# 14.GLOSARIO

**Actualización en Debian**: Para pasar a la última versión de Debian es necesario editar los servidores del fichero `/etc/apt/sources.list`. En dicho fichero habrá que sustituir las palabras "stable" por "testing" manteniendo el nombre de los servidores (aunque se pueden añadir nuevos). A continuación, tecleamos apt-get dist-upgrade para actualizar la versión, *update* para descargar nuevas listas de paquetes y *upgrade* para actualizar los paquetes. Con esto tenemos todo a la última versión excepto el núcleo.

```
debian:~# apt-get dist-upgrade
debian:~# apt-get update
debian:~# apt-get upgrade
```

**Actualización en Gentoo**: Hay que hacer uso del comando *emerge* y las opciones *world* para actualizar el sistema a la última versión estable. Opción *gentoo-sources* para descargar el núcleo y para actualizar a la última versión en fase de testeo hay que añadir la palabra clave "~x86" para arquitectura x86.

```
gentoo:~# emerge gentoo-sources
gentoo:~# emerge -puvD world
gentoo:~# ACCEPT_KEYWORDS="~x86" emerge -v prelude-manager
```

**Alerta**: Son alertas de bajo nivel. Este tipo de información viene directamente de los sensores a la red en formato IDMEF (prelude) y se almacenan en la base de datos de eventos.

**Alarma**: Son alertas de alto nivel de peligrosidad. Este tipo de información es la salida del motor de correlación y se almacenan en la base de datos de meta-eventos.

**Apache**: Es el programa del servidor Apache HTTP. Se diseña para ser ejecutado como un proceso demonio, escuchando peticiones de forma continua. Hay que enviar una señar para pararlo (TERM al proceso inicial o padre). El identificador (PID) del proceso se escribe en un fichero dado por el archivo de configuración. Apache también puede ser invocado por el demonio de internet *inetd*.

**API**: Una API (del inglés Application Programming Interface - Interfaz de Programación de Aplicaciones) es un conjunto de especificaciones de comunicación entre componentes software. Representa un método para conseguir abstracción en la programación, generalmente (aunque no necesariamente) entre los niveles o capas inferiores y los superiores del software.

**Appliance**: Se trata de una servidor de propósito específico, con un software instalado a bajo nivel que opera sobre un sistema operativo modificado (parcheado) y se instala en memorias tipo Compact Flash.

**Argus**: Acrónimo de "network Audit Record Generation and Utilization System" es una aplicación para sistemas de utilización y generación del expediente de la auditoría de redes. http://www.qosient.com/argus/.

**Cisco PIX Firewall**: véase PIX.

**ClamAV**: Antivirus "Clam" de software libre. www.clamav.net.

**CGI**: Pasarela de Interfaz Común, es el acrónimo de Common Gateway Interface. Es una importante tecnología de la www (World Wide Web) que permite a un cliente (explorador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el programa. Es un mecanismo de comunicación entre el servidor web y una aplicación externa.

**Copia de seguridad de base de datos**: `pg_dump -f nombrearchivo.sql eventdb`

**Draft**: Un draft es un documento de trabajo de la IETF (Internet Engineering Task Force) y sus áreas y grupos de trabajo. Además, otros grupos pueden distribuir documentos de trabajo como Internet-Drafts. Son válidos por un máximo de seis meses y pueden ser actualización, obsoleto o replazado de otro draft. La lista de los drafts actuales está en http://www.ietf.org/ietf/1id-abstracts.txt la de los directorios shadow en http://www.ietf.org/shadow.html.

**DTD** (Document type definition). Definición para describir el tipo de documento en XML. En principio se propuso usar SMI (Estructura de la información de gestión) del protocolo SNMP para describir una MIB, aunque por diversos motivos de internacionalización, agregación, combinación de mensajes, seguridad etc, se decidió por IDMEF sobre XML, por lo que es necesaria una definición del tipo de documento XML. Esta definición es la que se conoce como DTD.

**Fail-Over**: A prueba de fallos, con redundancia de equipo.. Característica de los servidores que permite les permite que los clientes se redireccionen a un servidor secundario cuando el primario cae.

**Falso positivo**: Es la generación de un mensaje de alerta o alarma que, teniendo alto riesgo de infección o intrusión, no ha tenido éxito al haber sido bloqueado. Por ejemplo, un IDS puede generar una alerta de intrusión que luego bloquea el cortafuegos. Se dice que el IDS ha generado un falso positivo.

**Glibc**: Librería de lenguaje C GNU. Todos los sistemas Como-Unix deben tener una librería en C para las llamadas al sistema, además de otras funciones como *open, malloc, printf, exit*...Para la creación de los perfiles de Prelude es necesario el uso del comando *prelude-adduser* de una versión de *libprelude* igual o mayor que la 0.9.7, la cual requiere una versión de **glibc** igual o posterior a la 2.3.6 (http://ftp.gnu.org/gnu/glibc/glibc-2.3.6.tar.bz2). Esta librería es muy dependiente de muchas otras por lo que se recomienda una actualización de versión del sistema operativo para mayor estabilidad. Véase "*Actualización en Debian"*.

**Grsecurity**: Es un conjunto de parches de seguridad para las versiones 2.4.x del núcleo de Linux.

**Honeyd**: Demonio para crear máquinas virtuales en Linux.

**HTTP**: Acrónimo de HyperText Transfer Prótocol, protocolo de transferencia de texto.

**IANA**: Es el acrónimo de Internet Assigned Number Authority (www.iana.org). La Agencia de Asignación de Números Internet era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN.

**ICANN:** Es el acrónimo en inglés de Internet Corporation for Assigned Names and Numbers o Corportación de Internet para la Asignación de Nombres y Números. Es una organización sin ánimo de lucro creada el 18 de Septiembre de 1998 con objeto de encargarse de cierto número de tareas realizadas con anterioridad a esa fecha por otra organización, la IANA. Las atribuciones de la ICANN vinieron dadas por el departamento de comercio de los Estados Unidos bajo la figura de adjudicación directa y única; es decir, no se permitió a ningún organismo o empresa adicional presentar ofertas para la adjudicación de las tareas. Dichas tareas incluyen la gestión de la asignación de nombres de dominio y direcciones IP. Hasta la fecha, casi todo el esfuerzo realizado ha estado involucrado con la creación de 7 nuevos dominios genéricos de primer nivel.

**Ipchains**: Administrador de cortafuegos de IP. Ipchains se usa para activar, mantener e inspeccionar las reglas del cortafuegos IP en el núcleo de Linux. Estas reglas pueden dividirse en cuatro categorías: La cadena de entrada IP, la cadena de salida IP, la cadena siguiente IP y las cadenas definidas de usuario.

**Ipfw**: Cortafuegos de IP. Las instalaciones del cortafuego del IP en el núcleo de Linux proporcionan los mecanismos para la contabilidad de los paquetes del IP, para los cortafuegos basados

en el filtrado a nivel de paquete, para los que usan servidores proxy transparentes, y para enmascarar los paquetes remitidos.

**IPSO**: IPSO es el sistema operativo de aplicaciones seguras de Nokia que se ejecuta en los *appliances* de las redes Nokia. Derivado de FreeBSD, IPSO es un sistema operativo evolucionado y escalable que gestiona fácilmente aplicaciones críticas de seguridad en plataformas Nokia.

**Iptables**: Iptables es una estructura de tablas genérica para la definición de conjunto de reglas. Cada regla en una tabla IP consiste en un número de clasificadores (*iptable matches*) y una acción conectada (*iptables target*).

**JDBC**: JDBC es el acrónimo de Java Database Connectivity, un API que permite la ejecución de operaciones sobre bases de datos desde el lenguaje de programación Java independientemente del sistema de operación donde se ejecute o de la base de datos a la cual se accede utilizando el dialecto SQL del modelo de base de datos que se utilice.

**MS-SQL**: Microsoft SQL. Lenguaje de bases de datos para Microsoft SQL Server, software propietario con licencia por servidor.

**Nagios**: Nagios es una plataforma de software libre que incluye programas de monitorización de red, servidor y servicios. www.nagios.org.

**Netfilter**: Es una solución de código abierto asociado con *iptables* para el filtrado de paquetes. Forma parte del núcleo de Linux en sus versiones 2.4.x y 2.6.x.

**NIC (Network Information Center)**: Es un grupo de gente, un ente o una institución encargada de asignar dominios de internet bajo su dominio de red sean genéricos o de países, a personas naturales o empresas que mediante un DNS pueden montar sitios de internet mediante un proveeedor de hospedaje.

**NIC (Network Interface Card)**: Dispositivo electrónico que permite a una DTE (Data Terminal Equipment) ordenador o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom, etc). Hay diversos tipos de adaptadores en función del tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, etc.), pero, actualmente el más común es del tipo Ethernet utilizando un interfaz o conector RJ45.

**Nokia IPSO:** véase IPSO.

**NTSUG**: Acrónimo de North Texas Snort User Group. Grupo de usuarios que organiza ponencias, y eventos relacionados con el sistema de detección de intrusiones Snort.

**Oinkmaster**: Gestor de reglas del sistema de detección de intrusiones Snort. http://oinkmaster.sf.net/.

**PAM**: Acrónimo de Pluggable Authentication Modules. Es un sistema de librerías que maneja las tareas de autenticación de las aplicaciones (servicios) del sistema. Provee de programas como *login* o *su* que garantizan los privilegios definidos en las listas de control de acceso (ACL).

**PCRE**: Acrónimo de Perl Common Regular Expressions. Librería para formar expresiones regulares en Perl. En este proyecto es de especial interés ya que el fichero de configuración de Prelude-LML usa este tipo de expresiones regulares para rellenar los campos IDMEF de los sensores que no tienen soporte para Prelude.

**PIX**: Cortafuegos PIX de Cisco. Es un software para “Appliance” de seguridad Cisco, es decir, sistema operativo de servidor de cortafuegos de propósito específico que incluye el PDM (PIX Device Manager) o gestor de dispositivo.

**Plugin:** Programa que interactúa con otro programa para aportarle una función o utilidad específica, generalmente muy específica. Este programa adicional es ejecutado por la aplicación principal. Por ejemplo, el Snort se puede instalar con el plugin de salida de Prelude, para enviar los mensajes en formato IDMEF.

**Portsentry**: Programa que escucha los puertos que le indiquemos que deben permanecer siempre inactivos en modo promiscuo. En caso de llegar una conexión a uno de ellos puede marcarlo en la bitácora del sistema, bloquear toda la comunicación con la dirección identificada como agresora, o ejecutar un comando externo.

**Postfix**: Postfix es un Agente de Transporte de Correos (MTA) de código abierto, un programa informático para el enrutamiento y envío de correo electrónico, que tiene la intención de ser una alternativa más rápida, fácil de administrar y segura del ampliamente utilizado Sendmail. Formalmente conocido como VMailer e IBM Secure Mailer, fue originalmente escrito por Wietse Venema durante su estadía en el Thomas J. Watson Research Center de IBM, y continúa siendo desarrollado activamente.

**Procchck**: Verificador de procesos que registra el estado IDS, p0f, nessus, demonios logwatch en el servidor de Foresight Prophet.

**Prophet**: Servidor de Foresight que se encarga de la recopilación de eventos, almacenamiento en una base de datos y procesamiento posterior.

**Samhain**: Es una solución multiplataforma de software libre para chequeo de la integridad de ficheros centralizados y detección de intrusiones basadas en host POSIX (Unix, Linux, Cygwin/Windows). Ha sido diseñado para monitorizar múltiples máquinas con distintos sitemas operativos desde una máquina central, aunque ello también puede ser usado como una aplicación independiente en una computadora individual.

**SNMP:** Protocolo simple de gestión de red, acrónimo de Simple Network Management Protocol. Forma parte de la arquitectura TCP/IP y soporta UDP, pero no soporta cifrado de datos. Secure-SNMP o S-SNMP es una extensión a SNMP con cifrado de datos, pero no está muy extendido al restar sencillez y rapidez.

**Ssh**: Programa para conectarse a una máquina remota y ejecutar comandos en dicha máquina. Se pide autenticación por RSA, por lo que provee de encriptación segura y reemplaza a los comandos *rlogin* y *rsh*. Es una solución software libre (OpenSSH).

**Restaurar base de datos**: Para la base de datos de nombre eventdb, y si está en un archivo comprimido, se realiza con el comando: `gunzip -c /tmp/eventdb.sql.gz | psql -d eventdb` De este modo el usuario dueño será *postgres* (usuario por defecto). Si por el contrario la salida del *pg_dump* no fue comprimida, el comando es: `psql -d eventdb < /tmp/eventdb.sql`

**Vacuum**: Para eliminar datos y purgar los ya marcados, de la base de datos. fichero postgresql.conf . Se deberán activar las siguientes líneas.

```
stats_start_collector = on
stasts_row_level = on
autovacuum = on
```

**XML**: Lenguaje de marcas extensible. (E**x**tensible **m**arkup **l**anguage)

**XSL:** Lenguaje de estilos extensible. (E**x**tensible **s**tyle **l**anguage)