Identificación de la gestión de red y su implicación con la seguridad

Prof. Dr. Javier Areitio Bertolín

El Prof. Dr. Javier Areitio Bertolín es Catedrático de la Facultad de Ingeniería. ESIDE y Director del Grupo de Investigación Redes y Sistemas de la Universidad de Deusto.
E. Mail: jareitio@eside.deusto.es

En el presente artículo se analizan los elementos implicados en la gestión de red. Se aborda la evolución de SNMP haciendo énfasis en las cuestiones de seguridad claves para el correcto funcionamiento de toda red. Por último se presta atención a tres protocolos de seguridad: SSL3/TLS1 que proporcionan seguridad a la capa de transporte y SSH2 que lo hace al nivel de aplicación. Los tres tienen en común: una fase de establecimiento de clave autenticada, una negociación protegida de ciphersuite, utilizan claves establecidas para construir un canal seguro, proporcionan seguridad, en capas TCP/IP distintas SSL/TLS en transporte y SSH en aplicación, la seguridad de los tres esta indeterminada por la debilidad de la implementación, la seguridad de las plataformas cliente (malware, keystroke-logers) y servidor (gusanos, rootkits, código malicioso), presentan limitado despliegue de certificados e infraestructura para soportarlos, especialmente los certificados del cliente, se detecta una carencia de educación y concienciación de los usuarios en ambos, todos se pueden utilizar para construir VPNs.

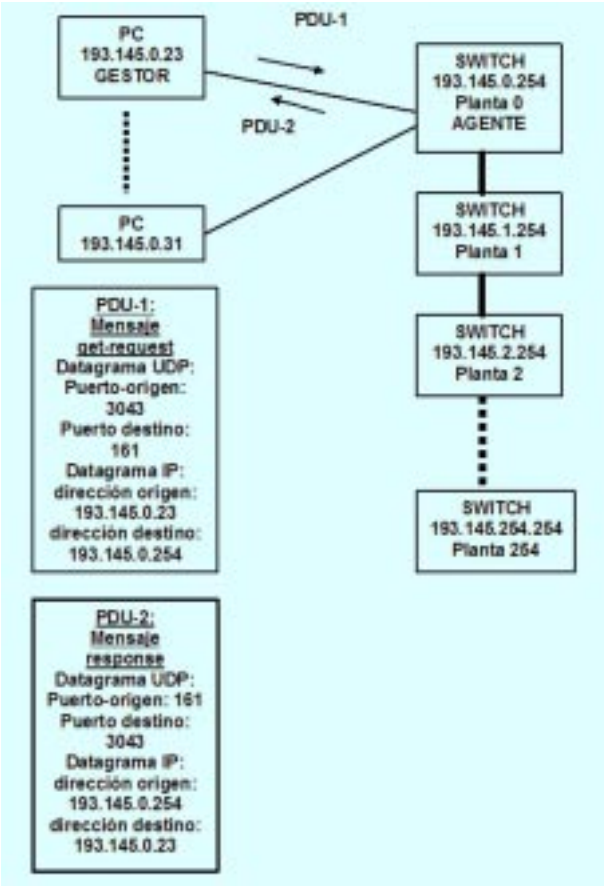

Figura 1. Contenido de los mensajes SNMP para la gestión de red

La gestión de redes complejas es una tarea muy difícil, sin gestión de red los fallos que acontecen:

- Interrumpirán el funcionamiento de la red.
- Se necesitará un esfuerzo sustancial para identificarlos.
- Se requerirá mucho tiempo para su reparación.

Los servicios de gestión de red en combinación con dispositivos convenientemente desplegados permitirán que:

- Los fallos se identifiquen y traten de forma local.
- Los mensajes de alerta se localicen y recojan de forma centralizada.
- Se tomen las acciones apropiadas.

Existe un conjunto amplio de herramientas especializadas de gestión de red disponible como por ejemplo *OpenView* de HP, *Netview* de IBM, *NetManager* de Sun, *Spectrum* de Aprisma, etc. Se pueden identificar como características comunes de todas estas herramientas de gestión de red:

- Interfaz gráfico o GUI.
- Permiten recoger un conjunto de mensajes de alerta de red.
- Permiten examinar la red y el tráfico que circula.

Protocolos de gestión de red

Los protocolos de gestión de red permiten la gestión *en línea* tanto de computadores o sistemas finales como de redes. Todos ellos soportan:

- Gestión de configuración.
- Contabilidad.
- *Logging* o recogida de eventos.
- Ayudan con el diagnóstico de problemas.

Los protocolos de gestión de red como SNMP son protocolos del nivel de aplicación y se utilizan para las comunicaciones intercambiadas en los sistemas de gestión de red. La gestión de red necesita protegerse, dos aspectos de la seguridad de gestión de red definidos en el estándar ISO 7498-2 son:

- Gestión de la seguridad, hace referencia al soporte proporcionado por los protocolos de gestión de red para la provisión de servicios de seguridad.
- Seguridad de la gestión, aquí se engloban todos los medios para proteger las comunicaciones de la gestión de red.

Protocolo SNMP. Modelo de arquitectura.

El protocolo SNMP (Simple Network Management Protocol), perteneciente a la pila de protocolos TCP/IP, es parte del sistema de gestión de Internet, ha evolucionado pasando por tres versiones:

- SNMP versión 1 o SNMPv1 (1990/91) especificado en los documentos del IETF (www.ietf.org): RFC 1155-1157 y 1212/1213.
- SNMP versión 2 o SNMPv2 (1993) incorpora algunas características de seguridad y se especifica en RFC 1441-1448.
- SNMP versión 3 o SNMPv3 (estandarizado por el IETF en 2002), presenta más características de seguridad, especificado en RFC 2570-2576. El SNMP lo utilizan muchas herramientas de gestión de red comercializadas.

El modelo de arquitectura esta basado en:

- Una estación de gestión de red (o sistema de computación) donde reside un gestor asociado con una MIB central, que ejecuta SNMP con software de gestión.
- Un agente de gestión asociado con su MIB, en cada elemento de red gestionado (router, switch, puesto

Figura 2. Arquitectura de protocolos SSL

de trabajo o *desktop*, servidor, etc.) que implementa SNMP, proporciona acceso a la Base de Información de Gestión o MIB.

El protocolo SNMPv1 utiliza el protocolo de la capa de transporte no orientado a la conexión UDP, por tanto no garantiza que el tráfico de gestión se reciba en la otra entidad. Como principales ventajas: reducido costo (también denominado *overhead*) y simplicidad del protocolo. Como inconvenientes: la operación orientada a la conexión debe integrarse en las aplicaciones de nivel superior si se necesitan características de fiabilidad y contabilidad. Las versiones 2 y 3 de SNMP pueden utilizar el protocolo de transporte TCP orientado a la conexión.

Operaciones de SNMPv1. Unidades de datos de protocolo. Números de puerto. Comportamiento del gestor y agente. Ejemplos de traps.

SNMPv1 proporciona tres operaciones simples:

- GET, permite al gestor de la estación de gestión recuperar los valores de los objetos de cada agente implantado en cada dispositivo de red o estación gestionada.
- SET, permite al gestor de la estación de gestión escribir valores de objetos del agente ubicado en un elemento gestionado.
- TRAP, permite al agente de un elemento gestionado notificar al gestor ubicado en una estación de gestión de eventos significativos. SNMP permite múltiples accesos con una única operación.

Las unidades de datos de protocolo o PDU utilizadas en SNMPv2 son:

- *Get-request*, se utiliza para obtener valores de una o más instancias de objetos MIB de un agente ubicado en un dispositivo de red gestionado.
- *Get-next-request*, es similar a *get-request* salvo que permite recuperar la siguiente instancia del objeto MIB en una lista o tabla en orden lexicográfico en el árbol de la MIB.
- *Get-bulk-request,* permite obtener valores en un bloque grande de datos, por ejemplo una tabla grande.
- *Inform-request*, la utiliza una entidad gestora para notificar a otra entidad gestora cierta información MIB que es remota a la entidad receptora; la entidad receptora responde con una PDU *response*.
- *Set-request*, se utiliza para dar o cambiar valor a una o más instancias de un objeto MIB de un agente.
- *Response*, permite responder a las PDUs: *get-request*, *get-next-request, get-bulk-request, inform-request* y *set-request*.
- Trap, permite a un agente informar al gestor de una estación de gestión de un evento; no responde en este caso la entidad del gestor.

Los números de puerto UDP utilizados por SNMP son el 161 para peticiones o *requests* y la 162 para *traps*.

El comportamiento del gestor es:

- Escucha los *traps* de los agentes sobre el puerto local 162.
- Envía *peticiones* al puerto 161 del agente remoto.

El comportamiento del agente es:

- Escucha *peticiones* del gestor sobre el puerto local 161.
- Envía *traps* al puerto 162 del gestor remoto.

El formato de los mensajes SNMPv1 consta de tres campos:

- La versión.
- La comunidad, concepto local definido en cada dispositivo. La comunidad SNMP es el conjunto de gestores SNMP que tienen permiso el acceso a un dispositivo concreto. Cada comunidad se define utilizando un único nombre (dentro del dispositivo) denominado nombre de comunidad. Cada gestor debe especificar una comunidad en todas las operaciones *get* y *set*. En los switch Matrix Serie C2 tipo C2H124-48 de Enterasys con 48 puertos Ethernet 10/100 la comunidad es pública por ejemplo ro/rw/su.
- Resto de la PDU SNMP propiamente dicha, donde se indica el tipo de operación.

Ejemplos de *traps* Cisco son:

- *Authentication*. El agente detecta que el gestor no esta adecuadamente autenticado, en SNMPv1 significa una cadena de comunidad incorrecta.
- *Linkup*. El dispositivo donde esta el agente reconoce que uno de los enlaces de comunicación representado en la configuración del agente se ha activado.
- *Linkdown*. El dispositivo donde esta el agente reconoce un fallo de uno de los enlaces de comunicación representado en la configuración del agente.
- *Coldstart*. El dispositivo donde esta el agente se re-inicializa por tanto la configuración puede estar alterada.
- *Warmstart*. El dispositivo donde esta el agente se re-inicializa pero la configuración no será alterada.

Servicios de seguridad de SNMPv1. Mecanismos de autenticación y control de acceso. Nombres y perfiles de comunidad.

El protocolo SNMPv1 proporciona los dos siguientes servicios de seguridad:

- Servicio de autenticación de origen de datos, asegura a un dispositivo destino que la PDU SNMP viene desde el origen que dice venir. El mecanismo de autenticación utilizado para implementar el servicio de su

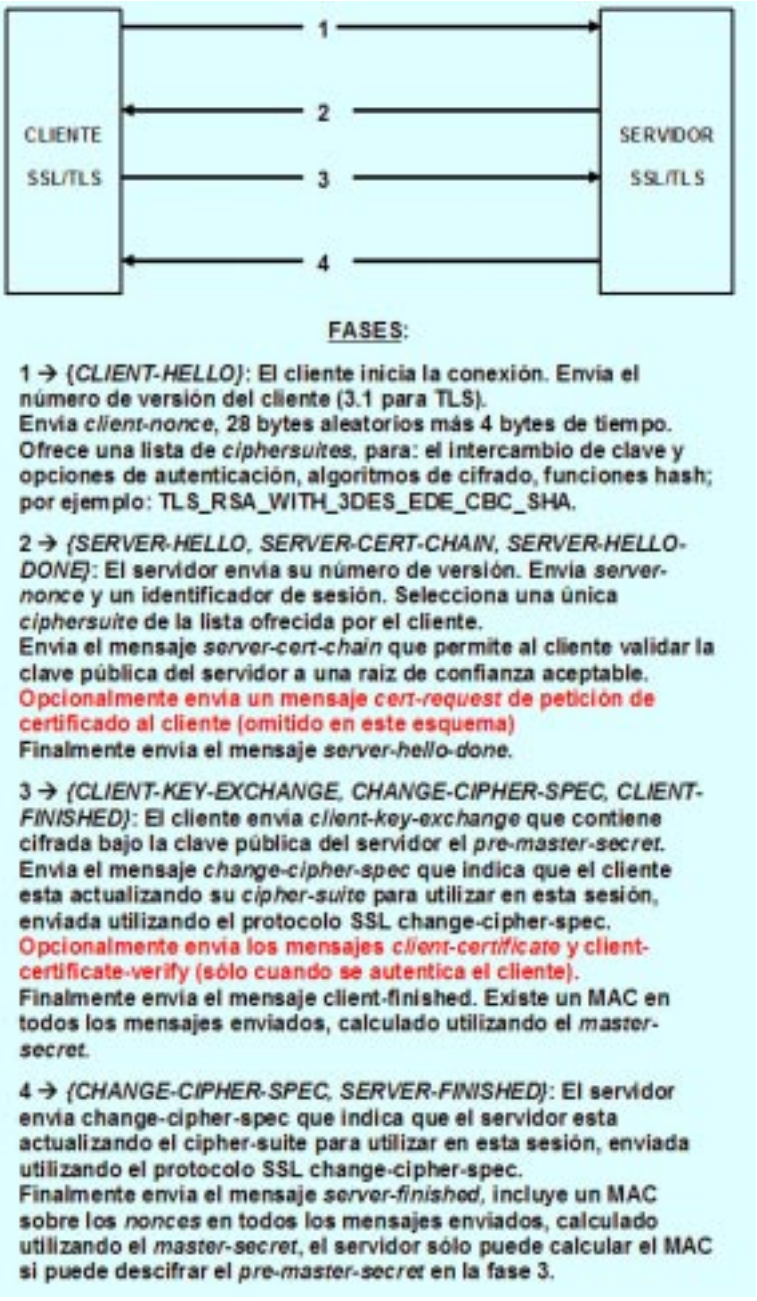

Figura 3. Esquema de funcionamiento del protocolo de handshake SSL/TLS sin autenticación del cliente pero con el servidor autenticado al cliente

mismo nombre se basa en el nombre de comunidad incluido en cada mensaje SNMP de una estación de gestión a un dispositivo gestionado. Este nombre de comunidad actúa como una contraseña, es decir el mensaje se supone que es auténtico si el emisor conoce la contraseña. No existe protección alguna por ejemplo cifrándolo en el nombre de comunidad.

• Servicio de control de acceso, limita las operaciones SNMP que un dispositivo puede pedir de acuerdo a la identidad del dispositivo. Estos servicios se implantan utilizando un mecanismo de autenticación y uno de control de acceso pero proporcionan un nivel trivial de seguridad. El mecanismo de control de acceso utilizado para implementar el servicio de su mismo nombre se basa en que cada dispositivo tiene guardado los perfiles de comunidad.

Un perfil de comunidad consta de una combinación de:

• Un subconjunto definido de objetos MIB o una vista de la MIB.

• Un modo de acceso para dichos objetos: sólo lectura o lectura-escritura.

Un perfil de comunidad se guarda para cada comunidad que un dispositivo puede reconocer. La decisión de acceso se basa en el nombre y perfil de comunidad.

Amenazas y vulnerabilidades en SNMPv1.

Las principales amenazas primarias son:

• Modificación de datos, un mensaje SNMPv1 puede modificarse en tránsito dando lugar a que ocurra una operación de gestión incorrecta.

• Suplantación, un atacante puede enviar mensajes SNMPv1 falsos causando que ocurran operaciones de gestión incorrectas.

Las amenazas secundarias más relevantes son:

• Modificación, reordenación, repetición y/ retardo del flujo de mensajes SNMPv1, debido al empleo de un protocolo UDP no orientado a la conexión para transportar mensajes SNMPv1.

• Escucha clandestina, puede darse la revelación no intencionada de la información de gestión.

Las principales vulnerabilidades de SNMPv1 son:

• No existe protección de integridad en los mensajes SNMPv1.

• No se garantiza la llegada a tiempo y oportuna de los mensajes SNMPv1.

• No existe protección contra repeticiones.

• El mecanismo de autenticación es muy débil: (a) Un atacante con acceso a red puede leer mensajes SNMP con ayuda de un *sniffer* y registrar el nombre de comunidad que va en texto en claro en las PDU. (b) Un atacante puede intentar utilizar nombres de comunidad comunes.
• El mecanismo de control de acceso es muy débil ya que una vez conocido el nombre de comunidad, todos los tipos de acceso especificados en el perfil de comunidad correspondiente son permitidos.
• No existe mecanismo de confidencialidad.

La seguridad de SNMPv1 es pésima ya que si un atacante tiene acceso a red y puede leer con un *sniffer* o averiguar el nombre de comunidad podrá tomar el control de los dispositivos gestionados:
• Puede reconfigurar switches y routers conduciendo a fugas de información y utilización no legítima.
• Puede permitir ataques de denegación de servicios o DoS, por ejemplo re-arrancando repetidamente los dispositivos de red.

El protocolo SNMPv1 fue diseñado bajo la suposición que la red y todos los dispositivos a ella conectados son confiables. En la práctica esta suposición normalmente no se sostiene y a pesar de todo SNMPv1 aún se utiliza. Las últimas versiones de SNMP (la 2 y la 3) han implantado los siguientes servicios de seguridad para hacer frente a las amenazas anteriormente señaladas:
• Autenticación del origen de los datos.
• Integridad de los datos.
• Integridad de la secuencia de mensajes.
• Confidencialidad de datos.
• Protección de repetición limitada y de la llegada a tiempo de los mensajes.

El protocolo SNMPv3 presenta una provisión más completa de servicios de seguridad que SNMPv2 que es un protocolo de transición de la versión una a la tres.

Protocolo SNMPv3. Entidades SNMP con autoridad.

Un usuario identificado por un nombre de usuario o *UserName*, soporta las claves secretas e información de seguridad adicional como algoritmos criptográficos a utilizar. Las entidades de SNMPv3 son identificadas por *snmpEngineID*, cada dispositivo gestionado o estación de gestión tiene un *snmpEngineID.* Siempre que se envía un mensaje, se puede identificar una entidad con autoridad; para *get* y *set*, el receptor es la entidad con autoridad, para *trap, response* o *inform-request* el emisor es la entidad con autoridad. Una *entidad snmp con autoridad* posee las claves localizadas y tiene indicadores de llegada a tiempo de mensajes. Los *indicadores de llegada a tiempo* de mensajes previenen la repetición de mensajes, cada entidad con autoridad mantiene un reloj. Una entidad que no tiene autoridad tiene que recuperar el tiempo de la entidad con autoridad, confirmar el valor recibido y mantener un reloj sincronizado. Los mensajes pueden llegar dentro de 150 segundos de su tiempo generado.

Las claves son generadas a partir de la contraseña de usuario, el usuario proporciona contraseña a todas las entidades. Cada entidad genera una clave a partir de la contraseña y genera dos claves más utilizando el *snmpEngineID* de la entidad, una para la autenticación/integridad de datos K1 y otra para la confidencialidad K2.

Figura 4. Arquitectura de protocolos SSH2

Integridad, autenticación y confidencialidad de datos. Gestión de la seguridad SNMPv3.

Para la integridad y autenticación de datos se genera un MAC (Código de autenticación de mensaje basado en criptografía simétrica) de los mensajes a proteger.

Se utiliza un algoritmo HMAC con claves derivadas de la clave de usuario localizada K1. Se envía el MAC con el mensaje. El receptor con la misma clave compartida puede comprobar el MAC y asegurarse de la integridad y autenticidad del mensaje SNMPv3.

La confidencialidad de datos se obtiene con algoritmos criptográficos simétricos como DES en modo CBC (Cipher Block Chiang), se utiliza la segunda clave localizada K2. Tiene que utilizarse junto con la integridad de datos y la autenticidad para prevenir ciertos ataques.

El servicio de control de acceso de SNMPv3 hace posible configurar agentes para que proporcionen a distintos gestores diferentes niveles de acceso a la MIB del agente. Por ejemplo un agente podría restringir a la mayoría de los gestores ver las estadísticas relativas al rendimiento y permitir ver y actualizar los parámetros de configuración sólo a un único gestor con autorización designado para ello; así mismo el agente puede limitar las operaciones que un gestor puede utilizar sobre esa sección de la MIB, por ejemplo se podría limitar a un gestor con autoridad determinado a un acceso de sólo lectura sobre una sección de la MIB del agente.

La política de control de acceso que ha de utilizar cada agente para cada gestor debe configurarse previamente y consiste en una tabla que especifica los privilegios de acceso de los diferentes gestores con autoridad.

Figura 5. Propiedades de las funciones criptográficas *hash*

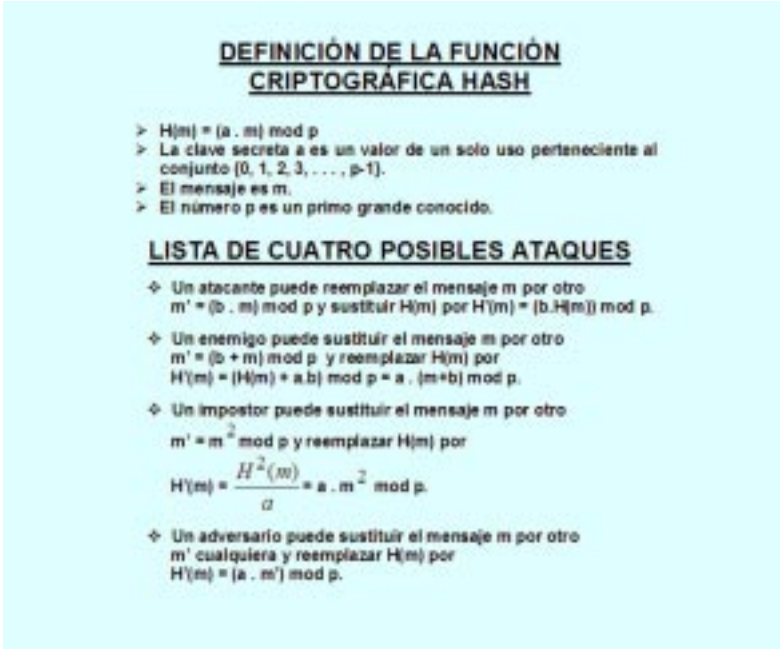

Figura 6. Batería de ataques a una función criptográfica *hash* H(m) dada

Para la gestión de la seguridad SNMP se necesitan gestionar los siguientes datos:

- Claves secretas de autenticación-integridad y privacidad-confidencialidad.
- Sincronización del reloj para la detección de repeticiones.
- Información de partes SNMP.

SNMP puede utilizarse para proporcionar gestión de claves y sincronización de reloj. Después de establecer manualmente algunas partes SNMP, el resto puede gestionarse utilizando SNMP. Las cuestiones de seguridad surgen del uso de contraseñas compartidas para generar todas las claves criptográficas. SNMPv3 actualmente lo soportan muchos fabricantes, véanse los sitios Web: http://www.ibr.cs.tu-bs.de/projects/snmpv3, http://www.ietf.org/IESG/Implementations/2571-2575-Deployment.txt.

Las principales debilidades de SNMPv3 pueden encontrarse en http://www.cert.org, entre otras son la incapacidad contra ataques DoS, de denegación de servicios y el análisis de tráfico que aunque se encuentren cifrados los mensajes, un adversario puede inferir a partir de aspectos estadísticos información sensible no autorizada.

Protocolos de seguridad SSL, TLS y SSH.

Los protocolos SSL/TLS proporcionan seguridad en la capa de transporte, utilizan el protocolo de transporte TCP para proporcionar transporte fiable extremo a extremo, las aplicaciones no necesitan prácticamente modificación.

El protocolo SSL (Secure Sockets Layer) fue desarrollado por Netscape en 1994, usualmente autentica sólo al servidor, normalmente con certificados X.509, utiliza clave de sesión de 40 o 128 bits (clave simétrica), soporta el nivel de aplicación https; la versión 1 no dada a conocer, la versión 2 con fallos pero útil y la buena es la versión 3.

TLS (Transport Layer Security) definida por el IETF en el RFC2246, TLSv1.0 presenta similitud con SSLv3.0. SSL/TLS se utiliza en los navegadores Web y servidores para soportar comercio electrónico seguro sobre HTTP. Esta integrado en Netscape, Mozilla, Internet Explorer de MS, IIS, Apache, etc. La arquitectura de SSL presenta dos niveles:

- *Protocolo de registro SSL*, proporciona un nivel seguro por encima de TCP de canal fiable.
- En la capa de aplicación junto a

Figura 7. Ejemplo de la MIB del módulo UDP de un dispositivo de red en SNMP

OBJETOS GESTIONADOS EN EL MODULO UDP DE MIB-2

ID de Objeto	Nombre	Tipo	Descripción
1.3.6.1.2.1.7.1	udpInDatagrams	Counter32	Número total de datagramas-UDP entregados en este nodo.
1.3.6.1.2.1.7.2	udpNoPorts	Counter32	Número de datagramas-UDP recibidos pero no entregados ya que no había una aplicación en el puerto destino.
1.3.6.1.2.1.7.3	udpInErrors	Counter32	Número datagramas-UDP recibidos pero no entregados por otras razones.
1.3.6.1.2.1.7.4	udpOutDatagrams	Counter32	Número total de datagramas-UDP enviados desde esta entidad.
1.3.6.1.2.1.7.5	udpTable	SEQUENCE	Una secuencia de objetos UDPEntry, uno por cada puerto que está abierto por aplicación, dado la dirección IP y el número de puerto utilizado por aplicación.

Nombre del objeto ISO – SNMP: 1.3.6.1.2.1.7.1 →

Organización identificada por ISO
ISO
DoD US
Internet
MIB2
Gestión
UDP
udpInDatagrams

CUATRO ELEMENTOS CLAVE DE SNMP

- MIB (Base de Información de Gestión) → Información distribuida almacenada de los datos de gestión de red en gestor y agentes.
- SMI (Estructura de Información de gestión) → Lenguaje de definición de datos para objetos MIB. Tipos de datos básicos: counter32, IPaddress, time-ticks, integer32, etc.
- Protocolo SNMP → Comandos y respuestas intercambiados entre gestores y agentes.
- Capacidades de seguridad y administración → En SNMPv3.

HTTP incluye tres protocolos: *protocolo de handshake SSL*, *protocolo de alerta SSL* y el *protocolo change cipher spec*, utilizado para indicar la entidad que cambia el *ciphersuite* acordado recientemente.

SSH (Secure Shell) proporciona seguridad en la capa de aplicación, sólo cubre tráfico explícitamente protegido, las aplicaciones necesitan modificación, se encuentra encima de TCP. La versión 1 presenta muchas vulnerabilidades, la mejor es la versión 2, es decir SSH2. SSH2 adopta una arquitectura de tres capas:

- *Protocolo de nivel de transporte SSH*, para la conexión inicial, autenticación de servidor, establece un canal seguro entre cliente y servidor.
- *Protocolo de autenticación de usuario SSH*, autenticación de cliente sobre un canal de nivel de transporte seguro.
- *Protocolo de conexión SSH*, soporta varias conexiones concurrentes sobre un único canal seguro de protocolo de nivel de transporte. Permite eficiencia, re-utilización de sesión y da soporte a varias aplicaciones.

Los objetivos de seguridad de SSH2 son:

- El servidor casi siempre se autentica en el protocolo de nivel de transporte, normalmente por un método de firma de clave pública. Las claves públicas soportadas por certificados X.509, PKI/SPKI/OpenPGP o distribuidas manualmente a los clientes.
- El usuario/computador cliente se autentica normalmente en el protocolo de autenticación de usuario, por método de clave pública (soporta muchos métodos) o por simple contraseña para una aplicación concreta sobre canal seguro o vía método basado en computador.
- Establecimiento de un secreto compartido fresco, utilizando intercambio de clave Diffie-Hellman. Secreto compartido utilizado para obtener claves adicionales similar a SSL/IPSec. Para confidencialidad y autenticación en el protocolo de nivel de transporte SSH.
- Negociación de la familia de mecanismos criptográficos seguros: cifrado, MAC y algoritmos de compresión. Autenticación de servidor y métodos de intercambio de claves.

Bibliografia

- Areitio, J. "Análisis en torno a la Seguridad de los Cortafuegos para la Seguridad de Red Perimetral". Revista Española de Electrónica. Nº 592. Marzo 2004.
- Areitio, J. "Análisis de métricas para cuadros de mando de seguridad para sistemas de información". Revista Española de Electrónica. Nº 608/609. Julio-Agosto 2005
- Dhillon, S. "Information Systems Security: A Management Challenge". John Wiley and Sons. Inc. 2005.
- Carr, H.H. and Snyder, C. "Data Communications and Network Security". 1st Edition. McGraw-Hill. 2006.
- Kenyon, T. "Implementing Network Security: Effective Security Strategies for the Enterprise". Digital Press. 2006.

Este artículo se enmarca en las actividades desarrolladas dentro del proyecto *LEFIS-APTICE: Legal Framework for the Information Society II* (financiado por Socrates 2005). *European Commission*