/. [Accessed: October 26, 2007].

[31] "OSVDB: The Open Source Vulnerability Database," [Online]. Available: http://osvdb.org/. [Accessed: September 20, 2007].

[32] "Tenable Network Security," [Online]. Available: http://www.nessus.org/. [Accessed: October 28, 2007].