Sistema de descubrimiento y control de equipamiento presente en redes

Leonardo de - Matteis – Karina Cenci – Jorge Ardenghi

Laboratorio de Investigación en Sistemas Distribuidos
Departamento de Ciencias e Ingeniería de la Computación
Universidad Nacional del Sur
{ldm,kmc,jra}@cs.uns.edu.ar

Resumen El trabajo del administrador de IT, específicamente en su rol de gestor de la red y de los equipos que configuran la infraestructura, se ve afectado por diversos factores que reducen el tiempo disponible para, por un lado, implementar políticas consistentes y con procedimientos predefinidos y, por el otro, para realizar los controles y verificaciones periódicas indispensables. En este contexto, el presente trabajo presenta una posible herramienta para mejorar la calidad de trabajo, la productividad y reducir los costos asociados, denominada *Si*stema de *De*scubrimiento y *Co*ntrol de *E*quipamiento (SIDECOE). A través de una arquitectura modular, utilizando una base de datos, mecanismos de monitoreo y de validación, este sistema permite ejecutar un conjunto de controles predefinidos y posibilita la identificación de errores y/o fallas de configuración de los equipos de una red y alerta a los administradores sobre los riesgos que de estas circunstancias se derivan.

Palabras claves: Redes de computadoras - Administración de redes - Gestión IT - Seguridad en redes - Monitor ARP - Validación de configuraciones

1. Introducción

En la actualidad, las funciones del administrador IT (Tecnología de la Información) son muy variadas y se percibe una importante sobrecarga de actividades relacionadas con la cantidad de elementos, aspectos y configuraciones que debe tener en cuenta durante la actividad laboral diaria. Si se consideran específicamente las tareas relacionadas a la administración de los equipos que conforman la infraestructura de una red, puede verificarse que en muchas organizaciones se producen situaciones en las que la implementación de las configuraciones resulta incompleta debido a los acotados tiempos disponibles para llevar a cabo las tareas. Es habitual que dichas tareas se programen en forma *ad hoc*, esto es, de manera poco precisa o que no se analicen adecuadamente, además de que con frecuencia no se verifican los trabajos realizados. También resulta un fenómeno común la inexistencia de procedimientos predefinidos para seguir, por ejemplo, en el caso de la inclusión de nuevos equipos en la red o bien frente a la necesidad de proceder a la actualización de equipos y a la posible rotación de los mismos.

La ampliación del equipamiento puede deberse a la incorporación de nuevo personal o a la implementación de nuevas funcionalidades a nivel de los servidores. En el caso de las incorporaciones de personal, se producen situaciones en las que los equipos reemplazados son asignados, a su vez, a otras personas dentro de la organización, quienes también pueden requerir al menos una pequeña mejora en sus equipos. Esto provoca la rotación de los equipos, proceso en el que pueden verse involucradas hasta 3 o 4 reasignaciones. Estas reasignaciones pueden (o no) provocar cambios en la configuración de servicios tales como DNS [10,11], DHCP [5,6] o RADIUS [13,9,2,1,4]. Asimismo, también es posible que los cambios ocurran en los servidores de VPN o en el equipamiento específico de la infraestructura de red, por ejemplo, en los conmutadores (*switches*), donde hay reglas de seguridad asociadas a sus diferentes bocas.

En el presente trabajo, se presenta el sistema SIDECOE (*Si*stema de *De*scubrimiento y *Co*ntrol de *E*quipamiento), una propuesta diseñada para mejorar la calidad de los trabajos y servicios asociados que los administradores de red de una organización prestan en diversas áreas o ubicaciones a sus usuarios finales, es decir, al personal en general. Sintéticamente, esta propuesta consiste en brindar a los administradores información sobre los equipos de la red, información que será registrada y estará disponible —para el caso de ser requerida— desde el preciso momento en que los equipos son conectados en la red de la organización, realizando una serie de chequeos prefijados que posibilitan descubrir errores o fallos en la configuración asignada a cada uno de ellos.

Los ejemplos siguientes permiten ilustrar, de manera sintética, el contexto en el que se inserta la propuesta desarrollada. Como primer caso, si un nuevo equipo fue configurado en la red, habiendo hecho el administrador de red una reserva de IP para la dirección MAC asociada a la tarjeta *Ethernet* pero no para la dirección MAC del dispositivo *Wifi*, SIDECOE avisa a los administradores de la situación detallando la siguiente información: que la dirección MAC del dispositivo *Wifi* no se encuentra con una reserva estática en el DHCP; que el equipo no cuenta con gestión centralizada del antivirus y, por último, que la entrada de DNS asociada al IP asignado no respeta las normativas de asignación de nombres de la organización.

Otro ejemplo es el de una organización que cuenta con un rango de reserva dinámico en el servidor DHCP para los equipos catalogados como visitantes. En este caso, el sistema notifica la existencia de equipos visitantes y el administrador puede corroborar, en cada momento de la jornada, qué equipos asociados a personal de visita están activos en la red. Con este tipo de información, el personal dedicado a la administración de la red y de la seguridad de la misma puede verificar si hay configuraciones no adecuadas, por ejemplo, de equipos para los cuales se hicieron reservas en el DHCP pero a los que no se les instaló el antivirus de la organización (con gestión centralizada). En este mismo escenario, también es posible verificar si se registran equipos con definiciones de nombres en el DNS que no se corresponden con su nombre actual, ya que la reserva del número de IP se pudo haber modificado en cuanto a la dirección MAC registrada y, en consecuencia, se asocia a una nueva sin haber asignado un nuevo registro A en el DNS y su correspondiente registro PTR.

La presentación de una propuesta capaz de dar estas y otras respuestas se organiza en este trabajo en cuatro secciones principales. En primer lugar, se mencionarán algunos antecedentes mientras que el núcleo central del trabajo lo constituye la sección dedicada a la descripción de la arquitectura seleccionada para el SIDECOE y los detalles de su implementación. Por último, en las conclusiones se apuntan algunas perspectivas para su desarrollo futuro.

2. Antecedentes

En la actualidad existen numerosos estudios, técnicas y propuestas asociadas a los diversos aspectos relacionados con la seguridad de las transmisiones en la red, que podemos resumir en las siguientes categorías:

- detección y/o prevención de problemas de ARP *spoofing*;
- detección y/o prevención de técnicas de envenenamiento ARP asociadas a ataques de tipo *Man-in-the-Middle* (MITM) ;
- mecanismos de control de acceso a la red;

Por otra parte, también existen productos comerciales que, en mayor o menor medida, proveen información recopilada a partir del análisis de los datos obtenidos a través de sensores en la red, los cuales mediante el monitoreo del protocolo ARP permiten descubrir y catalogar equipos. Entre estos productos podemos mencionar, a modo de ejemplo, el McAfee Policy Orchestator, una aplicación que permite no solo definir políticas sobre diversos tipos de *software* presentes en los equipos de la red, sino que también posibilita crear una infraestructura administrable en forma centralizada para controlar el despliegue de sensores y agentes de antivirus y HIDS, entre otros.

A diferencia de estos aportes, la propuesta formulada en este trabajo involucra otros aspectos que hacen a los objetivos planteados en la introducción, por lo que no podemos mostrar propuestas similares con las cuales contrastar características, ventajas o desventajas.

3. Arquitectura para SIDECOE

La arquitectura del sistema SIDECOE presenta módulos que se comunican entre sí, posibilitando el almacenamiento de datos surgidos de la inspección continua de una red IP. Los módulos que componen el sistema intercambian información entre sí, para poder brindar información relevante a sus usuarios mediante diversos mecanismos configurables de alerta.

A continuación se enumeran los principales módulos, para los que se detallan sus funciones principales:

- Módulo de descubrimiento
- Módulo de consultas
- Módulo de gestión
- Módulo de alertas

En primer lugar, el *módulo de descubrimiento* se encarga de gestionar la detección de los equipos que se conectan a la red, en tanto el método para dicha búsqueda consiste en el análisis de los mensajes del protocolo ARP. Cada equipo detectado recibe un identificador único que se le asocia y que está basado en la dirección MAC obtenida del análisis. Los datos del momento de la detección (fecha y hora), de la dirección MAC y del número de IP conforman los campos de los registros almacenados en una base de datos relacional, que permite posteriores consultas para el procesamiento y análisis de la información, tal como quedará ilustrado al describir el módulo de gestión. Por medio de agentes de instalación, este módulo, entonces, permite desplegar múltiples sensores de monitoreo en diversos equipos de la red, preferentemente en aquellos con el rol de servidores, para poder mejorar la detección de equipos.

Otra característica relevante de este módulo es que permite la detección de cambios tipo *flip-flop* sobre un par de direcciones MAC asociadas a una sola dirección IP. En muchas oportunidades, este dato no llega como información a los administradores de red, y es el principal aspecto a tener en cuenta cuando direcciones IP iguales se encuentran en diferentes adaptadores. En otras palabras, este dato por sí solo puede indicar fallos de la configuración o problemas en la seguridad interna.

Por su parte, el *módulo de consultas* provee diferentes interfaces para efectuar consultas en base a los datos asociados a los equipos detectados. Dichas interfaces permiten efectuar consultas a los servidores DHCP y DNS disponibles en la infraestructura de red de la organización. En el caso de la interface de consulta a un servidor DHCP (puede existir más de uno), esta permite verificar el tipo de concesión de dirección IP asignada al adaptador asociado a la dirección MAC descubierta. Estas concesiones pueden ser: *dinámicas* con tiempo de expiración, o bien *estáticas*, por reserva previa para la MAC involucrada.

Por otro lado, la interface de consulta sobre un servidor de DNS hace posible una doble verificación. En primer lugar, permite verificar los nombre(s) asociado(s) a una dirección de IP, esto es, reversa o registro PTR. Como contrapartida, una vez determinado(s) dicho(s) nombre(s), el sistema puede verificar la dirección IP asociada, es decir, la(s) inversa(s) respectiva(s), en este caso, registro(s) A. Esta doble verificación posibilita la identificación de potenciales discrepancias en la relación nombre-IP, que pueden deberse a la falta de mantenimiento y actualización de los datos del DNS, circunstancias que, a su vez y según ya se ha señalado, pueden haberse originado por reasignación de equipos entre el personal de la organización.

Sobre la base de su dirección IP, por último, el módulo de consultas también proporciona un servicio para determinar si en un determinado equipo se está ejecutando el agente del servicio centralizado de antivirus de la organización (por ejemplo, agentes de McAfee ePolicy Orchestator).

El tercer módulo, el *módulo de gestión*, constituye el elemento principal de la arquitectura, pues tras consultar a otros servidores de la infraestructura, instrumenta el procesamiento de esta información y la obtenida por el módulo de descubrimiento y toma las decisiones finales de la información que debe ser remitida a los usuarios del sistema a través de notificaciones que envía al módulo de alertas.

Este último módulo, el *módulo de alertas*, permite definir diferentes mecanismos de notificación a los usuarios del sistema. En función de las necesidades operativas, se puede configurar cuáles de dichos usuarios deben o no recibir notificaciones por correo electrónico, pudiendo especificar los diversos tipos de periodicidad (las posibilidades son: inmediata, diaria, semanal o mensual).

Además, las alertas se registran por defecto como sucesos del sistema y todas ellas pueden observarse a través de una interface web que provee el sistema lo que, mediante avisos visuales, permite al usuario identificar la información relevante referida a los eventos recientes, a los eventos sin atender (es decir, sin aceptación y rechazo) así como a otras alertas en general.

En la figura 1, pueden apreciarse las relaciones jerárquicas entre los componentes lógicos del sistema. Como medio de almacenamiento permanente se utiliza una base de datos (BD) de tipo relacional, donde se almacenan los datos obtenidos y algunos parámetros de configuración. Entre los datos almacenables pueden mencionarse, en primer lugar, todos aquellos obtenidos por el módulo de descubrimiento, pero también otros que el sistema genera durante su funcionamiento, como por ejemplo:

- relaciones establecidas entre direcciones MAC y direcciones IP,

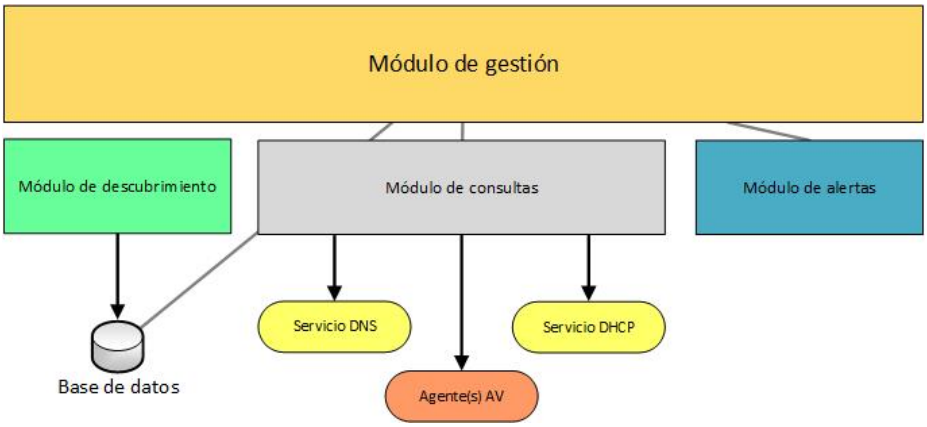

Figura 1. Componentes lógicos del sistema

- entre direcciones IP y nombres de equipos,
- datos de configuración de alertas,
- alertas emitidas.

4. Implementación

La implementación e instalación principal de SIDECOE se realiza sobre sistema operativo GNU/Linux. Los módulos de gestión y de alertas están programados en lenguaje C. Sobre la base de los equipos descubiertos, el módulo de gestión lleva a cabo consultas a los servidores de DNS y DHCP, para así poder ejecutar chequeos predefinidos en busca de errores o fallos en las configuraciones realizadas por el administrador de la red. Por otra parte, el módulo de gestión también puede invocar programas auxiliares, por ejemplo, para verificar si en un determinado equipo se encuentra instalado el agente del antivirus con gestión centralizada de la organización. En particular, se utiliza *Nmap Scripting Engine* para verificar la presencia del agente del producto *ePolicy Orchestator* de McAfee/Intel Security [7,8].

El módulo de alertas lleva a cabo las consultas SQL sobre una base de datos MySQL, en la que el módulo de descubrimiento almacena información en forma centralizada sobre la base de la información que recibe de los diversos sensores. Como puede observarse, en la arquitectura planteada se define una única BD pero los sensores están distribuidos en diferentes equipos (preferentemente servidores) para incrementar y mejorar las detecciones.

El módulo de descubrimiento está conformado por un conjunto de *scripts* (en lenguaje PHP) y programas (binarios). Entre ellos, el más importante es el agente de instalación de los sensores, que según el sistema operativo despliega monitores de ARP compilados para ejecutarse en distribuciones GNU/Linux, o bien en sistemas operativos Microsoft Windows. El despliegue se realiza autenticando en el sistema operativo remoto y luego, según el caso, copiando los archivos necesarios. Actualmente, como monitor ARP se utiliza el programa `arpwatch` en entornos GNU/Linux, que mediante *scripts* complementarios permite almacenar los datos obtenidos en una base de datos,

más allá de su funcionamiento normal de registro de sucesos vía *syslog* y notificaciones por correo electrónico.

5. Conclusiones

En la realidad cotidiana del trabajo de administración de redes, el personal se ve superado con frecuencia por la falta de definición de uno o varios de los siguientes aspectos: políticas, planes, instrucciones y verificaciones. A ellos se suman otros factores preponderantes como la falta de tiempo, la cantidad suficiente de personal y el escaso presupuesto para poder realizar trabajos más prolijos y adecuados. Ante este tipo de escenarios, la propuesta descripta del SIDECOE se plantea como objetivo formular una intervención práctica para mejorar la calidad de los servicios que los administradores de red prestan a los usuarios. Esta intervención se basa en la comunicación de situaciones que se identifican a partir de la ejecución de procesos de chequeo prefijados, que posibilitan descubrir errores o fallos en la configuración de los equipos de la red de trabajo en una organización.

La arquitectura planteada en este trabajo constituye una solución práctica que permite señalar a los administradores aquellas incongruencias o errores en la configuración de servicios vinculadas a la infraestructura de soporte de la red que pueden conducir a la detección de problemas o al hallazgo de incongruencias que hagan necesarias tanto correcciones posteriores como revisiones y reinstalaciones generales, tanto del equipamiento en la red como de sus servicios. Es evidente que estas circunstancias no solo pueden provocar reclamos posteriores por parte de los usuarios sino también la disminución de la productividad de la organización un incremento considerable de sus costos.

Como futuros desarrollos de esta propuesta se prevé realizar extensiones para incluir el despliegue de sensores de monitoreo en sistemas operativos Microsoft Windows, mediante el mecanismo clásico de autenticación con credenciales adecuadas y despliegue del *software* relacionado, que deberá ejecutarse como un servicio.

Asimismo, se analiza hacer las ampliaciones de la arquitectura que permitan realizar chequeos de los equipos detectados en la red y su presencia o no en servidores RADIUS (*Remote Authentication Dial In User Service*), ya que en la actualidad muchas organizaciones poseen conmutadores (*switches*) donde se chequean los permisos para conectarse por parte de los equipos utilizando la norma estándar IEEE 802.1x con EAP. De esta manera, estos conmutadores pueden detectar equipos no previstos que pueden pertenecer a personal no autorizado y que están tratando de conectarse, pudiendo derivar situaciones de este tipo en ataques desde la red interna. En este sentido, la intención futura es confeccionar, en cambio, un mecanismo *genérico* de alertas, a partir de la detección y chequeo de la base de datos asociada al servidor RADIUS, más allá de que muchos equipos poseen sus propios mecanismos de registro de sucesos internos o externos (en este último caso, a través del almacenamiento de los detalles de conexiones en servidores *syslog*).

Una última posibilidad de desarrollo posterior consiste en la inclusión de mecanismos de detección de *spoofing* [3,14,15,12], para lo que se cuenta con abundante literatura, de tal manera que resulta factible implementar alguno de ellos a corto plazo para complementar aspectos que hacen a la seguridad informática interna de la organización.

Referencias

1. B. Aboba and P. Calhoun. RADIUS Support for Extensible Authentication Protocol (EAP). Technical report, IETF, Sep 2003.
2. B. Aboba, G. Zorn, and D. Mitton. Radius and ipv6. Technical report, IETF, Aug 2001.
3. Mohamed Al-Hemairy, Saad Amin, and Zouheir Trabelsi. Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks. In *Current Trends in Information Technology (CTIT), 2009 International Conference on the*, pages 1–6. IEEE, 2009.
4. P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese. IEEE 802.1x remote Authentication Dial In User Service (RADIUS) Usage guidelines. Technical report, IETF, Sep 2003.
5. R. Droms. Dynamic Host Configuration Protocol (DHCP). Technical report, IETF, Mar 1997.
6. R. Droms, J. Bound, B. Volz, T. Lemon, and C. Perkins. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Technical report, IETF, Jul 2003.
7. McAfee, Inc. *Installation Guide. McAfee ePolicy Orchestrator 5 Software*, 2013.
8. McAfee, Inc. *Product Guide. McAfee ePolicy Orchestrator 5 Software*, 2013.
9. D. Mitton. Network access servers requirements: Extended RADIUS practices. Technical report, IETF, Jul 2000.
10. P. Mockapetris. Domain names. Concepts and facilities. Technical report, IETF, Nov 1987.
11. P. Mockapetris. Domain names. Implementation and specification. Technical report, IETF, Nov 1987.
12. Vivek Ramachandran and Sukumar Nandi. Detecting ARP spoofing: An active technique. In *Information Systems Security*, pages 239–250. Springer, 2005.
13. C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). Technical report, IETF, Jun 2000.
14. Robert Wagner. Address resolution protocol spoofing and man-in-the-middle attacks. *The SANS Institute*, 2001.
15. Sean Whalen. An introduction to ARP spoofing. *Node99 [Online Document], April*, 2001.