Aplicación de control de puertos lógicos

Sockets Control Application

M. Sánchez-Monge, A. Sola, M. Oliva y M. Titos

Resumen

Cada día es mayor el número y el tipo de dispositivos que se conecta a una red y una red, amplia como la de una universidad no es una excepción. Por esta razón, el uso que se hace de ella también se ve incrementado, de la misma forma que crece la preocupación por parte de los administradores por su gestión y seguridad.

En el Centro de Tecnologías de la Información (CTI) de la Universidad de las Islas Baleares (UIB) se han desarrollado unos módulos de supervisión de la red con el fin de cubrir las distintas necesidades que este crecimiento nos supone. En esta línea, los últimos módulos desarrollados han sido la aplicación de control de puertos lógicos y una base de datos de integración global, que será el tema del que se trate en este artículo.

Palabras clave: TCP, UDP, puerto lógico, plataforma de gestión, sistema gestor de red, inventario de red, base de datos, BBDD, seguridad informática.

Summary

Nowadays, the number of network devices and their kind are increasing very fast and a campus network is not an exception. As a result of it, the amount of tasks that daily are carried out, taking benefit of the network advantages, grows as much as administrators worry about network security and management.

At the Centre of Information Technologies (CTI) of the University of the Balearic Islands (UIB) different network management modules have been developed with the purpose of solving the different problems that appear because of this network rise. A Sockets Control Application and a database are the last two modules developed at the Centre.

Keywords: TCP, UDP, socket, Network Management System, network inventory, database, computer security.

En el Centro de Tecnologías de la Información de la UIB se han desarrollado unos módulos de supervisión de la red con el fin de cubrir las distintas necesidades de su crecimiento

1.- Introducción

En el Centro de Tecnologías de la Información (CTI) de la Universidad de las Islas Baleares (UIB) se lleva trabajando durante los últimos años en un ambicioso proyecto que tiene por finalidad cubrir toda una serie de necesidades en materia de gestión de red y seguridad, generadas debido al crecimiento de la red de comunicaciones.

Aunque el mercado ofrece distintas soluciones para cada una de estas necesidades, se requería una solución integrada dentro de nuestra plataforma de gestión que permitiera cubrir todos los requisitos de forma centralizada.

El proyecto se ha desarrollado de forma modular, relacionando cada módulo con cada una de las diferentes necesidades. Los módulos que integran el proyecto son:

- Control de inactividad de puertos (MCIdeP, Módulo de Control de Inactividad de Puertos), o cómo detectar inactividad en las interfaces de los dispositivos de red con el fin de reciclarlas y evitar la adquisición innecesaria de otro nuevo equipo de red. Al darse de baja el acceso a puntos de red, también se pretende conseguir que los usuarios deban ponerse en contacto con el CTI para solicitar acceso a la misma y de esta forma poder inventariar a qué usuario pertenece cada máquina y punto de acceso.
- Control por dirección MAC (MCMAC, Módulo de Control por dirección MAC), o cómo saber en todo momento dónde está conectada una máquina dentro de la red.

El MCPL tiene como objetivo integrar la funcionalidad de control de puertos lógicos dentro de nuestra plataforma de gestión

- Control por dirección IP (MCIP, Módulo de Control por dirección IP), o cómo saber en cada instante a qué máquina pertenece cada IP. Ayudando a resolver, por ejemplo, los comunes "conflictos de IPs".
- Control de puertos lógicos TCP y UDP (MCPL, Módulo de Control de Puertos Lógicos), o cómo detectar si en algún dispositivo crítico de la red se ha abierto algún servicio no deseado o si algno que estaba funcionando ha caído, reduciendo al máximo el tiempo de detección de estos cambios.
- Repositorio centralizado de la información (BBDD, base de datos), o un lugar donde tener almacenada de forma concentrada toda la información relativa a la red y, especialmente, el inventario dinámico generado por los cuatro módulos mencionados.

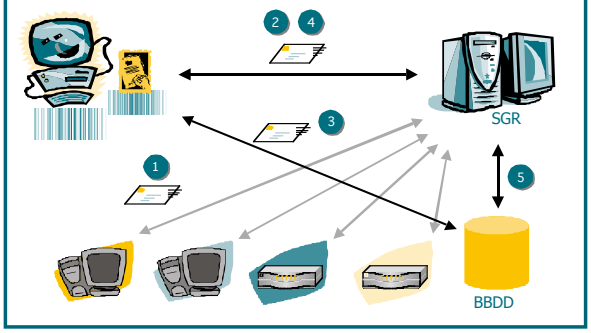
De los tres primeros módulos ya se habló en anteriores Jornadas Técnicas. En este número vamos a hablar del MCPL y de la BBDD que han sido los últimos módulos del proyecto global desarrollados.

2.- Módulo de Control de Puertos Lógicos (MCPL)

El MCPL tiene como objetivo integrar la funcionalidad de control de puertos lógicos, tanto TCP como UDP, dentro de nuestra plataforma de gestión (o sistema gestor de red, SGR).

Supongamos que se conecta a la red una máquina crítica con un servidor de HTTP y un servidor de FTP activados y que estos servicios se tienen configurados para mantenerse en escucha en los puertos TCP 80 y 21, respectivamente.

FIGURA 1.- ESQUEMA DE INTEGRACIÓN DEL MCLP



Ahora imaginemos que un usuario malicioso conoce una vulnerabilidad del servidor web, del servidor de transferencia de ficheros o bien, del propio sistema operativo utilizado y, de esa manera, consigue entrar en la máquina iniciando un nuevo servicio de Telnet que deja el puerto 23 TCP también a la escucha. Con el MCPL lo que se pretende es detectar la apertura de este nuevo puerto, distinto a los conocidos y configurados inicialmente por el administrador del equipo. El gestor de red detectaría una alarma en ese equipo a través de la plataforma de gestión pudiendo actuar en consecuencia; dando de baja el servicio de Telnet no deseado y realizando un análisis forense con el fin de determinar la causa que ha llevado a la apertura de este puerto.

Otra finalidad del MCPL es atender a la siguiente situación. Por ejemplo, supongamos que uno de los puertos de la máquina crítica, con un servicio a la escucha, cae. El MCPL debería detectar también la parada del servicio, generando una alarma. De este modo el gestor de red sería alertado de una manera inmediata, actuando de forma conforme y minimizando así el tiempo de respuesta.

El MCPL está formado por un *script* desarrollado en Bash, un intérprete de comandos Unix, cuya finalidad es la de comunicarse con el SGR.

El SGR es el encargado de obtener, vía SNMP (paso 1 de la figura 1), la información en tiempo real de los puertos lógicos que cada dispositivo de red tiene dentro del dominio de gestión. El MCPL a través del *script* programado cogerá esta información del SGR (paso 2) así como de la BBDD (el repositorio centralizado del proyecto global, paso 3). A continuación, comparará los puertos lógicos de cada dispositivo de red que le ofrece el SGR (los que tiene cada dispositivo en ese momento, en tiempo real) con la información que tiene la BBDD (los puertos que cada dispositivo debería mantener abiertos, configuración inicial).

El SGR es el encargado de obtener, vía SNMP, la información en tiempo real de los puertos lógicos que cada dispositivo de red tiene dentro del dominio de gestión

Tras la comparación de la información obtenida por las dos partes, el MCPL actualizará el SGR (paso 4) de forma que esté presente para cada dispositivo de red la información actualizada relativa a los puertos lógicos. Finalmente, en caso de ser necesario, se registraría la incidencia en la BBDD con la información obtenida (paso 5).

El trabajo llevado a cabo con el MCPL no comprende sólo la programación del *script*. El SGR utilizado es Spectrum de Aprisma, y la solución que, por defecto, ofrecía éste a nuestra necesidad de controlar los puertos lógicos no era suficiente. El SGR, a través del respectivo módulo de aplicación TCP o UDP de cada dispositivo gestionado, presentaba una tabla como la que figura a continuación (se muestra para el caso TCP, pero una tabla similar podríamos visualizar para el caso UDP).

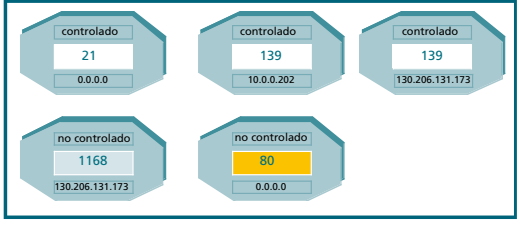
FIGURA 2.– TABLA DE CONEXIONES TCP SPECTRUM

El control de los puertos lógicos por parte del gestor de red para cada dispositivo, utilizando los recursos básicos que ofrece Spectrum, implicaba tener que ir a consultar cada tabla TCP y UDP de cada dispositivo de red. A continuación, bien mentalmente o comparando con otra tabla, el gestor debía deducir si existía algún puerto lógico abierto o cerrado que no fuera correcto.

Como resultado del desarrollo del MCPL, esta comparación de tablas de puertos se realizaría de manera automática, agilizando la actuación por parte del gestor de red a la hora de detectar problemas a nivel de puertos lógicos en los dispositivos gestionados.

Esto ha sido posible gracias a un rediseño del control de puertos lógicos dentro del SGR. Se ha mantenido la solución de Spectrum (relativa a la tabla de la figura anterior) y se ha aprovechado su potencia para el desarrollo de nuevas funcionalidades. Se ha creado un modelo de puerto lógico así como una vista que permite mostrar estos puertos, tanto TCP como UDP, de forma independiente, como si se trataran de dispositivos, tal y como se puede observar en la figura 3.

FIGURA 3.- PUERTOS MODELADOS COMO DISPOSITIVOS



En cada puerto se indica si se corresponde con un puerto controlado (de los que conoce el administrador de la máquina y que está inventariado en la BBDD) o si, por el contrario, es un puerto no controlado que para nada tendría que estar activo. Asimismo, se puede observar como también aparece el número de puerto del que se trata, así como de la interfaz de red a la que está asociado

El control de puertos lógicos se puede complementar mediante el uso de otras herramientas existentes en el mercado

dentro de esa máquina (ya que, por ejemplo, si se gestiona un PC, éste puede tener dos tarjetas de red y por tanto, dos interfaces con puertos lógicos asociados a cada una de ellas totalmente distintos).

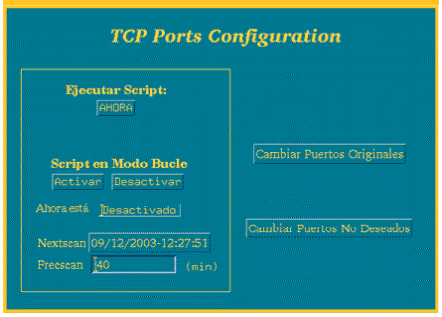
Según el puerto sea controlado o no, el código de colores que se utiliza indicará visualmente al gestor de red el tipo de problema con ese puerto. Además, se ha conseguido que la alarma también quede reflejada en la vista general del dominio de gestión, por lo cual, a través de esa vista, el gestor de red no sólo podrá ver si se ha perdido el *link* con un dispositivo (como se puede apreciar en la mayoría de los SGRs), sino también si ese dispositivo tiene algún problema con los puertos lógicos (característica particular de nuestro SGR gracias al MCPL).

Finalmente, hemos creado otra vista a través de la cual se configura, para cada dispositivo, la frecuencia con la que se debe ejecutar el *script* para esa máquina en concreto, ya que es el *script* el que mantiene activa la vista de puertos de la figura 3.

A través de esta segunda ventana se podrán actualizar los puertos lógicos o bien programar la ejecución del *script* para que, con la frecuencia que se considere necesaria, se mantenga actualizada de forma automática (opción recomendada).

Mediante esta vista, también se tendrá la opción de cambiar la configuración de servicios iniciales o controlados que tiene asignada una máquina mediante el acceso a la BBDD, así como, realizando también consultas a la misma, conocer qué puertos tiene actualmente abiertos este equipo y entrarían dentro de la categoría de no controlados.

FIGURA 4.– VISTA DE CONFIGURACIÓN DEL MCPL



El control de puertos lógicos se puede complementar mediante el uso de otras herramientas existentes en el mercado. El MCPL no es una solución separada de otras como un TCP-Wrapper, *firewalls* personales o escáners de puertos, sino que nos permite detectar, de forma más rápida, cualquier incursión a nivel de puertos lógicos que pudiera acontecer en nuestra red.

Con el MCPL se busca ante todo integración con nuestro SGR y una rápida detección de la violación y caída de un servicio, solución que no da ninguna de las tres herramientas mencionadas, no obstante:

- TCP-Wrapper permite configurar para qué IPs un puerto lógico puede ser accedido, lo cual es un filtro de seguridad adicional en nuestro sistema siempre deseable
- Los *Firewalls* personales, aunque no permiten saber si uno de los servicios ha caído y dependen del sistema operativo, permiten conocer qué aplicación hay detrás de una determinada conexión.
- Los escáneres de puertos permiten llevar a cabo un control más exhaustivo sobre la máquina crítica que ha sufrido un cambio de configuración en sus puertos.

3.- Base de Datos (BBDD)

El MCPL, al igual que los otros tres módulos que forman parte del proyecto global, se encuentra en continua comunicación con la BBDD ya que al generar una alarma en el SGR, sea por el módulo que sea, también automáticamente se está registrando la incidencia en la BBDD. El SGR se debe entender

como la situación actual, en tiempo real, del estado de la red, mientras que la BBDD almacena un histórico de todo movimiento acontecido, actual y pasado, de la red.

La base de datos nacía con dos funciones básicas: por una parte, solucionar la necesidad de almacenar toda la información relativa a la red de una manera automática, dinámica y centralizada y, por otra, alimentar al MCPL y los otros módulos que ya estaban en funcionamiento.

Como repositorio centralizado de información de la red, los datos que se almacenan en la base de datos son muy variados. Se guarda en ella toda la información acerca de usuarios, dispositivos, conexiones, direccionamiento IP e incidencias.

Para cada usuario se almacenan sus datos personales y, principalmente, los dispositivos de los que es responsable. Es importante conocer a los responsables de estos equipos ya que los módulos que se desarrollaron para complementar el SGR sólo analizan el tráfico de red, mientras que es necesaria una BBDD que aúna los datos de cada uno de los módulos y ayude a identificar al dispositivo implicado y al responsable del mismo, pasa resolver posibles incidencias.

En el apartado de dispositivos se guardan todos los elementos activos de la red y el equipamiento final de usuario. Por una parte, se almacena la información relativa a los modelos de estos dispositivos, como pueda ser información acerca de posibles composiciones entre modelos, características de funcionamiento o el número de interfaces. Para cada dispositivo individual, se generará una instancia en la BBDD, almacenando características imprescindibles para facilitar el control por parte del gestor de red, como son la dirección física, la dirección o direcciones IP que tenga configuradas, número, nombre y tipo de interfaces, VLAN a la que pertenece, ubicación física,…

En el apartado de dispositivos se guardan todos los elementos activos de la red, así como el equipamiento final de usuario

En relación a las conexiones se conocerá qué interfaces intervienen en la interconexión de los dispositivos, cuál es el medio utilizado en cada uno de los enlaces, así como el punto de red utilizado, en caso de estar utilizando un cableado estructurado.

La gestión de direccionamiento IP es también una parte del sistema desarrollado. Se debe conocer en todo momento qué dispositivo está utilizando una determinada dirección de red, así como conocer a qué rango pertenece y qué utilidad podemos darle. Además, el sistema facilitará el proceso de asignación de direcciones cuando se tenga un nuevo dispositivo y se quiera incluir en la red.

Finalmente, otra de las partes importantes de la BBDD es la relativa a la gestión de incidencias de red. En este módulo se deberá registrar cualquier cambio de funcionamiento, avería o problema que se haya detectado. Tendrá dos modos de alimentación, uno manual, en el que el operador de la aplicación introducirá los datos, y el modo dinámico y más importante ya que permitirá las actualizaciones dinámicas, en el que los datos serán introducidos automáticamente por el MCPL o cualquier otro módulo de los desarrollados.

Una incidencia podrá referirse a multitud de elementos, podrá implicar a un usuario, a un dispositivo, a una interfaz del mismo, a un puerto lógico, a un modelo determinado, a una dirección IP, a un armario de comunicaciones o incluso a un edificio.

Cuando una incidencia se registra en la base de datos, quedará en espera hasta que el gestor de red tome una decisión acerca de ella. Esta incidencia podrá ser una avería por solucionar o, simplemente, un cambio en la configuración de la red. En este último caso, la BBDD recopila automáticamente toda la información necesaria para actualizarse dinámicamente, es decir, se produciría una actualización del inventario de red sin la necesidad de que el operador introduzca los datos manualmente. Gracias a esta característica se consigue de una manera rápida, cómoda y eficaz mantener el inventario de red con la información en tiempo real.

Ahora se consigue una mejora en seguridad del sistema, ya que permite detectar de forma automática y centralizada un ataque que haya podido tener éxito con la consiguiente reducción del tiempo de respuesta

Recopilando la información pasada y presente obtenida de cada una de estas partes, la BBDD permitirá también la generación de informes, muy útiles para el administrador en un análisis forense.

4.- Conclusión

Gracias al desarrollo del Módulo de Control de Puertos Lógicos y de la Base de Datos se ha conseguido mejorar nuestro Sistema Gestor de Red, añadiendo funcionalidades que previamente no tenía, tales como la gestión de puertos lógicos, tanto TCP como UDP, y la gestión del inventario de red, muy importante a nivel del proyecto global.

Se consigue una mejora en seguridad del sistema, ya que permite detectar de forma automática y centralizada un ataque que haya podido tener éxito con la consiguiente reducción del tiempo de respuesta. Del mismo modo permite conocer de manera inmediata la caída de un puerto y, por tanto, de un servicio para poder recuperarlo rápidamente, obteniendo de esta forma una mayor fiabilidad del sistema.

Se automatizan muchas tareas que un gestor de red debe realizar, como puedan ser la generación y mantenimiento de inventarios de red, o la revisión de *logs* o tablas acerca del estado de los puertos de los dispositivos gestionados.

Finalmente, señalar que el resultado final de estos módulos ha sido el de complementar la plataforma de gestión, para operar sobre ella de una manera fácil y cómoda al uso y, lo más importante, dejar un diseño abierto a nuevas funcionalidades, tanto en el MCPL como en la BBDD.

Mª del Mar Sánchez-Monge Aleñar
(mar.sanchezm@uib.es)
Antonio Sola Venteo
(toni.sola@uib.es)
Maria Oliva Suárez
(maria.oliva@uib.es)
Miguel Titos Ramis
(miguel.titos@uib.es)
Centre de Tecnologies de la Informació
Universitat de les Illes Balears