Seguridad en Linux

María Laura Chiesa

Sepa por qué es importante atender a la seguridad informática de su sistema operativo. No crea que por trabajar con Linux está exento de riesgos. Todo sistema operativo tiene más o menos vulnerabilidades. Aprenda sobre los tipos de seguridad existentes, conozca cuáles son las amenazas más frecuentes y obtenga un listado de herramientas útiles para enfrentarlas. ¡Que no lo agarren desprevenido!

linux@software.com.pl

¿Qué significa *seguridad informática*? Para definir el término *seguridad informática* antes vamos a explicar qué significa *seguro*. Obviamente, lo opuesto a *inseguro*, que es aquello que implica una mayor o menor probabilidad de riesgo o peligro de que ocurra algo malo.

También vamos a definir *informática*, que, según la Wikipedia, es la disciplina que estudia el tratamiento automático de la información (datos) utilizando dispositivos electrónicos (hardware) y sistemas computacionales (software). La informática se utiliza en un enorme número de tareas y es cada vez más indispensable para apoyar y potenciar la memoria, el pensamiento y la comunicación de los hombres. Por ende, su seguridad, principalmente la que respecta a los datos y la información, es un tema prioritario.

Entonces, entendemos como seguridad informática un estado del sistema informático que nos indica que ese sistema está libre de peligro, daño o riesgo. Para que un sistema sea seguro deberá cumplir los siguientes requisitos:

- Integridad: la información no puede ser modificada por quien no está autorizado.
- Confidencialidad: la información sólo debe ser legible para los autorizados.
- Disponibilidad: la información debe estar disponible cuando se necesita.
- Irrefutabilidad: no rechazo o no repudio. La autoría de esa información no puede ser negada.

Para la mayoría de los expertos, el concepto de seguridad en la informática es utópico porque no existe un sistema

Sobre las autoras

Este artículo se desarrolló a través del equipo de Serviweb.es: Paula Sebastián, periodista y próxima a recibirse de Licenciada en Comunicación Social en la Universidad de Buenos Aires, trabaja en el área de e-marketing desde hace varios años y María Laura Chiesa, diseñadora gráfica recibida en la Universidad de Buenos Aires, y docente de la misma universidad desde el año 1999, especialista en Diseno Web y Marketing online.

Figura 1. Seguridad informática: existen diferentes tipos de seguridad, la mayoría se enfoca en la protección de datos

seguro al cien por ciento. Esto se debe a que siempre su funcionamiento directo o los resultados que se obtienen del mismo se ven afectados por algunos de los siguientes riesgos: la involuntaria ejecución de programas malignos, como virus electrónicos; el mal funcionamiento de programas en sí benignos; la penetración ajena en nuestra máquina al estar conectada a una red.

Seguridad, Internet y Linux

Internet es la red más popular y exitosa porque es abierta, se accede a ella fácilmente y permite realizar un número cada vez mayor de actividades. Por eso tiene un enorme atractivo comercial y las empresas invierten cada vez más en ella. Pero donde hay dinero, hay inseguridad. A través de Internet, muchos sistemas informáticos sufren riesgos. Linux no es ajeno a ellos a pesar de que tiene la ventaja respecto a otros sistemas operativos de que los drivers de dispositivos corren en el espacio del usuario y no en el kernel del sistema.

Al tratarse de un sistema multiusuario real, puede haber varios usuarios trabajando a la vez cada uno desde su terminal. El sistema tiene la obligación de proteger a unos usuarios frente a otros y protegerse a sí mismo. Es por eso que la seguridad es un requisito básico para aquellos que utilizan Linux.

Mucho se ha hablado sobre la superioridad de Linux en cuanto a seguridad respecto al resto de los sistemas operativos. Quizás sea verdad, pero no significa que sea totalmente seguro.

Como vimos, Linux también corre riesgos y tiene vulnerabilidades, aunque menos que los otros. Por sus características, a través de él es fácil evitar catástrofes o limitarlas y, llegado el caso, remediarlas. Igualmente, es importante tomar ciertas precauciones.

Pasos previos

Antes de intentar asegurar su sistema, debe delimitar contra qué nivel de amenaza tiene que protegerlo, qué riesgos debe o no asumir y cuan vulnerable resultará. Además, tendrá que conocer qué está protegiendo, por qué, qué valor tiene y de quién es la responsabilidad sobre los datos y otros elementos.

Normalmente querrá garantizar que su sistema permanezca en funcionamiento de forma adecuada, que nadie pueda obtener o modificar la información a la que no tiene derecho legítimo, asegurar comunicaciones seguras, preservar la confidencialidad, integridad y disponibilidad de la información, etc.

Como no existe un sistema completamente seguro, todo lo que puede hacer es aumentar la dificultad para evitar que alguien ponga en riesgo o comprometa su sistema.

Otro factor a tener en cuenta es que cuanto más incremente la seguridad de su sistema, mayor será la pérdida de funcionalidad y comodidad.

Entonces, una buena planificación es la ayuda para conseguir los niveles de seguridad que pretende.

¿Qué tipos de seguridades hay?

Para poder definir una política de seguridad que indique qué niveles requiere su sistema deberá comenzar por definir qué tipo de seguridad está buscando:

Seguridad física

¿Quienes tienen acceso físico a los ordenadores? ¿Realmente deberían poder acceder a ellos?

El nivel de seguridad física que necesita un sistema depende de su situación física concreta. Un usuario doméstico no necesitará preocuparse demasiado por la protección física, salvo de proteger su ordenador de un niño, del agua, de un cambio de tensión eléctrica, etc. En una oficina los cuidados requeridos pueden ser diferentes.

Linux proporciona los niveles exigibles de seguridad física para un sistema operativo:

- Un arranque seguro con identificación de usuario a través de un login. El sistema puede registrar todos los intentos de acceso (fallidos o no), por lo que no pasarán desapercibidos intentos repetidos de acceso no autorizado.

Seguridad, Internet y Linux

Pros	Contras
Linux es un sistema en constante cambio, desarrollo y mejora.	
Cualquier inconveniente en cuanto a seguridad, será solucionado por el gran número de programadores que contribuyen en su desarrollo.	Sus ajustes no son auditados de manera exhaustiva.
Linux tiene fama de ser el sistema operativo más seguro.	
Por lo general, el usuario de este sistema suele prestar más atención a lo que descarga, a su proveniencia, a lo que ejecuta y a cómo lo ejecuta.	La excesiva confianza en su superioridad conduce al usuario a bajar la guardia y aumentar los riesgos.
Detección de bugs.	
Lo bugs se conocen de manera natural y en menos de 24 horas se encuentra la solución a ellos o aparecen versiones del mismo software con el problema corregido.	Las versiones del software que se incluyen en los CD suelen tener numerosos bugs al poco tiempo de su lanzamiento.
Presencia de virus.	
Su estructura de permisos y políticas de seguridad no permite la fácil propagación de los virus.	Los virus existen en Linux.

Figura 2. Los pros y contras de Linux como sistema operativo seguro

- La posibilidad de bloquear las terminales.
- Salvapantallas.
- Las capacidades de un sistema multiusuario real.

Seguridad Local

- Puede haber varios usuarios trabajando al mismo tiempo con Linux, cada uno en su puesto. Esto obliga a tener en cuenta medidas de seguridad adicionales.
- Un control de acceso a los usuarios verificando una pareja de usuario y clave. Cada fichero y directorio debe tener su propietario y permisos.
- Las claves deben ser fáciles de recordar y difíciles de adivinar. Recomendamos que contengan letras, números y caracteres especiales.
- Localizar y borrar o modificar los ejecutables SUID/SGIDs innecesarios.

Seguridad del Sistema de Archivos

Cada usuario debería poseer sólo los permisos necesarios para poder cubrir las necesidades de su trabajo sin arriesgar el trabajo de los demás. Utilizar medidas como:

- Hacer una correcta distribución del espacio de almacenamiento. Esto limita el riesgo de que el deterioro de una partición afecte a todo el sistema. La pérdida se limitaría al contenido de esa partición.
- Asegurarse de que los ficheros del sistema y los de cada usuario sean sólo accesibles por quienes tienen que hacerlo y de la forma que deben.
- Enlaces. Los sistemas de ficheros de tipo Unix permiten crear enlaces entre ficheros. Los enlaces pueden ser duros o simbólicos.
- Ejecutar un programa, como Tripwire, que verifique la integridad de la información almacenada en los ficheros

Figura 3. Utilizar una encriptación resistente ayuda a mejorar la seguridad de la red

- Limitar el espacio asignado a los usuarios para evitar que un ataque consuma el espacio de todo el disco duro.

Seguridad del Núcleo

- Linux muestra el código fuente del núcleo, lo que permite a los usuarios crear núcleos a medida de sus necesidades, entre ellas, la mejora de la seguridad.

Como el núcleo controla las características de red de su sistema es importante que tenga las opciones que garanticen la seguridad y que el propio núcleo no pueda verse comprometido. Para prevenir algunos de los últimos ataques de red, debe tener una versión del núcleo actualizada.

Tenga como primera medida la de usar la cuenta de root sólo para realizar tareas concretas y breves y el resto hacerlo como usuario normal. En los casos de tareas que necesiten privilegios de administrador puede usar la orden *su* (Super Usuario) o también *sudo*. Así podrá acceder a los privilegios de root sólo cuando le interese.

Otra medida preventiva consiste en no conectarse a un servicio IRC como usuario root.

Seguridad del Root

Muchas veces, el propio administrador daña el sistema por descuido, por exceso de confianza, por ignorancia. Evite llegar a esa situación:

- No use la cuenta de root por norma, como ya dijimos más arriba.
- Ejecute los comandos de forma segura verificando previamente la acción que va a realizar.
- Ciertos mandatos admiten una opción (-i) para actuar de forma interactiva. Actívela añadiendo estas líneas a su fichero de recursos para la shell:
  - alias rm='rm -i'
  - alias cp='cp -i'
  - alias mv='mv -i'
- Evite que la clave del root viaje por una red sin cifrar. Utilice ssh u otro canal seguro.

Seguridad del Host

Elegir buenas contraseñas, asegurar los servicios de red local del host, mantener buenos registros de las cuentas y mejorar los programas con exploits de seguridad conocidos. Todas, tareas que el administrador de seguridad local tiene la responsabilidad de hacer.

Seguridad de la Red

Es imposible pretender que con tantos ordenadores conviviendo en una misma red cada uno de ellos sea seguro. Por eso es importante que sólo los usuarios autorizados pueden usar su red. Lo puede lograr de la siguiente manera:

- Construir firewalls.
- Usar una encriptación resistente.
- Verificar que no haya máquinas inseguras.
- Instalar un servidor proxy con caché.
- Proporcionar acceso transparente a Internet a una red local mediante IP masquerade. De esta forma, si utiliza direcciones de red privadas, se asegura que los equipos de la red interna no sean accesibles desde Internet si no es a través del equipo Linux.
- Efectuar conexiones con sistemas remotos manteniendo una conexión cifrada a través de SSH y stelnet. Con esto evita, entre otras cosas, que las claves circulen por la red sin cifrar.

Es importante también tener en cuenta que muchas veces son los propios usuarios de la red los que sin quererlo la exponen a riesgos. Como la mayoría de las aplicaciones de seguridad corporativas se actualizan desde dentro de la propia red y previo registro o login, el uso de portátiles puede ser peligroso en caso de que se utilicen en redes externas a la de la empresa. Muchos trabajadores, por ejemplo, llevan la notebook a su casa, se conectan a Internet y quedan expuestos a muchas vulnerabilidades.

Herramientas para cada necesidad

- Filtrado de Paquetes:
  - Netfilter / Iptables (*http://www.netfilter.org*)
- Detección y Prevención de Intrusiones (IDS/IPS):
  - Los IDS basados en red, conocidos como Network-based IDS (NIDS), trabajan sobre el tráfico de red (Snort) capturando paquetes, normalizando los protocolos, analizando encabezados o datos y disparando alertas para que se puedan tomar las contramedidas adecuadas (poner parches, filtrar hosts o redes, asegurar el sistema operativo, etc). Los IDS's, al tener la capacidad de reconocer ataques o anomalías, evolucionaron como sistemas de respuesta activa y de prevención de intrusiones.
- Filtrado de Contenidos:
  - Proxy / Caché (HTTP) Squid (*http://www.squid-cache.org*) Proxy y caché de HTTP y FTP. Proxy SSL Jerarquías

de caché ICP, HTCP, CARP, Cache Digests Proxy transparente Aceleración https Caché de búsquedas DNS Listas de control de acceso Redirectores (SquidGuard para URL Filtering).
- DansGuardian (*http://dansguardian.org/*) Filtra el contenido de páginas basándose en búsqueda de frases, PICS y URL.

- Redes Privadas Virtuales (VPN):
  - IPSEC – Kernel 2.6 Stack (ipsec-tools). Incluido por defecto en las versiones de Kernel 2.6. Implementa las principales características de IPSEC (ESP, AH, Modos Transporte y Tunnel, NAT-T, X509).
  - IPSEC – OpenSWAN (*http://openswan.org*)
    Derivado del proyecto FreeSWAN, soporta ampliamente IPSEC incluyendo: OE, IPSEC UDP Encapsulation, IKE v2, XAUTH, NAT-T en modo túnel. Es necesario parchar las fuentes del Kernel y recompilarlo. De igual manera requiere la instalación de sus herramientas de usuario.
  - SSL VPN – OpenVPN (*http://openvpn.net*).
    Implementa túneles utilizando UDP como transporte y seguridad mediante TLS/SSLv.3. Implementado en User-Space, fácil de instalar y disponible en múltiples plataformas.
- Servicios de Directorio y Autenticación:
  - Servidor de Directorios LDAP: Open LDAP (*http://openldap.org*)
  - Servidor de Autenticación de Red: Kerberos (*http://web.mit.edu/kerberos/*)
  - RedHat / Fedora Directory Server: (*http://directory.fedora.redhat.com*)
  - Servidor LDAP, incluye replicación multimaster, GUI de administración: creación de *usuarios/grupos/roles/cuentas, backup/restore/import/export*, replicación, *database/suffix*, control de acceso, monitoreo, logs. Autenticación SALS, Kerberos.
- Criptografía:
  - OpenSSH (*http://www.openssh.org/*)
    Implementación del protocolo Secure Shell versiones: 1.3, 1.5 y 2.0. Soporta autenticación simple con usuario / contraseña y utiliza certificados digitales X.509. Soporta la creación de túneles.
  - OpenSSL (*http://www.openssl.org*). Implementación de los protocolos SSL versiones: 2, 3 y TLS versión 1. Muchos otros proyectos Open Source, utilizan la Librería (API de programación) de OpenSSL para la creación de conexiones seguras.
- Auditoría de Redes:
  - Nessus (*http://www.nessus.org/*)
    Analizador de vulnerabilidades. Realiza diversas comprobaciones (tests) en busca de vulnerabilidades contra servicios de red. Su base de datos de vulnerabilidades es actualizable y extensible mediante NASL (Nessus Attack Scripting Language). Genera reportes basados en HTML.
  - NMAP (*http://www.insecure.org/nmap/*).
    Mapeador de redes, analizador de puertos, altamente configurable. Realiza reconocimiento activo de S.O. remotos mediante la identificación de huellas digitales de S.O. Muchas otras más: Hping, nikto, SARA, etc.
- Auditoría de redes inalámbricas:
  - WifiSlax (*http://www.wifislax.com/*)
    Se trata de una distribución española de Linux basada en Slax. Está orientada principalmente a la seguridad WiFi. Es bastante rápida y funcional y cuenta con muchas aplicaciones para estar al tanto sobre la seguridad de su red, como pueden ser analizadores de tráfico o debuggers. Además cuenta con herramientas de Internet y con aplicaciones para grabar, escuchar música, etc. Inicialmente es un live CD para poder testearla, pero si le gusta puede instalarla sin problemas en el sistema operativo.
  - BackTrack (*http://www.remote-exploit.org/backtrack.html*)
    Es una de las distribuciones de Linux más conocidas por aquellos que se dedican a hacer tests de penetración. Es un live CD que le permite arrancar directamente sin necesidad de instalar nada en el disco duro y provee de multitud de herramientas. La lista de las incluidas en la distribución es muy grande y comprende desde programas para obtener información del equipo y de la red hasta exploits para aumentar los niveles de privilegios.

Glosario

- *Bug*: fallo de un programa por una equivocación en el diseño o desarrollo del mismo.
- *Cache*: espacio en el disco duro donde se guardan datos temporales.
- *Exploits*: método concreto de usar un error de algún programa (bug) para entrar en un sistema informático. Puede ser un programa o no.
- *Firewall*: combinación de hardware y software que proporciona un sistema de seguridad, generalmente para ayudar a evitar el acceso de externos no autorizados a una red.
- *Host*: ordenador directamente conectado a una red, que efectúa las funciones de un servidor y alberga servicios, como correo electrónico, grupos de discusión Usenet, FTP o World Wide Web accesibles por otros ordenadores de la red.
- *IDS*: sistema de detección de intrusos.
- *IP masquerade*: truco que permite que varias máquinas usen una sola dirección IP, haciendo que las otras máquinas se hagan pasar por la máquina que realmente tiene la conexión.
- *Multiusuario*: sistema capaz de soportar el trabajo de varios usuarios en una misma máquina o grupo reducido de ellas.
- *Patch*: parche.
- *Plugin*: componente de software (usualmente pequeño) que agrega funcionalidades a otra pieza mayor de software.
- *Root*: administrador. Aquel que puede realizar muchas cosas que un usuario común no.
- *Script*: una serie de instrucciones escritas en un programa, para ser interpretadas por otro programa.
- *IRC*: un sistema de conversación en tiempo real para usuarios de Internet.
- *Shell*: programa ordinario (ejecutable) que sirve de interfaz entre el Kernel y el usuario. Es también un lenguaje de programación y como tal permite usar variables, estructuras sintácticas, entradas/salidas etc.
- *Stelnet*: programas que le permiten efectuar conexiones con sistemas remotos y tener una conexión cifrada.
- *SUID/SGID*: Set User IDentity y Set gid, en inglés. Permisos que hacen que los ficheros que los tengan se ejecuten con los privilegios de su propietario y no del usuario que los ejecuta. Si el propietario es el root un mal uso puede comprometer el sistema.
- *UDP*: User Datagram Protocol, en inglés. Protocolo que se usa básicamente para transmitir mensajes dentro de una red.

Figura 4. Algunos de los logos de las herramientas usadas para cada requerimiento de seguridad

- Antivirus Perimetral/Antispam:
  - Clam Antivirus (*http://www.clamav.net*)
- ANTISPAM:
  - SpamAssassin (*http://pamassassin.apache.org/*).
    Potente herramienta antispam, utiliza algoritmos de redes neuronales: PERCEPTRON (rule-weigthing algorithm), para su sistema de puntuación. Amplia variedad de tests para la identificación de SPAM. Escrito en PERL, ofrece al programador las librerías Mail::SpamAssassin classes para la integración con sistemas de correos.
- Integración Antivirus/Antispam para sistemas de correos con:
  - EXIM: (*http://www.exim.org*)
    Exim puede ser configurado como proxy SMTP e integrar al ClamAV y Spam Assassin. Se requiere compilar: WITH_CONTENT_SCAN=yes. Las versiones previas a Exim 4.50 no incorporaban análisis de contenido y se realizaba a través de Exiscan (parche para Exim).
- Seguridad del Núcleo:
  - The Linux Kernel Archives. (*http://www.kernel.org/*)
- Seguridad del Root:
  - SUDO (*http://www.courtesan.com/sudo/*)
    Herramienta que permite a ciertos usuarios usar comandos privilegiados sin necesidad de ser root, como montar o desmontar dispositivos. También registra las actividades que se realizan, lo que ayuda a determinar qué hace realmente ese usuario.

Las 10 herramientas más utilizadas

Existen varias herramientas que permiten hacer de Linux un sistema operativo más seguro.

Bastille

Es una aplicación diseñada para aplicarse en entornos Linux y darle mayor seguridad a nivel local. Es decir, en el caso de que un atacante logre ingresar a su sistema, Bastille gestiona una serie de medidas para evitar los males que pueda provocar el invasor. Se basa en el concepto de "bastionar" un sistema a posteriori (una vez instalado) automatizando tareas comunes (eliminar servicios). Se trata de un conjunto de scripts que, en unos pocos pasos, le permitirá aumentar la seguridad de su sistema operativo de una manera gráfica o en modo texto. Sólo tiene que responder una serie de preguntas claves, todas repartidas entre los diversos módulos detallados abajo, y el script configurará las opciones de la manera más segura posible conforme a sus preferencias. Posee una función "undo" que le permite restaurar la configuración inicial del sistema en caso de que fuera necesario. Tiene un enfoque muy pedagógico ya que se aprende mucho durante su instalación. El proyecto está dividido en 16 módulos entre los cuales están:

- Wrapper Script
- Actualizacion de patchs
- Permisos de archivos
- Creación de cuentas y seguridad
- LILO/Usuario único
- inetd/ TCP
- Wrappers
- PAM!!!
- Logging
- UserSpace Tools
- Etc.

http://www.bastille-linux.org/

Nessus

Scanner de vulnerabilidades para diversos sistemas operativos. Consta de dos partes, cliente y servidor, que pueden estar instaladas en la misma máquina por comodidad. El servidor realiza los ataques mientras que el cliente interactúa con el usuario a través de una interfaz gráfica. Nessus desarrolla una completa exploración de todos los puertos con nmap o con su propio scanner para detectar los que están abiertos y luego intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL. Opcionalmente, los resultados del escaneo pueden ser exportados en reportes en varios formatos. En ellos hay enlaces que explican el tipo de vulnerabilidad encontrada, cómo explotarla y cómo evitarla. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades. Contras: es un poco lento. Además, algunas de las pruebas de vulnerabilidades de Nessus pueden causar que los servicios o sistemas operativos se corrompan y caigan. Puede evitar esto desactivando *unsafe test* (pruebas no seguras) antes de escanear.

http://www.nessus.org/

TCP Wrappers (Envolvedor de TCP)

Pequeños programas que permiten una conexión controlada, restringiendo determinados servicios del sistema.

TCP Wrappers trabaja en terminales y se usa para filtrar el acceso de red a servicios de protocolos de Internet que corren en sistemas operativos (tipo UNIX), como ser Linux o BSD. Permite que las direcciones IP, los nombres de terminales y/o respuestas de consultas ident de las terminales o subredes sean usadas como tokens sobre los cuales filtrar para propósitos de control de acceso.

Se pueden monitorizar y filtrar las peticiones de entrada de servicios como Systar, Finger, FTP, Telnet, Rlogin, RSH, TFTP, etc. El wrapper reporta el nombre del cliente y del servicio que ha solicitado pero no intercambia información con el cliente o el servidor de la aplicación/servicio solicitado porque lo que hace es comprobar si el cliente tiene permiso para utilizar el servicio que está pidiendo y si no es así, corta la conexión.

ftp://ftp.porcupine.org/pub/security/index.html

Tripwire

Herramienta de seguridad e integridad de datos Open Source útil para monitorear y alertar en cambios específicos de ficheros en un rango de sistemas.Tripwire asume que todos los controles de seguridad han fallado y que el sistema fue alterado. Tripwire alerta al administrador de estos cambios a fin de tomar acciones con rapidez.

Para esto, Tripwire monitorea rutinariamente y por intervalos la integridad de los archivos que tienden a ser blanco de los atacantes. El programa debe ser instalado antes de haber conectado el computador por primera vez a Internet a fin de crear una base de datos de los ficheros existentes en el sistema, para poder contrastar los posibles cambios en éstos una vez conectado a la red.

http://www.tripwire.com

Netcat

Es una herramienta de red bajo licencia GPL disponible para sistemas UNIX, Microsoft y Apple que permite a través de intérprete de comandos y con una sintaxis muy sencilla abrir puertos TCP/UDP en un HOST (quedando netcat a la escucha), asociar una shell a un puerto en concreto (para conectarse por ejemplo al intérprete bash de Linux remotamente) y forzar conexiones UDP/TCP, útil por ejemplo para realizar rastreos de puertos o realizar transferencias de archivos bit a bit entre dos equipos.

Sus capacidades hacen que sea a menudo usada como una herramienta para abrir puertas traseras una vez invadido un sistema y obtenidos privilegios de administrador o root del equipo. También resulta extremadamente útil a efectos de depuración para aplicaciones de red. Se ha usado mucho también para explotar el bug del Isapi en los servidores IIS.

http://netcat.sourceforge.net/

TCPDump

Monitoriza todo el tráfico de una red, recolecta toda la información posible y detecta así problemas, como ataques ping. Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está atado. En UNIX y otros sistemas operativos, es necesario tener los privilegios del root para utilizar TCPDump. El usuario puede aplicar varios filtros para que sea más depurada la salida.

La utilización más frecuente de TCPDump es para:

- Depurar aplicaciones que utilizan la red para comunicar.
- Depurar la red misma.
- Capturar y leer datos enviados por otros usuarios u ordenadores.

http://www.tcpdump.org/

Snort

Es un sniffer de paquetes y un detector de intrusos basado en red. Sirve para detectar intrusiones y ataques tipo búfer overflows, CGI, SMB, escaneo de puertos, etc. Snort puede enviar alertas en tiempo real, mandándolas directamente al archivo de Unix syslog o incluso a un sistema Windows mediante SAMBA.

http://www.snort.org

SAINT (Security Administrator's Integrated Network Tool)

Es un scanner de seguridad de red. Es una evolución del conocido SATAN para plataformas Unix que sirve para evaluar toda la seguridad de un sistema recibiendo incluso múltiples updates desde el CERT y CIAC. Saint produce una salida muy fácil de leer y entender, graduando por prioridad los problemas de seguridad y también soporta módulos de escaneo añadidos, lo cual lo hace muy flexible.

http://www.wwdsi.com/saint

SARA (Security Auditor's Research Assistant)

Es la tercera generación de herramientas para el análisis de seguridad en plataformas Unix.

http://www-arc.com/sara

OpenBSD

Es un sistema operativo libre tipo Unix, multiplataforma, basado en 4.4 BSD. Es un descendiente de NetBSD , con un foco especial en la seguridad y criptografía. Este sistema operativo, se concentra en la portabilidad, cumplimiento de normas y regulaciones, corrección, seguridad proactiva y criptografía integrada.

http://www.openbsd.org/