REFERENCIAS

[1] Anderson Neil, Della Maggiora Paul, Doherty Jim, "Cisco Networking Simplified", Segunda edición. Cisco Press. 2007.

[2] Argus – Auditing Network Activity http://www.qosient.com/argus/

[3] Argus practical botnet detection http://www.rawpacket.org/anonymous/papers/Argus-PracticalBotNetDetection.pdf

[4] Arnold Jon, Dwarshius Russell, Howell Paul, Jahanian Farnam, Malan Rob, Ogden Jeff, Poland Jon, Smart Matthew, University of Michigan, Merit-Research Paper, "Observations and Experiences Tracking Denial-Of-Service Attacks Across a Large Regional ISP", http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=97

[5] Bailey Michael, Cooke Evan, Jahanian Farnam, Nazario Jose, Watson David, University of Michigan, Arbor Networks ,"The Internet Motion Sensor: A Distributed Blackhole Monitoring System", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.4081&rep=rep1&type=pdf

[6] Bailey Michael, Cooke Evan, Jahanian Farnam, Nazario Jose, Watson David, University of Michigan, Arbor Networks , Research Paper, "Toward Understanding Distributed Blackhole Placement", Presented at The 2nd Workshop on Rapid Malcode (WORM), http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=107

[7] Bailey Michael, Cooke Evan, Jahanian Farnam, Watson David, Electrical Engineering and Computer Science Department, University of Michigan, Nazario Jose, Arbor Networks , "The Internet Motion Sensor: A distributed global scoped Internet threat monitoring system ", http://eecs.umich.edu/techreports/cse/04/CSE-TR-491-04.pdf

[8] Barford Paul, University of Wisconsin at Madison, "Toward Self-Directed Network Intrusion Detection and Prevention", Conferencia, http://www.csail.mit.edu/events/eventcalendar/calendar.php?show=event&id=871

[9] Binkley Jim (Portland State University), "Anomaly-based BotServer (and more!) Detection", http://cert.org/flocon/2006/presentations/botserver2006_ppt.pdf

[10] Bjarte Malmedal, Gjøvik University College, "Using Netflows for slow portscan detection", 2005, http://www.malmedal.net/Malmedal_Master_Thesis.pdf

[11] Bullard Carter, QoSient LLC, "Network Flow Data Fusion. GeoSpatial and NetSpatial Data Enhancement", FloCon 2010,

https://tools.netsa.cert.org/wiki/download/attachments/10027010/Bulla rd_DataFusion.pdf
[12] Chuvakin Anton blog, http://chuvakin.blogspot.com/
[13] Chuvakin Anton homepage, http://www.chuvakin.org/
[14] Gadsden Richard, "Mass-Mailing Worms: Prevention, Detection and Response (A Case Study)", SANS Institute InfoSec Reading Room, http://www.sans.org/reading_room/whitepapers/malicious/mass-mailing-worms-prevention-detection-response-a-case-study_1148
[15] Gartner Inc. "Gartner Information Security Hype Cycle Declares Intrusion Detection Systems a Market Failure" , http://gartner.com/5_about/press_releases/pr11june2003c.jsp
[16] Haile Jed, "Using Argus Audit Trails to Enhance IDS Analysis", Nitro Data, Systems, http://cansecwest.com/core03/jhaile-cansec03.ppt
[17] Honeynets, conoce a tu enemigo. Presentación en V Foro de seguridad RedIRIS Detección de Intrusiones. Abril de 2007, http://www.rediris.es/cert/doc/reuniones/fs2007/archivo/Honeynets_RaulSiles_VForoSeguridadRedIRIS_Abril2007.pdf
[18] Honeypots Definitions and Value of Honeypots, http://www.tracking-hackers.com/papers/honeypots.html
[19] Huffaker Bradley, Cooperative Association for Internet Data Analysis CAIDA, San Diego Supercomputer Center, University of California, San Diego. "CAIDA, Report 2010", http://caida.org/publications/presentations/2010/caida_update/
[20] Ido Dubrawsky, Wes Noonan,. "Firewalls fundamentals", Cisco Press, 2006.
[21] Insecure magazine Issue 4. Octubre 2005, http://www.net-security.org/dl/insecure/INSECURE-Mag-4.pdf
[22] Internet Background Noise (IBN), http://www.switch.ch/security/IBN/
[23] Internet Security Monitoring, Monitoring and coordination of intrusion detection, http://www.authorstream.com/Presentation/Wanderer-17376 -intrusion-detection-monitoring-Internet-Security-Current-Practice-Protecting-against-Intrusions-One-Promising-Approa-as-Entertainment-ppt-powerpoint
[24] Introduction to Intrusion Detection, http://ciscosecurity.org.ua/1587051672/ch10lev1sec1.html
[25] Kent Karen, Northcutt Stephen, Winters Scott, W. Ritchey Ronald, Zeltser Lenny, "Inside Network Perimeter Security", SAMS, 2005.
[26] Kippo Project http://code.google.com/p/kippo/

[27] Know Your Enemy: GenII Honeynets, http://old.honeynet.org/papers/gen2/index.html
[28] Know Your Enemy: Honeynets in Universities, http://old.honeynet.org/papers/edu
[29] Know Your Enemy: Honeynets, http://old.honeynet.org/papers/honeynet/
[30] Lee Rob, "SANS Computer Forensics and e-Discovery, Interview with Michael Cloppert", 2009, http://blogs.sans.org/computer-forensics/2009/03/04/michael-cloppert-computer-forensic-hero/
[31] Mason Andrew, "Cisco firewall Technology", Cisco Press, 2007.
[32] McPherson Danny, Arbor Networks; Tim Battles, AT&T; Bailey Michael, Cooke Evan, University of Michigan – Presentation, "Tracking Global Threats with the Internet Motion Sensor", http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=108
[33] McPherson Danny, Nazario Jose, Arbor Networks; Michael Bailey, University of Michigan - Presentation, "Measuring Global Worm Activity", Presentacion en NANOG 30, http://www.arbornetworks.com/index.php?option=com_docman&task=doc_download&gid=103
[34] McRee Russ, "Argus – Auditing network activity". 2007, http://holisticinfosec.org/toolsmith/docs/november2007.pdf
[35] McRee Russ, "Expanding Response: Deeper Analysis for Incident Handlers", SANS Institute InfoSec Reading Room. 2008.
[36] Moore David, Cooperative Association for Internet Data Analysis – CAIDA, San Diego Supercomputer Center, University of California, San Diego, "Detecting Internet Worms", http://www.caida.org/publications/presentations/2005/detecting_worms
[37] Moore David, Cooperative Association for Internet Data Analysis – CAIDA, San Diego Supercomputer Center, University of California, San Diego, "Network Telescopes", http://caida.org/publications/presentations/2003/dimacs0309/
[38] Moore David, Cooperative Association for Internet Data Analysis – CAIDA, San Diego Supercomputer Center, University of California, San Diego, "Network Telescopes: Observing Small or Distant Security Events", http://www.caida.org/publications/presentations/2002/usenix_sec

[39] Moore David, Cooperative Association for Internet Data Analysis – CAIDA, San Diego Supercomputer Center, Geoffrey M. Voelker, Stefan Savage, Department of Computer Science and Engineering, University of California, San Diego, "Network Telescopes: Technical Report", http://caida.org/publications/papers/2004/tr-2004-04/

[40] On the Design and Use of Internet Sinks for Network Abuse Monitoring, http://pages.cs.wisc.edu/~vinod/raid-paper.pdf

[41] Packet Capture library, http://www.tcpdump.org/pcap3_man.html

[42] Papoulis, A. "Bernoulli Trials." 3-2 in Probability, Random Variables, and Stochastic Processes, 2nd ed. New York: McGraw-Hill, pp. 57-63, 1984.

[43] Portal de herramientas de seguridad de Carnivore, http://carnivore.it

[44] Richard Bejtlick, "Implementing Network Security with Open Source Tools", http://sce.uhcl.edu/yang/teaching/csci5931webSecuritySpr04/8-21sSecurity-FINAL%20net%20security%20monitoring.pdf

[45] SANS – Internet Storm Center, "Survival time", http://isc.sans.edu/survivaltime.html

[46] SGUIL: The analyst console for network security monitoring, http://sguil.sourceforge.net/

[47] Shannon Colleen, Cooperative Association for Internet Data Analysis CAIDA, San Diego Supercomputer Center, University of California, San Diego, "CAIDA Activities", http://caida.org/publications/presentations/2007/terena_caida/

[48] Shannon Colleen, Moore David, Cooperative Association for Internet Data Analysis, CAIDA, San Diego Supercomputer Center, University of California, San Diego , "Security Data Collection at CAIDA",http://www.caida.org/publications/presentations/2004/security_collection_wide/

[49] Shannon Colleen, Moore David, Cooperative Association for Internet Data Analysis, CAIDA, San Diego Supercomputer Center, University of California, San Diego, "Network Telescopes: Remote Monitoring of Internet Worms and Denial-of-Service Attacks", http://www.caida.org/publications/presentations/2004/network_telescopes/

[50] Sourcefire Vulnerability Researh Team, http://www.snort.org/snort-rules/

[51] Spenneberg Ralf, “Keeping an eye on the network with Argus WATCHFUL EYE”, Linux Magazine. Febrero 2007, http://www.linux-magazine.com/w3/issue/75/Argus.pdf

[52] Splunk IT Search for Log Management, Operations, security compliance, http://www.splunk.com/

[53] Team Cymru, The Darknet Project http://www.team-cymru.org/Services/Darknets.html

[54] The Cooperative Association for Internet Data Analysis, http://www.caida.org/research/security/

[55] The IUCC/IDC Internet Telescope, http://noc.ilan.net.il/research/telescope/

[56] The Shadowserver Foundation, http://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Organizations

[57] Thomas Joshua, Conley Thomas, Ohio University, Internet Traffic Analysis for Threat Detection. Midwest Regional Conferences, 2005, http://www.educause.edu/Resources/InternetTrafficAnalysisforThre/159269

[58] Trost Ryan, “Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century”, Addison-Wesley Professional, 2009.

[59] UCSD Network telescope, http://www.caida.org/data/passive/network_telescope.xml

[60] Van Epp Peter (Simon Fraser University), “Using archived argus flow records to secure and troubleshoot your network”, http://www.internet2.edu/presentations/jtvancouver/20050720-Argus-VanEpp.pdf

[61] Vinod Yegneswaran, University of Wisconsin, “Empirical Foundations for Network Defense”, Conferencia, http://www.cs.pitt.edu/events/talks/06-2/vinod-yegneswaran.01mar2006.php