Siuderlan: Sistema Informático para la Ubicación de Estaciones de Red en una LAN alámbrica

Por: MSc. Denis Morejón López, Administrador de red, División Territorial Cienfuegos, ETECSA e Ing. Jesús Alberto Leandro León, Informático Ferrocarriles Cienfuegos.
denis.morejon@etecsa.cu; jexus@nauta.cu

RESUMEN
La ubicación física de computadoras en una red informática alambrada de mediana o grandes dimensiones es una tarea de importancia vital para la seguridad de cualquier organización. Generalmente, se tiene cierto control sobre los nombres de las estaciones de trabajo, su dirección IP o el identificador de su tarjeta de red, pero estos datos muchas veces no se adquieren de forma automática por lo que es difícil mantenerlos con fidelidad. Este trabajo propone un sistema informático capaz de interactuar con conmutadores y enrutadores de diversas tecnologías para ubicar de manera precisa y en el tiempo los puestos de trabajo o locales desde donde se conectan las computadoras que forman parte de una red LAN a fin de controlar el acceso de estaciones nuevas en la red.
Palabras clave: Control de acceso, Localización física, Estaciones, LAN, SNMP, Seguridad informática.

ABSTRACT
Physical Computer Location in a wired mid- or high dimension computer network is an important task for the security of any organization. Generally, workstation names, IP addresses or network card ID are somehow controlled, but this information sometimes is not obtained automatically, therefore is difficult to keep accurate record about it. This work proposes a computer system able to interact with switches and routers from diverse technologies for locating in a precisely time and manner the working positions and facilities from where LAN networking computers are connected in order to control access to new stations within the network.
Keywords: Access Control, Physical Location, Stations, LAN, SNMP, Computer Security.

Introducción

Las tecnologías empleadas en la fabricación de computadoras personales (PC) y en otros elementos de redes locales como conmutadores (*switches*) y enrutadores (*routers*) han alcanzado un alto desarrollo lo que hace más fácil el montaje de este tipo de redes para las organizaciones [1]. Por tanto, existe una tendencia al crecimiento en el número de redes locales y en el tamaño de las mismas. El tamaño es proporcional al número de miembros (computadoras) que se poseen. Esto ayuda a la productividad de las organizaciones, pero trae aparejado riesgos de seguridad que hay que tener en cuenta para el normal desarrollo de los negocios o actividades de las mismas.

Existen y se implementan en el mundo muchas medidas para asegurar las redes locales como: Antivirus, Sistemas Detectores de Intrusos —*Intrusion Detection Systems* (IDS)—, corta fuegos perimetrales, sistemas para la supervisión de tráfico, subsistemas de trazas o historiales que se activan en las aplicaciones fundamentales de la organización [2]. Todos estos sistemas son capaces de detectar anomalías en la red e identificar la computadora que las provoca o su número IP. En redes pequeñas (en espacio y número de integrantes) este dato pudiera ser suficiente para que el administrador de red localice físicamente la PC infractora porque puede memorizar sus respectivos identificadores y el lugar donde está instalada. Incluso, si se tratara de una computadora portátil externa a la organización que fuera insertada desde uno de esos lugares bastaría recorrerlos para encontrarla y tomar las medidas administrativas pertinentes en caso necesario.

Este proceder no es efectivo aplicarlo cuando se trata de redes de más de 200 PC distribuidas en más de 3 edificios que, a su vez, poseen más de 20 locales cada uno, por citar un ejemplo. El tiempo invertido sería muy prolongado y si se tratara de un intruso que agrede intencionalmente la red, este podría retirarse a tiempo después de cumplir su objetivo antes de que fuese ubicado.

Otra manera de salir del control habitual de identificadores por PC y locales es cambiar el número IP de una estación de trabajo normal. En este caso, cuando los sistemas de seguridad reportan una anomalía proveniente de un número IP nuevo, el administrador de red pudiera pensar que se trata de una máquina introducida en la red, pero en realidad se trata de la estación habitual con el identificador alterado [2]. Si el número IP nuevo fuera el de otra estación de trabajo que está apagada en otro local pudiera pensarse, en primera instancia, que el intruso yace en esa PC cuando tampoco es el caso.

La acción de cambiar el número IP solo puede ser realizada por un usuario con privilegios de administración sobre su máquina o por un usuario que adquirió por alguna vía la clave necesaria para poseer estos privilegios. Es por esto, entre otras causas, que limitar el número de usuarios con estos privilegios constituye un bastión en la seguridad de las redes. En la red de la División Territorial de ETECSA en Cienfuegos solo tienen este privilegio el personal de informática y algunos trabajadores que lo necesitan para el normal desempeño de sus actividades. No obstante, en ocasiones se ha configurado incorrectamente un número IP a alguna máquina por errores del personal de informática. De manera que tampoco es fácil mantener el orden en estas circunstancias si las medidas son solo organizativas.

Otras veces sucede que se descubre la acción de un posible intruso cuando ya ha pasado un tiempo prolongado desde la ocurrencia del hecho, por ejemplo, un mes. Entonces es realmente difícil probar que fue desde una estación de trabajo determinada, suponiendo que la acción se realizó con un identificador conocido. Más difícil es saber desde cuál local se conectó la PC si se tratara de un identificador no conocido.

De lo anterior se infiere que el problema se reduce a encontrar medidas técnicas o programas que logren ubicar con exactitud la relación en el tiempo entre los identificadores de PC y los locales donde están instaladas, además de prohibir la inserción de PC con nuevos identificadores en la red.

Esta rama en las redes de telecomunicaciones es conocida como "control en el acceso" porque el acceso significa el área donde se conecta el elemento final, receptor o transmisor de datos [3]. En cambio, el término "control de acceso" en informática suele relacionarse con los permisos o roles que en una aplicación o sistema puede tener determinado usuario o grupo de usuarios, sin importar dónde están vinculados trabajando. No obstante, es necesario tener en cuenta que en algunos textos se trata el término "control de acceso" con el primer significado referido.

El control en el acceso en redes LAN es una de las ramas a las que menos se le ha prestado atención en Cuba y en muchas partes del mundo [3]. Se carece de herramientas informáticas que hagan posible gestionar el control en el acceso en organizaciones donde se adquieren elementos de red como conmutadores y enrutadores de distintos fabricantes. Los conmutadores son el primer elemento por donde fluye el tráfico proveniente de una PC por lo que son esenciales a la hora de ejercer el control en el acceso sobre un ordenador. Cualquier solución de software tiene que interactuar con los conmutadores.

Administración del control en el acceso en redes LAN

En la actualidad existen pocos sistemas para la administración del control en el acceso en redes LAN. En ETECSA se utilizan, principalmente, dos de ellos: OpUtils y Observer. Estos se ocupan de la gestión de los dispositivos que se utilizan en la operación de la red, pero presentan algunas desventajas que impiden que estos sistemas se adecuen a las necesidades existentes en la Empresa entre las que se encuentran:

- Son sistemas propietarios
- Realizan el escaneo de forma manual, en vez de forma automática e indefinida
- Carecen de un registro histórico en el tiempo de la conexión y desconexión de un ordenador a la red
- No muestran la relación entre el puerto del conmutador y el local para la ubicación de un ordenador en la red

Mecanismos para implementar un control en el acceso de las estaciones a la red LAN alámbrica

Para la comunicación entre estaciones de una red LAN se emplean los identificadores de nivel de red (dirección IP) y los identificadores de nivel de enlace (dirección MAC — *Media Access Control*—). Para implementar una localización de estaciones es vital trabajar alrededor de la captura o control de estos números. Existen varias formas para implementar un control en el acceso en las redes LAN, entre ellas:

- Listas de Control de Acceso (ACL)
- Protocolo IEEE 802.1x
- Registro automático de las relaciones MAC contra puerto de conmutador y MAC contra IP con bloqueo del puerto usado por el intruso.

Para el sistema SIUDERLAN se utilizó la tercera forma de control en el acceso.

Es válido señalar que el registro automático de relaciones tiene como característica que debe ser implementado con la ayuda de un sistema informático, porque se trata de varias acciones que hoy no existen integradas en una sola solución informática.

Relación entre los identificadores MAC y los puertos del conmutador

Dentro de la memoria RAM de los conmutadores se almacenan los puertos y las direcciones MAC origen de las tramas que han pasado por ellos en los últimos minutos. Esa información tiene un carácter volátil por lo que debe ser accedida cada cierto tiempo por una aplicación y ubicada en una base de datos que registre correctamente el tiempo en que existen esas relaciones para que puedan ser consultadas de manera retroactiva. Esta acción es clave para garantizar que una estación pueda ser luego ubicada físicamente, ya que enlaza el identificador MAC de la estación con el puerto de un conmutador.

Relación entre las direcciones IP y los identificadores MAC

Evidentemente falta relacionar las direcciones MAC con las direcciones IP que poseen esas estaciones en cada momento, ya que la mayoría de las veces el número IP constituye el dato inicial en una búsqueda de infracciones. Existen dos métodos generales para encontrar esta relación. Esta clasificación obedece al nivel de injerencia en el tráfico de la red LAN: el método invasivo (o activo) y el método no invasivo (o pasivo).

Este último es el más efectivo para obtener la relación en el tiempo entre direcciones MAC y direcciones

IP ya que utiliza como fuente de datos las tablas ARP de los enrutadores. Estas tablas deben descargarse por medio de otra aplicación hacia una base de datos. Debe almacenarse también el tiempo en que se registran dichas relaciones.

Una vez registradas las relaciones MAC vs Puerto de conmutador vs IP vs Tiempo se puede responder a eventos complejos que se consideren anómalos, por ejemplo, si aparece una dirección MAC que no ha sido registrada en un periodo inicial de tiempo pudiera considerarse proveniente de un intruso. Las acciones que se tomen en consecuencia pueden ser varias como efectuar una alerta al administrador de red o ejecutar un bloqueo temporal por software del puerto por donde se avista dicha dirección MAC. De esa manera se está realizando un control en el acceso que combina flexibilidad y efectividad.

Mecanismos estándares para adquirir información de los conmutadores y enrutadores de distintos fabricantes

La adquisición de las relaciones entre direcciones MAC vs Puerto en los conmutadores y las relaciones entre direcciones IP vs MAC en los enrutadores puede ser obtenida de varias formas:

• Mediante las interfaces web de administración que habilitan los fabricantes para interactuar con los dispositivos.

• Mediante la interfaz en línea de comandos que habilitan los fabricantes.

• Mediante la lectura o escritura de variables utilizando el protocolo estándar SNMP [1].

El sistema SIUDERLAN emplea el protocolo SNMP para obtener de los conmutadores las relaciones MAC vs puerto y de los enrutadores las relaciones MAC vs IP.

Descripción del sistema SIUDERLAN

Para el diseño y desarrollo del sistema se utilizó la metodología RUP —*Rational Unified Process*— y el lenguaje de modelado UML —*Universal Markup Language*—. Dentro de las tecnologías de programación se utilizó el web framework Django [4] que está basado en el lenguaje multiplataforma y de propósito general Python [5]. Como gestor de base de datos se empleó PostgreSQL [6]. El sistema está concebido para que se utilice y redistribuya como código abierto. Puede instalarse sobre GNU/Linux o sobre Windows, aunque se enfoca en el primero, fundamentalmente, por las ventajas que ofrece el uso del software libre.

El SIUDERLAN consta de un proceso en ejecución permanente nombrado ***controller,*** un número de procesos llamados **agentes** que se encargan de interactuar con los elementos activos de red, una **interfaz web** para administración y explotación del sistema y una **base de datos** donde guarda las configuraciones y datos como los identificadores de las estaciones en el tiempo.

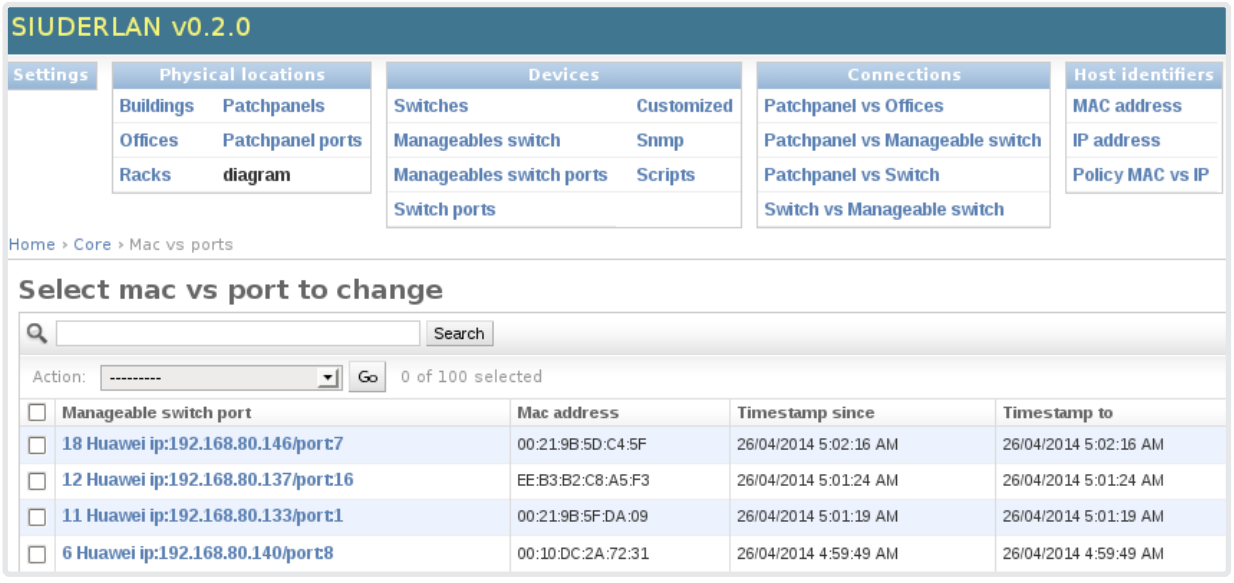

Figura 1. Sección de la interfaz web del sistema SIUDERLAN. (Fuente: elaboración propia).

A través de la interfaz web se realiza casi todo el trabajo, desde la configuración inicial o puesta a punto hasta las consultas para determinar la posición o ubicación de una estación en la red, determinada por su identificador MAC. En la figura 1 se observa una sección de dicha interfaz.

En la configuración inicial se deben definir los detalles del cableado como las edificaciones, los locales, puntos de red en los locales, bastidores, paneles de parcheo con sus puertos, las relaciones entre los puntos de red y los puertos del panel de parcheo, los conmutadores con sus puertos, las relaciones entre los puertos de los conmutadores y los puertos de los paneles de parcheo, etc. Toda esta configuración es vital para relacionar un puerto de conmutador con la localización física de una posible estación infractora.

Como los paneles de parcheo, locales, edificaciones, etc. son elementos pasivos hay que introducirlos al sistema de forma manual. Una opción para mitigar el trabajo en este caso sería distribuir la responsabilidad de la carga y actualización de la infraestructura al dar acceso a distintos administradores de subredes, utilizando un rol, para que introduzcan los datos correspondientes a sus edificaciones.

Por otra parte, se define inicialmente un número de agentes que se encargarán, de forma permanente, de extraer de los conmutadores las relaciones entre la MAC y el puerto de conmutador y de los enrutadores las relaciones MAC contra dirección IP. Esta búsqueda la realiza cada agente en un intervalo de tiempo que se puede establecer.

Cada agente es responsable de un número de conmutadores o enrutadores por lo que se hace un balance de la carga a fin de abarcar muchos elementos activos sin penalización de tiempo en correspondencia con la complejidad de la red donde se ejecute SIUDERLAN. Para una red de menos de 20 conmutadores y un enrutador pudiera bastar con un agente para recuperar la información del enrutador y otro para recuperar la información de todos los conmutadores.

Los agentes insertan la información en la base de datos donde queda establecida también la fecha y hora de la identificación. De esta forma se pueden crear consultas en intervalos de tiempo.

El SIUDERLAN tiene un periodo de aprendizaje donde acepta como válidas o de confianza a todas las direcciones MAC que transiten por la red. Después de ese periodo cada MAC distinta que se encuentre es reportada mediante avisos por correo electrónico o se bloquea el puerto del conmutador por donde transita. Esto último lo hace el agente que atiende el conmutador correspondiente. El puerto se bloquea por un periodo de tiempo y vuelve a activarse imitando las operaciones clásicas de bloqueo de cuentas.

Visto así, la MAC nueva sería el único criterio para declarar un intruso; sin embargo, si por otros sistemas (como IDS) se detectan actividades anómalas provenientes de un número IP determinado es posible localizar y bloquear dicha estación declarando como intrusa a la MAC correspondiente. Esto es viable gracias a las consultas que se hacen a las relaciones MAC contra IP almacenadas. El campo de acción del sistema radica en los identificadores de estaciones y el cableado para una efectiva localización física, no en otras funcionalidades como IDS, etc.

El sistema comprende el establecimiento de políticas donde se fijan direcciones IP a direcciones MAC y de violarse esta regla emite los avisos correspondientes.

Protocolos para la captura de datos

Los agentes pueden utilizar para su gestión tanto el protocolo SNMP —*Simple Network Management Protocol*— como un *script* personalizado, en cualquier lenguaje de programación, para cada modelo de elemento activo que no soporte la gestión SNMP. Este detalle hace al sistema superior a otros existentes. La clave está en que se normaliza el formato en que dicho *script* entrega la solicitud, por ejemplo, mac<espacio>puerto.

SIUDERLAN también ofrece la posibilidad de emplear conmutadores de distintos fabricantes. En la implementación realizada en la división territorial de ETECSA en Cienfuegos se utilizaron conmutadores y enrutadores de los fabricantes Huawei, Cisco y Allied Telesync.

Cuando los agentes encargados de los conmutadores trabajan por SNMP utilizan un juego de variables MIB —*Managenent Information Base*— nombrada BRIDGE-MIB. De este juego se utiliza la tabla Dot1dTpFdbTable (Tabla 1).

Cuando los agentes encargados de los enrutadores trabajan por SNMP para recuperar la relación MAC contra IP utilizan la MIB INTERFACE, específicamente el OID: ipNetToMediaPhysAddress (1.3.6.1.2.1.4.22.1.2).

OID	Descripción
dot1dTpFdbAddress	Dirección MAC.
dot1dTpFdbPort	Puerto asociado a la MAC anterior.

Tabla 1. Nodos terminales de la tabla Dot1dTpFdbTable. (Fuente: elaboración propia).

Resultados

Los resultados obtenidos con el sistema SIUDER-LAN desde la puesta en marcha de su última versión (0.2) en la División Territorial de ETECSA en Cienfuegos han sido muy alentadores. Entre otros logros se destacan los siguientes:

- Bloqueo de intrusiones
- Detección de invitados sin autorización previa
- Localización de estaciones extraviadas temporalmente
- Resolución de muchos conflictos IP
- Detección de *sniffers* en la red que ponen la tarjeta de red en modo promiscuo
- Observación de patrones donde una misma dirección MAC posee varias direcciones IP en intervalos muy cortos de tiempo

Conclusiones

Se diseñó y programó un sistema para ubicar físicamente (por locales o puestos de trabajo) y en el tiempo dónde están conectadas las estaciones de trabajo que forman parte de una red LAN. El sistema puede utilizarse para localizar posibles intrusos dentro la red y bloquearles el acceso automáticamente. También puede ser empleado para resolver problemas de conflicto de direcciones IP y, fundamentalmente, para dejar constancia de la ubicación de las estaciones de trabajo en el tiempo, posibilitando descifrar anomalías o eventos de seguridad ocurridos en el pasado.

Referencias bibliográficas

[1] Comer, Douglas E. Redes globales de información con internet y tcp/ip: New Jersey, Prentice Hall, 2000.

[2] Barrientos, Francisco J. Seguridad informática Ethical Hacking.Cornellá, Ediciones ENI, 2011.

[3] FreeNAC | Control de acceso a redes. http://freenac.net/es/solutions/lanaccesscontrol (acceso mayo 30, 2012).

[4] Django web framework. http://www.djangoproject.com (acceso abril 7, 2014).

[5] Python documentation. http://www.python.org (acceso enero 5, 2014).

[6] Postgresql. http://www.postgresql.org (acceso marzo 6, 2014).