

BIBLIOGRAPHY AND CITATION

- [1] Mehیار Dabbagh .Ali J.Ghandour.Kassem Fawaz.Wassim El Hajj.Hazem Hajj: Slow Port Scanning Detection, American University of Beirut, 2011 7th International Conference on Information Assurance and Security (IAS).
- [2] Roger Larsen: Slow Port Scanning with Bro, Gjøvik University College, 27/11/2013
- [3] Roger Christopher: Port Scanning Techniques and the Defense against THEM, SANS Institute InfoSec Reading Room 2002.
- [4] Monowar H Bhuyan.D K Bhattacharyya.and J K Kalita: Surveying Port Scans and Their Detection Methodologies, Oxford University Press Oxford, The Computer Journal Volume 54 Issue 10 October 2011.
- [5] Vinod Yegneswaran, Paul Barford and Johannes Ullrich: Internet Intrusions: Global Characteristics and Prevalence.
- [6] Marco de Vivo, Eddy Carrasco, Germinal Isern, Gabriela O. de Vivo: A Review of Port Scanning Techniques, LACORE U.C.V, April 1999.
- [7] **nmap**: www.nmap.org, 05 /04/2014.
- [8] Fyodor: The Art of Port Scanning, Phrack Magazine, Volume 7, Issue 51 September 01, article 11 of 17, 1997.
- [9] **nmap**:<http://nmap.org/book/man-port-scanning-techniques.html> ,10/04/2014.
- [10] hybrid@hotmail.com (1999) Distributed information gathering.Phrack Mag., Article 9, 9.
- [11] Heberlein, T., Dias, G., Levitt, K., Mukherjee, B., Wood, J., and Wolber, D. (1990) A network security monitor.Proceedings of RISP'90, Oakland, California,USA, May, 7-9, pp. 296–304. IEEE Computer Society
- [12] Fyodor (1997) The art of port scanning.Phrack Mag., Article 11, 7.
- [13] QoSient. Argus. <http://www.qosient.com/argus/>. Consulted on 9/6/2014
- [14] Staniford-Chen, S., Cheung, S., Crawford, R., Dilger,M., Frank, J., Hoagland, J., Levitt, K., Wee, C., Yip, R., and Zerkle, D. (1996) Grids: a graph based intrusion detection system

for large networks. Proceedings of 19th NISS'96, Baltimore, MD, USA, October, pp. 361–370. NIST.

[15] Leckie, C. and Kotagiri, R. (2002) A probabilistic approach to detecting network scans. Proceedings of NOMS'02, Florence, Italy, April, 15-19, pp. 359–372. IEEE Computer Society.

[16] Kim, H., Kim, S., Kouritzin, M. A., and Sun, W. (2004) Detecting network portscans through anomaly detection. Proc. SPIE 5429, Orlando, FL, USA, April, 12, pp. 254–263.

[17] Kato, N., Nitou, H., Ohta, K., Mansfield, G., and Nemoto, Y. (1999) A real-time intrusion detection system (ids) for large scale networks and its evaluations. IEICE Trans. Commun., E82-B, 1817–1825.

[18] Robertson, S., Siegel, E. V., Miller, M., and Stolfo, S. J. (2003) Surveillance detection in high bandwidth environments. Proceedings of DARPA DISCEX III'03, Washington, DC, April, 22-24, pp. 130–139. IEEE Computer Society.

[19] Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P.-N., Dokas, P., Kumar, V., and Srivastava, J. (2003) Detection of novel network attacks using data mining. Proceedings of ICDM WDMCS'03, Melbourne, Florida, USA, November, 19, pp. 30–39.

[20] Gates, C., McNutt, J. J., Kadane, J. B., and Kellner, M. (2006) Scan detection on very large networks using logistic regression modeling. Proceedings of ISCC'06, Pula-Cagliari, Sardinia, Italy, June, 26-29, pp. 402–408. IEEE Computer Society.

[21] Porras, P. and Valdes, A. (1998) live traffic analysis of TCP/IP gateways. Proceedings of ISOC NDSS'98, San Diego, California, March. ISOC Press.

[22] Porras, P. A. and Neumann, P. G. (1997) EMERALD: Event monitoring enabling responses to anomalous live disturbances. Proceeding of NCSC'97, Menlo Park, CA 94025, October, 22-25, pp. 353–365. NIST.

[23] Udhayan, J., Prabu, M. M., Krishnan, V. A., and Anitha, R. (2009) Reconnaissance scan detection heuristics to disrupt the pre-attack information gathering. Proceedings of N2S'09, Paris, France, June, 24-26, pp. 1–5. IEEE Computer Society.

[24] Roesch, M. (1999) Snort-lightweight intrusion detection for networks. Proceedings of LISA'99, Seattle, WA, USA, November, 7-12, pp. 229–238. USENIX Association.

- [25] Gyorgy, S. U., Gy?rgy, J. S., and Hui, X. (2005) Scan detection: A data mining approach. Proceedings of SIAM ICDM'05, Sutton Place Hotel, Newport Beach, CA, April, 21-23, pp. 118–129. SIAM.
- [26] Haan, G.-H. K. (2005) Detection of portscans using IP header data. Proceedings of TBRC'05, Enschede, January 21.
- [27] Rong-sheng, S., Xiao-yong, L., and Jian-hua, L. (2004) an adaptive algorithm to detect port scans. J. Shanghai Univ. (English Edit.), 8, 328–332.
- [28] Gates, C. (2006) Co-ordinated Port Scans: A Model, A Detector and An Evaluation Methodology. PhD thesis, Dalhousie University Halifax, Nova Scotia.
- [29] Jung, J., Paxson, V., Berger, A. W., and Balakrishnan, H. (2004) Fast portscan detection using sequential hypothesis testing. Proceedings of SECPRI'04, Oakland, CA, May, 9-12, pp. 211–225. IEEE Computer Society.
- [30] Paxson, V. (1998) Bro: A system for detecting network intruders in real-time. Proceedings of USENIX Security Symposium'98, San Antonio, Texas, January, 26-29, pp. 2435–2463. USENIX Association.
- [31] A. S. Tanenbaum, “Computer Networks, Fourth Edition”, 2003.
- [32]**Wikipedia:** [http://en.wikipedia.org/wiki/Java_\(programming_language\)](http://en.wikipedia.org/wiki/Java_(programming_language)) , 01/06/2014.
- [33]**Wikipedia:**<http://en.wikipedia.org/wiki/NetBeans>,02/06/2014.
- [34] **Winpcap:**<http://www.winpcap.org/> ,01/06/2014.
- [35] Mihai Dorobanțu, M.Sc., Mihai L. Mocanu, Ph.D: A Simple Way To Capture Network Traffic: The Windows Packet Capture (Winpcap) Architecture, Department of Software Engineering, School of Automation, Computers and Electronics, University of Craiova, 13 A.I. Cuza Str., 1100 Craiova, Romania.
- [36] **Sipinspector:** http://www.sipinspector.com/download/jpcap/JPCap_tutorial ,03/06/2014.