fs2007
V Foro de Seguridad RedIRIS

BIBLIOGRAFÍA

Detección de Intrusos desde el interior y a vista de pájaro

Carlos Fragoso, CESCA / JSS

En la Web

"Security Event Manager", Wikipedia
- URL: *http://en.wikipedia.org/wiki/Security_Event_Manager*

"Host-based Intrusion Detection System", Wikipedia
- URL: *http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system*

"Herramientas HIDS", JSS
- URL: *http://www.jessland.net/JISK/IDS_IPS/*

"Logging News and Information", Loganalysis.org
- *URL: http://www.loganalysis.org*

"Top 5 Intrusion Detection Systems", Insecure.org
- *URL: http://sectools.org/ids.html*

"Central Loghost Mini-HOWTO", Nate Campi
- *URL: http://www.campin.net/newlogcheck.html*

"Magic Quadrant for Security Information and Event Management", Nate Campi
- *URL: http://mediaproducts.gartner.com/reprints/computerassociates/139431.html*

Guías de implementación y estándares

"CCN-STIC Seguridad Perimetral: Detección de Intrusos", Centro Criptológico Nacional (CCN)
- URL: *http://www.cert.ccn.cni.es*

"SP800-92: Guide to Computer Security Log Management", National Institute of Standards and Technology (NIST)
- URL: *http://csrc.nist.gov/publications/*

"SP800-94: Guide to Intrusion Detection and Prevention Systems", National Institute of Standards and Technology (NIST)
- URL: *http://csrc.nist.gov/publications/*

"Syslog Working Group", IETF
- URL: *http://www.ietf.org/html.charters/syslog-charter.html*

"RFC3164: The BSD syslog Protocol", C.Lonvick

- URL: *http://www.ietf.org/rfc/rfc3164.txt*

"RFC3195: Reliable Delivery for Syslog", D.New, M.Rose

- URL: *http://www.ietf.org/rfc/rfc3195.txt*

"Internet Draft: The syslog Protocol", R.Gerhards

- *URL: http://www.ietf.org/internet-drafts/draft-ietf-syslog-protocol-19.txt*

"TLS Transport Mapping for syslog", F.Miao, M.Yuzhi

- URL: *http://www.ietf.org/internet-drafts/draft-ietf-syslog-transport-tls-06.txt*

"Signed syslog messages", F.Miao, M.Yuzhi

- URL: *http://www.ietf.org/internet-drafts/draft-ietf-syslog-sign-21.txt*

Cursos y certificaciones

"Curso de Acreditación STIC: Detección de Intrusos", Centro Criptológico Nacional (CCN)

- URL: *https://www.ccn-cert.cni.es/*
- URL: *https://www.ccn.cni.es*

"SEC503: Intrusion Detection In-Depth", SANS Institute

- URL: *http://www.sans.org/training/description.php?tid=242*

"GIAC Certified Intrusion Analyst (GCIA)", GIAC

- URL: *http://www.giac.org/certifications/security/gcia.php*

Libros

"Advanced Intrusion Detection with Cisco Security Agent (CSA)", Cisco Press

- ISBN: *978-1-58705-252-1*

"Intrusión Detection and Prevention", Osborne McGraw-Hill

- ISBN: *9780072229547*

"Security Threat Mitigation with Cisco Security MARS", Cisco Press

- ISBN: *978-1587052606*

"Security Log Management: Identifying Patterns in the Chaos", Syngress

- ISBN: *978-1597490429*

Herramientas

Gestión, tratamiento y centralización de logs

LogCheck

- *URL: http://logcheck.org/*

LogWatch

- *URL: http://www.logwatch.org/*

Swatch

- *URL: http://swatch.sourceforge.net/*

LogSurfer

- *URL: http://www.cert.dfn.de/eng/logsurf/*

Syslog-NG

- *URL: http://www.balabit.com/products/syslog_ng/*

MSyslog

- *URL: http://sourceforge.net/projects/msyslog/*

NTSyslog

- *URL: http://ntsyslog.sourceforge.net/*

KiwiSyslog

- *URL: http://www.kiwisyslog.com/syslog-info.php*

WinLogd

- *URL: http://www.edoceo.com/products/winlogd.php*

STunnel

- *URL: http://www.stunnel.org/*

Gestión y correlación de eventos de seguridad

"Open Source HIDS (OSSEC)"

- URL: *http://www.ossec.net*

"Open-Source Security Information Management (OSSIM)"

- URL: *http://www.ossim.net*

"Security Event Correlator (SEC)"

- URL: *http://www.estpak.ee/~risto/sec/*

"Cisco Security Monitoring, Análisis and Response System (MARS)"

- URL: *http://www.cisco.com/go/mars/*

"RSA EnVison / NetworkIntelligence"

- URL: *http://www.rsa.com/node.aspx?id=3170*

"Microsoft Operations Manager (MOM)"
- URL: *http://www.microsoft.com/mom/default.mspx*

"netForensics nFX Open Security Platform"
URL: *http://www.netforensics.com/products/nFX_osp/*

"ArcSight Enterprise Security Management"
URL: *http://www.arcsight.com/product.htm*

"Computer Associates Security Command Center"
URL: *http://www3.ca.com/solutions/Product.aspx?ID=4351*

"Novell Sentinel"
URL: *http://www.novell.com/products/sentinel/*

"LogLogic Log Management and Intelligence Platform"
URL: *http://www.loglogic.com/products/*

"Symantec Security Information Manager"
URL: http://www.symantec.com/es/es/enterprise/products/overview.jsp?pcid=1004

Verificación de código malicioso tipo 'rootkit'

Chkrootkit
- *URL: http://www.chkrootkit.org*

Klister
- *URL: http://www.rootkit.com/project.php?id=14*

Rootkit Revealer
- *URL: http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx*

Verificación de integridad de ficheros

Advanced Intrusión Detection Environment (AIDE)
- *URL: http://www.cs.tut.fi/~rammer/aide.html*

The SAMHAIN File Integrity Intrusión Detection System
- *URL: http://www.la-samhna.de/samhain/*

Tripwire
- *URL: http://www.tripwire.com*

Revisión de configuraciones débiles

Tiger
- *URL: http://savannah.nongnu.org/projects/tiger/*

Debcheck

- *URL: http://qa.debian.org/debcheck.php*

Agentes HIDS

McAfee Host Intrusión Prevention
- *URL: http://www.mcafee.com/us/enterprise/products/host_intrusion_prevention/index.html*

Cisco Security Agent
- *URL: http://www.cisco.com/go/csa/*

Open-HIDS
- *URL: http://www.securiteam.com/tools/5HP072AFPK.html*

Snare
- *URL: http://www.intersectalliance.com/projects/Snare/*

Perfilado de red

Sancp
- *URL: http://www.metre.net/sancp.html*

Otras

Arpwatch
- *URL: http://www-nrg.ee.lbl.gov/*

Sentry Tools
- *URL: http://sourceforge.net/projects/sentrytools*

Prelude
- *URL: http://www.prelude-ids.org/*

Wkr
- *URL: http://www.cs.ucsb.edu/~wkr/projects/ids_alert_verification/*

Systrace
- *URL: http://www.citi.umich.edu/u/provos/systrace/index.html*

Otras

"Centre de Supercomputació de Catalunya (CESCA)"
- URL: *http://www.cesca.es*

"Jessland Security Services (JSS)"
- URL: *http://www.jessland.net*

"Carlos Fragoso Website"
- URL: *http://carlos.fragoso.es*