Implementación virtual de redes LAN, enfocadas en el análisis comparativo de las ventajas y desventajas del uso y aplicación de las diferentes versiones del protocolo SNMP

Alisson Karina Lago Castillo [(1)] Daniel Mera Moreano [(2)] Ing. Washington Medina [(3)]
Facultad de Ingeniería en Electricidad y Computación [(1) (2) (3)]
Escuela Superior Politécnica del Litoral (ESPOL) [(1) (2) (3)]
Campus Gustavo Galindo, Km 30.5 vía Perimetral [(1) (2) (3)]
Apartado 09-01-5863. Guayaquil-Ecuador [(1) (2) (3)]
aklago@espol.edu.ec [(1)] dmmera@espol.edu.ec[(2)] wmedina@espol.edu.ec [(3)]

Resumen

Cada día, el mundo se ve enfrentado a cambios significativos en muchos ámbitos, las Redes de Telecomunicaciones no se quedan atrás. En la actualidad su uso se caracteriza por el constante incremento y complejidad en las estructuras de los recursos utilizados en ellas, pero a medida que se produce esta expansión se van presentando algunos hechos evidentes, pues las redes ya no pueden ser fácilmente gestionadas directamente por el hombre; se debe realizar una planificación estratégica de su crecimiento y utilizar herramientas que funcionen de manera automatizada para el control y la gestión de la red, debido a que cualquier tipo de error o falla en alguno de sus elementos pueden desencadenar una serie de problemas que afectará directa o indirectamente a los otros dispositivos conectados a la red, por esta razón nace la importancia de incluir herramientas encargadas de gestionar de manera individual cada uno de los dispositivos y recursos pertenecientes a una red. Hay que tener claro que la gestión no solo está encargada de un monitoreo, se adentra mucho más buscando controlar fallas, rendimiento, configuración, seguridad y costos haciendo uso de varias herramientas.
En respuesta a esta necesidad se han desarrollado estándares que tratan sobre la gestión de red, los mismos que abarcan servicios, protocolos y bases de datos de información de gestión. El enfoque de este proyecto investigativo será estudiar y analizar el estándar SNMP.

Palabras Claves: *SNMP, SNMPv1, SNMPv2, SNMPv3, MIB, LAN*

Abstract

Everyday the world faces a series of changes and the telecommunication networks don't stay behind. Currently it's use is characterized by the constant increase and complexity of the structural resources used in them, but as this expansion occurs we are presented some obvious facts. Because networks can´t easily be managed directly by humans, we must carry out strategic planning for its growth and use tools that will work with automated control and management network , because any type of error or failure in one of its elements can trigger a series of problems that will directly or indirectly affect the other devices connected to the network, hence the importance of including tools responsible for individually managing each of the devices and resources belonging to a network. It should be clear that management is not only responsible for monitoring, but also for controlling failures, performances, configuration, security and costs using various tools.
In response to this need we have developed standards that address network management that covers the same services, protocols, databases and management information. The focus of this research project is to study and analyze the SNMP standard.

Keywords*: SNMP, SNMPv1, SNMPv2, SNMPv3, MIB, LAN*

1. Introducción

Desde que se creó el sistema de internet y de redes de comunicación, a la actualidad, estas han evolucionado y se han vuelto más complejas, por esta razón es importante mantener una correcta administración que no solo consista en un simple monitoreo de la red, si no que se involucre mucho más, realizando una gestión con herramientas que proporcionen una información más completa, amplia y eficiente que ayude en el correcto control, uso y desempeño de los equipos, para que de manera más

sencilla se haga un reconocimiento del comportamiento y del estado de todo lo utilizado en la red y del estado de los mensajes. Es así como dentro de algunas herramientas existentes se encuentran ciertos protocolos que nos mantienen al tanto de este correcto funcionamiento, uno de estos es el protocolo "SNMP".

Este se ha convertido en un protocolo bastante utilizado, porque brinda una forma simple de implementación y la funcionalidad que ofrece es variable.

2. Objetivos

2.1. Objetivo General

Comparar mediante la simulación virtual de redes LAN las ventajas y desventajas de las tres versiones existentes del protocolo SNMP.

2.2. Objetivos específicos

- Comprender los conceptos básicos del protocolo SNMP.
- Realizar un análisis teórico y establecer diferencias y semejanzas entre las versiones del SNMP.
- Analizar los Software a utilizarse, incluyendo la instalación y operación de los mismos.
- Simular virtualmente una pequeña red LAN con un Router y dos máquinas virtuales con diferentes sistemas operativos.
- Mostrar a través de simulaciones la operación del protocolo SNMPv1 dentro de la red LAN.
- Mostrar a través de simulaciones la operación del protocolo SNMPv2 dentro de la red LAN.
- Mostrar a través de simulaciones la operación del protocolo SNMPv3 dentro de la red LAN.
- Analizar y comparar los resultados obtenidos en las simulaciones.
- Explicar por qué la versión 2 tiene mayor acogida que la versión 3.

3. SNMP

"Simple Network Management Protocol" o SNMP se originó en la comunidad de Internet como medida para administrar redes TCP/IP, este es un sistema de administración de red basado fundamentalmente en dos elementos principales: un administrador, el cual es el terminal que le va a permitir al administrador de la red realizar las diferentes solicitudes de administración, y los agentes, los cuales son entidades que se encuentran al nivel de cada una de las interfaces, permitiendo conectar a la red los dispositivos administrados y recopilar información sobre los diferentes objetos.

Actualmente se presentan tres versiones disponibles de este protocolo; SNMPv1, SNMPv2 y SNMPv3. En las primeras dos versiones se encontraron algunos errores en lo que respecta a la seguridad del sistema, entre otras, por lo cual en la versión tres se implementaron grandes mejoras en este punto, dando una mejor seguridad, mejor autentificación y correcto control de acceso, sin embargo aunque esta es la última y mejorada versión no ha tenido tanta acogida, ni es muy aceptada como lo es la versión 2 del protocolo.

3.1. SNMPv1

SNMPv1 constituye la primera definición e implementación del protocolo SNMP, estando descrito en las RFC 1155, 1157 y 1212 del IETF (Internet Engineering Task Force).Es un protocolo de petición y respuesta sencilla. Su comportamiento se implementa mediante el uso de una de las cuatro operaciones de protocolo: Get, GetNext, Set, y Trap.

La operación Get se utiliza por el NMS para recuperar el valor de una o más instancias de objetos de un agente. La operación GetNext es utilizada por el NMS para recuperar el valor de la siguiente instancia de objeto de una tabla o una lista dentro de un agente.

La operación Set es utilizada por el NMS para configurar los valores de instancias de objetos dentro de un agente. La operación Trap es utilizada por los agentes para informar de forma asíncrona el SMN de un hecho relevante.

3.2. SNMPv2

SNMPv2 apareció en 1993, estando definido en las RFC 1441-1452. SNMPv1 y SNMPv2 tienen muchas características en común, siendo la principal mejora la introducción de nuevas operaciones de protocolo:

GetBulk: para que el gestor recupere de una forma eficiente grandes bloques de datos, tales como las columnas de una tabla

Inform: para que un agente envíe información espontánea al gestor y reciba una confirmación

Report: para que el agente envíe de forma espontánea excepciones y errores de protocolo.

SNMPv2 también incorpora un conjunto mayor de códigos de error y más colecciones de datos. En 1995 apareció una revisión de SNMPv2, denominada SNMPv2c y descrita en las RFC 1901-1910, añadiendo como mejoras una configuración más sencilla y una mayor modularidad; pero manteniendo el sencillo e inseguro mecanismo de autentificación de SNMPv1 y SNMPv2 basado en la correspondencia del denominado nombre de comunidad.

3.3. SNMPv3

[14] La última versión de SNMP, SNMPv3, refuerza las prestaciones de seguridad, incluyendo autentificación, privacidad y control de acceso; y de administración de protocolo, con una mayor modularidad y la posibilidad de configuración remota. SNMPv3 apareció en 1997, estando descrito en las RFC 1902-1908 y 2271-2275.

Cabe destacar que SNMPv3 no se trata de un estándar que reemplaza a SNMPv1 y/o SNMPv2, sino que define una serie de capacidades adicionales de seguridad y administración a ser utilizadas en conjunción con SNMPv2 (preferiblemente) o SNMPv1. Estas mejoras harán que SNMP se constituya en un protocolo de gestión susceptible de ser utilizado con altas prestaciones en todo tipo de redes, desplazando a mediano plazo a CMIP como estándar de gestión de las grandes redes de las operadoras de telecomunicación.

Fue diseñada para proteger contra las siguientes amenazas de seguridad, mediante el uso de algoritmos de autenticación y de encriptación, como lo especifica el RFC 2574

4. Elementos del Protocolo

El protocolo SNMP está compuesto por 4 elementos:

1. Estación de gestión (Manager)
2. Agente administrador (Agente)
3. Base de información de administración (MIB)
4. Protocolo de administración de redes.

4.1. Estación de gestión

[8] Se define al NMS (Network Management Station) como una interfaz entre el Administrador de red y el sistema de gestión de red, tiene una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades gestionadas en la red.

4.2. Agente administrador

[8] Es un módulo del software de gestión de red que reside en los dispositivos gestionados.

El agente, al recibir un GetRequest o GetNextRequest, emitirá un mensaje GetResponse a la estación gestora, ya sea con la información solicitada o una indicación de error indicando porqué la solicitud no pudo ser procesada.

Con un SetRequest, SNMP permite solicitar un cambio de valor a una variable específica en este caso, el agente SNMP responderá con un GetResponse que indicará que el cambio se ha hecho o en el caso de que este no pueda realizarse responderá con una indicación de error. Con el Trap, SNMP permitirá que el agente informe espontáneamente a la estación gestora de un evento "importante".

4.3. Base de información de administración

[1] MIB es un tipo de base de datos definida en el modelo OSI, su función principal es definir las variables que utiliza el protocolo SNMP para la gestión control y supervisión de los dispositivos de red.

4.4. Protocolo de administración de redes

[8] El protocolo de administración de red es un protocolo de aplicación por el cual pueden examinar o cambiar varias MIB de un agente. La comunicación de información de administración entre las entidades de gestión (gestor-agente) es realizada en el SNMP a través del intercambio de mensajes protocolares.

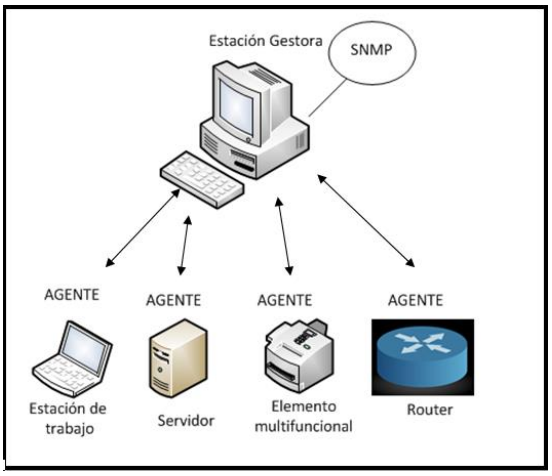

Figura 1. Elementos del protocolo de Gestión de SNMP

5. Estructura de la PDU

[7] Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU (Protocol Data Unit - Unidad de datos de protocolo).

Todas las implementaciones del SNMP soportan 5 tipos de PDU:

1. GetRequest
2. GetNextRequest
3. GetResponse
4. SetRequest
5. Trap

5.1. GetRequest

[4] Es una PDU que solicita a la entidad destino los valores de ciertas variables, las mismas que se encuentran en la lista VarBindList; en el de GetNextRequest

Esta PDU siempre tiene cero en los campos ErrorStatus y ErrorIndex y es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP.

El GetRequest siempre espera como respuesta una GetResponse.

5.2. GetNextRequest

[4] Es una PDU que solicita a la entidad destino los valores de ciertas variables, estas son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista VarBindList, El GetNextRequest es útil para confeccionar tablas de información sobre una MIB.

Esta PDU al igual que el GetRequest siempre tiene cero en los campos ErrorStatus y ErrorIndex y es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP.

El GetNextRequest siempre espera como respuesta una GetResponse.

5.3. GetResponse

[4] La forma del GetResponse es idéntica a la del GetRequest a excepción de la indicación del tipo de PDU. El GetResponse se genera por una entidad de protocolo únicamente a la recepción de la GetRequest, GetNextRequest, o SetRequest.

Esta PDU a diferencia del GetRequest y GetNextRequest no siempre tiene cero en los campos ErrorStatus y ErrorIndex, estos ya reciben datos, el primero indicando el valor que hace referencia al error generado y el segundo señalará el objeto de la lista que ha generado el error.

5.4. SetRequest

[4] Ordena a la entidad destino poner a cada objeto reflejado en la lista VarBindList el valor que tiene asignado en dicha lista. Es idéntica al formato de GetRequest, salvo por el identificador de PDU. Es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Espera siempre como respuesta un GetResponse.

5.5. Trap

[4] Es una PDU que indica una excepción o falla. Es generada por una entidad de protocolo sólo a petición de una entidad de aplicación SNMP. Cuando una entidad de protocolo recibe una Trap, presenta sus contenidos a su entidad de aplicación SNMP.

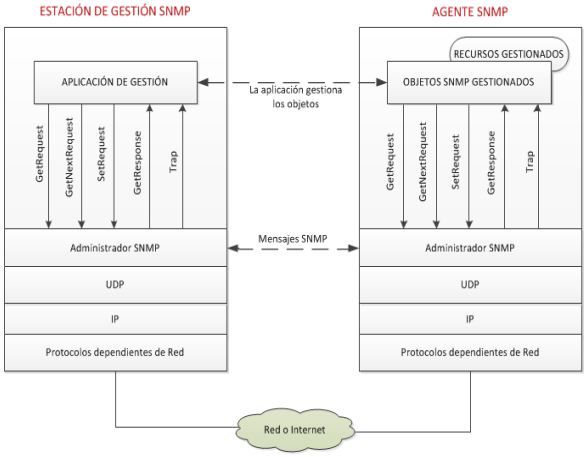

Figura 2. Principio Operativo SNMP [10]

6. Diseño e implementación

Este proyecto describe el conjunto de características pertenecientes a las operaciones de cada una de las versiones existentes del protocolo, realizando una comparación expuesta de manera sencilla con la ayuda de una red LAN.

Como recursos se tiene un Router Mikrotik y dos máquinas virtuales con sistemas operativos correspondientes a Linux y Windows Server 2008, así como también dos Softwares Wireshark, y Net-SNMP que ayudaran a mostrar detalladamente el comportamiento del sistema, el modo de seguridad brindado, el empaquetamiento y el formato de la PDU.

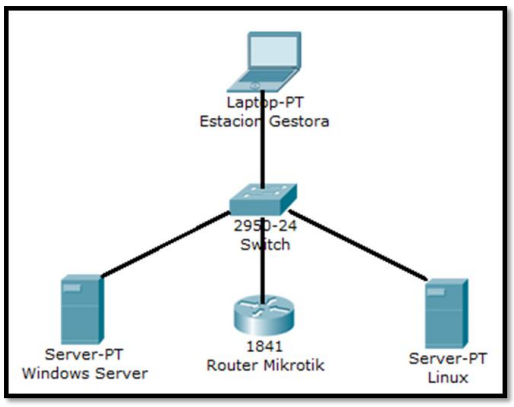

Figura 3. Topografía de la Red Lan

6.1. Sistemas Operativos

Los Sistemas Operativos son el software básico de toda computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario.

Los sistemas operativos usados en el proyecto son Windows y Linux pero como todo el desarrollo se realizara dentro de una misma computadora se hará uso de máquinas virtuales, las mismas que simularan a las dos servidores y les permitirán ejecutar programas como si fueran computadoras reales.

6.2. Router Mikrotik

[10] Un Router es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra.

Para el desarrollo del proyecto se hará uso de un Mikrotik, este un sistema Operativo de Router, es decir que con él se podrá convertir cualquier computador en un poderoso Router y no necesita de un sistema operativo previamente instalado, ya que la herramienta viene encapsulada dentro de un microkernel de Linux, lo que brinda flexibilidad y escalabilidad.

6.3. Programa Net-SNMP

[12] Net-snmp es un programa que provee herramientas y librerías relacionadas al protocolo SNMP que incluye: un agente extensible, esto quiere decir que el agente básico que viene con el programa puede ser extendido a manejar otras MIB's que uno puede desarrollar y estas pueden ser fácilmente introducidas al agente, por lo cual, éste puede monitorear lo que se le ha incorporado; una librería SNMP, provee una implementación del protocolo con la funcionalidad especificada en los RFC's que definen el funcionamiento de SNMPv1, SNMPv2 y SNMPv3.

6.4. Programa WireShark

[13] WireShark un analizador de paquetes de red, una utilidad que captura todo tipo de información que pasa a través de una conexión.

Wireshark es de código abierto, y se puede usar para diagnosticar problemas de red, efectuar auditorías de seguridad y aprender más sobre redes informáticas.

6.5. Estación Gestora

La estación gestora será la encargada de la administración de la gestión de todos los elementos conectados a la red, es desde aquí donde se ejecutarán todos los comandos para observar el funcionamiento del protocolo.

Para realizar lo antes mencionado, se instalará en la estación el programa Net-SNMP para de esta manera tener acceso a los programas que ayudarán a realizar las distintas consultas por SNMP, estos son ejecutables y programados en C, pueden correr tranquilamente en el MS-DOS del Windows, que es el que se usará en el proyecto, algunos de ellos son: snmpget snmpgetnext, snmptrap, snmpwalk, snmpbulkget, snmpbulkwalk.

7. Resultados y Comparaciones

Una vez realizadas todas las pruebas y obtenidos los resultados de manera independiente, se muestra un análisis en conjunto del protocolo SNMP en sus distintas versiones.

En SNMPv1, siendo la más básica de todas, se puede constatar con el sniffer (Wireshark), el formato de la PDU y todos sus campos definidos.

Se observa también que los traps en esta versión manejan otro tipo de formato que cambia a partir de la versión dos para estandarizarlo con el resto de las directivas.

En SNMPv2 se observa una gran similitud con la versión 1 y se aprecia que el formato de las traps ya se estandariza con el descrito en la PDU.

Se implementan nuevas directivas que optimizan las operaciones del protocolo, siendo una de estas el "GetBulk", que permite obtener múltiples OIDs en un solo paquete, lo cual es útil en una larga transmisión de datos.

SNMPv1 y SNMPv2 usan el campo de comunidad como método de seguridad y autenticación, el elemento de red compara el campo de comunidad enviado por el agente con el definido en su configuración, si estos son iguales acepta el solicitud y envía la respuesta respectiva, caso contrario no responde nada, y el agente asume que su mensaje no fue recibido por lo que sigue intentando hasta llegar al límite de su tiempo máximo de conexión definido.

En SNMPv3 se emplean campos adicionales que se usan para la seguridad adicional implementada en esta versión. Ya no se utiliza la comunidad y en su lugar existe autenticación de usuarios. También se tiene la posibilidad de encriptar el contenido del paquete evitando que su contenido pueda ser leído usando un sniffer de red como se apreció en las pruebas. Estos dos parámetros de seguridad son opcionales y su uso se define en el elemento de red. El agente también puede especificar estos parámetros mediante tres niveles de seguridad:

- noAuthNoPriv: Sin autenticación y sin encriptación.

- authNoPriv: Autenticación y sin encriptación. Los protocolos permitidos para autenticación son MD5 y SHA.

- authPriv: Autenticación y encriptación. Los protocolos permitidos para autenticación son: MD5 y SHA. Los protocolos permitidos para encriptación son: DES y AES.

Se aprecia que en toda comunicación con SNMPv3, el primer mensaje es un Get-Request que se encarga de negociar los parámetros de seguridad con el elemento de red. En este proceso los dispositivos se ponen de acuerdo en los protocolos de autenticación y encriptación y se validan credenciales. En caso de existir errores de acceso o falla en la negociación se retorna un mensaje SNMP de tipo REPORT definiendo el motivo del rechazo.

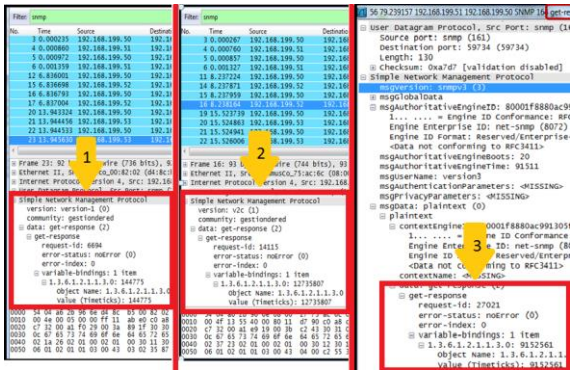

Figura 4. Comparación de la estructura de la PDU en las tres versiones con la operación GetResponse

Tabla 2. Tabla sintetizada de ventajas del protocolo SNMP

Simple Network Management Protocol
Permite y da la facilidad de monitorear y administrar la red
Opera en el nivel de aplicación utilizando el protocolo de transporte TCP/IP
Compuesto por dos elementos fundamentales el agente y el gestor
Los mensajes son recibidos en el puerto UDP 161 y las Traps en el puerto 162
Describe la información exacta y precisa de cada tipo de agente que tiene que administrar y el formato con que éste le proporciona los datos
La operación de su gestión que se necesita para intercambiar información ocupa pocos recursos de la red

Tabla 2. Tabla sintetizada de características de SNMPv1

SNMP Versión 1	
Seguridad	Usa el campo de comunidad como método de seguridad y autenticación. Permite el acceso a cualquier tipo de persona a la información que lleva la red
Operaciones	Operaciones que puede realizar: GetRequest, GetNextRequest, GetResponse, Set y Trap.
Traps	Los traps tienen una estructura de PDU distinta a la de las versiones sucesoras, Se comunican por el puerto 162

Tabla 3. Tabla sintetizada de características de SNMPv2

SNMP Versión 2	
Seguridad	Usa el campo de comunidad como método de seguridad y autenticación. Permite el acceso a cualquier tipo de persona a la información que lleva la red
Operaciones	Tiene mejoras que optimizan las operaciones entre los agentes y los elementos de red. Operaciones que puede realizar: GetRequest, GetNextRequest, GetResponse, Set, Trap, GetBulk e Inform.
Traps	Estandariza la Versión 1 del protocolo en la estructura de la PDU

Tabla 4. Tabla sintetizada de características de SNMPv3

SNMP Versión 3	
Seguridad	Se emplean campos adicionales que se usan para la seguridad y la autenticación de usuarios. Tiene tres niveles de seguridad: 1.-"noAuthNoPriv" 2.-"AuthNoPriv" 3.-"AuthPriv". Se puede encriptar el contenido de los paquetes evitando que su contenido pueda ser leído por otros usuarios
Operaciones	Operaciones que puede realizar: GetRequest, GetNextRequest, GetResponse, Set, Trap, GetBulk e Inform.
Traps	Se mantiene la estructura expuesta en la Versión 2.

8. Conclusiones

1. SNMP sirve para intercambiar y definir la estructura de una información mediante un mensaje entre una estación gestora y un agente

2. SNMP es un protocolo estándar que ayuda en la administración de redes utilizadas en Internet, se implementa de una manera fácil y sencilla, consume pocos recursos y poco tiempo del procesador, además posee la capacidad de unir distintos elementos de red sin importar marcas, modelos o fabricantes de los mismos, brinda también alarmas de alerta detectoras de fallas que se pueden observar mediante incidentes o gráficas.

3. Se pudo validar que todos los campos, del protocolo SNMP, aparecen en los paquetes capturados por el Sniffer de red tal como fueron definidos en los RFCs respectivos, para las distintas versiones del protocolo.

4. SNMPv2 definitivamente tiene mejoras que optimizan las operaciones entre los agentes y los elementos de red y además estandariza la versión 1 del protocolo.

5. En todos los escenarios se consultó el mismo OID para comprobar que la respuesta sea siempre la misma sin importar la aplicación, sistema, o hardware de los distintos elementos de red utilizados en las pruebas y los resultados fueron satisfactorios.

6. Con el Wireshark se pudo confirmar la falencia en seguridad existente en las versiones 1 y 2 del protocolo SNMP, al poderse leer la comunidad usada en la red e incluso la información de los dispositivos. Si bien es cierto se cubre esta debilidad con controles de acceso por IP, se añade una capa más de administración que puede incluso llegar a ser vulnerada con ataques más sofisticados o incluso aprovechándose de descuidos en la configuración de accesos. Con la encriptación en la versión 3 se cubre esta vulnerabilidad y se puede apreciar en las capturas de paquetes.

7. Según lo investigado, a pesar de las mejoras en seguridad implementadas en SNMPv3 la versión 2 del protocolo aun es la opción preferida para el monitoreo de las redes actuales a tal punto que muchos sistemas incluso no soportan aun SNMPv3. Esto se debe a que las falencias de seguridad de las versiones anteriores a SNMPv3 pueden ser perfectamente controladas con políticas adecuadas de seguridad en la red. Si bien es cierto esto conlleva a una capa más de administración y configuración, el grado de complejidad es menor a la que involucraría una gestión de coexistencia entre diferentes versiones.

8. A pesar de que SNMPv3 soporta los protocolos DES y AES para encriptación, el procesamiento de los mismos tienen que ser gestionados por programas externos como por ejemplo openSSL.

9. Recomendaciones

1. Para la implementación de SNMPv3 en Windows Server 2008 se tuvo que utilizar el paquete Net-SNMP debido a que el servicio de SNMP nativo de Windows no soporta esta versión.

2. Para poder hacer uso de la encriptación en SNMPv3, es necesario instalar el Net-SNMP con la característica de "EncryptionEnable", esta opción se la define durante la instalación del programa.

3. Net-SNMP para Windows requiere de OpenSSL v0.9.8y, si se lo va a instalar con la característica de EncryptionEnable. Es importante tener en cuenta que Net-SNMP es una aplicación de 32 bits por lo que los binarios de OpenSSL también deben trabajar con la misma arquitectura.

4. Dado que Net-SNMP no es un servicio nativo de Windows, se deben ejecutar unos scripts adicionales que integran este paquete a los servicios de Windows.

5. Se recomienda comenzar a emplear SNMPv3, pues esta brinda mayor seguridad debido a la encriptación y evita que sea visible la información en texto plano, esto puede llegar a ser complicado de implementar en sistemas viejos que no dan soporte a esta versión, pero para redes actuales es preferible diseñar un plan que lleve versión 3.

10. Referencias

[1] Barba Marti, A. Gestión de red, Ediciones OPC, Universita Politécnica de Catalunya, España 2001

[2] Barrios J. (2013). Cómo configurar SNMP. Extraído el 20 de abril de 2013, desde http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-linux-snmp

[3] Botero, N. (2005) Modelo de Gestión de seguridad con soporte SNMP. Extraído el 20 de abril de 2013, desde

http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf

[4] Case J. (2001). Request for Comments: 1157, SNMP. Extraído el 18 de abril de 2013, desde http://www.ietf.org/rfc/rfc1157.txt

[5] Case J. (2002). Request for Comments: 3410, SNMPv3. Extraído el 18 de abril de 2013, desde http://tools.ietf.org/html/rfc3410

[6] Case J. (1993). Request for Comments: 3410, SNMPv3. Extraído el 19 de abril de 2013, desde http://tools.ietf.org/html/rfc1449

[7] García G. Desarrollo de plano de gestión para una red MPLS (2005). Extraído el 1 de Agosto del 2013, desde http://upcommons.upc.edu/pfc/bitstream/2099.1/3781/2/40628-2.pdf

[8] Edgar Pallo, Andrés Yajamin. "Escritura y compilación de una MIB para un transmisor de microondas" Extraído el 8 de abril de 2013, desde Repositorio Digital EPN: http://bibdigital.epn.edu.ec/bitstream/15000/5413/1/T2247.pdf

[9]Wikipedia. (n/d). Extraído el 22 de mayo de 2013, desde https://es.wikipedia.org/wiki/Router

[10] William Stallings, versión 2, 2003. Fundamentos de seguridad en redes: aplicaciones y estándares

[11] Botero, N. (2005). "Modelo de gestión de seguridad con soporte a SNMP"

[12] Wikipedia. (n/d). Extraído el 20 de mayo de 2013, desde http://es.wikipedia.org/wiki/Sistema_operativo

[13] Inteco Cert. "Análisis de Trafico con Wireshark". Manual, 2011. http://openyourshell.files.wordpress.com/2011/02/analisis-de-trafico-con-wireshark.pdf

[14] Millan Ramon. (2003). "SNMPv3 (Simple Network Management Protocol version 3)" Extraído el 21 de mayo de 2013, desde http://www.ramonmillan.com/tutoriales/snmpv3.php

[15]Manage Engine. (n/d). Extraído el 16 de mayo de 2013, desde http://www.manageengine.com/products/mibbrowser-free-tool/