Rediseño E Implementación De Herramientas Informáticas Para La Auditoria De Sistemas En Red

Ciolli María Elena, Porchietto Claudio, Rossi Roberto
Grupo de Investigación Instituto Universitario Aeronáutico
Córdoba, Argentina

Resumen. *Esta ponencia presenta el resultado del análisis e implementación de herramientas para el control remoto del hardware y software de una red informática. Tras un análisis comparativo basado en la conceptualización GLPI (gestión libre del parque informático) y en la norma ISO 27002 dominio 7 (gestión de activos) sección 7.1 (inventario de activos) entre dos plataformas: OCS Inventory NG [1] y Open Audit [2], se concluyó que la segunda plataforma es la que más se adecua a los objetivos planteados [3]. Sin embargo también reveló que no satisface dichos objetivos en su totalidad, por lo que fue necesario reprogramar su código fuente corrigiendo errores y agregando nuevas funciones tales como detección de intrusos con NMAP, centralizado de configuración, Autenticación de scripts de auditoria, formularios en HTML5, etc.*

A través del presente trabajo se pretende mostrar la experiencia, los resultados y los motivos por los que se sigue trabajando en la herramienta Open Audit luego de haberla desplegado a la red interna del Instituto Universitario Aeronáutico. El mismo cuenta con un plantel de más de 1000 máquinas, repartidas entre las distintas dependencias del Instituto Universitario Aeronáutico (IUA), en su sede central y centros de apoyo de Rosario y Buenos Aires. El despliegue se realizó a través de los dominios internos, fuera de áreas críticas, sobre un total de 70 hosts auditados. Este desarrollo fue hecho sobre máquinas basadas sobre entorno Windows, por lo que se continúa la experimentación de auditorías sobre host fuera de dominio o intrusos.

Palabras clave: Open Audit, GLPI, Auditoria, Monitoreo, NMAP.

INTRODUCCIÓN

Los distintos entes que intervienen en una auditoría son:

- Estaciones de trabajo.
- Auditor.
- Informe o reporte.
- Base de datos.
- Estación para el análisis de datos.
- Lista de procedimientos.

Este modelo pese a ser muy rudimentario y simplista, nos ayuda a contextualizar el origen de nuestro trabajo.

El rol del auditor lo encarna una persona física. El informe o reporte obtenido, es transportado en un medio físico y la base de datos la constituye una PC donde se guardan los informes [4] [5]. Todo esto se ejecuta en base a unos procedimientos internos estandarizados y normalizados.

Como resulta evidente, es muy ardua la tarea de tener actualizada dicha base de datos, por lo que resulta imprescindible la investigación, el desarrollo y la implementación de un software que permita el control automático y la generación y actualización de reportes [6] del parque informático, mediante supervisión de la base de datos.

El esquema concebido está centrado en la auditoría de las máquinas que pertenecen a una red determinada. Todas las máquinas pueden contactarse con un servidor. A priori esta red se encuentra segmentada, contando con diferentes dominios, sistemas operativos y usuarios. De más está decir que una herramienta de auditoría es netamente un sistema distribuido en toda la red.

¿Cómo funciona Open Audit para auditar un dominio determinado?

La figura 1 muestra un esquema general de auditoría de dominio con la herramienta Open Audit.

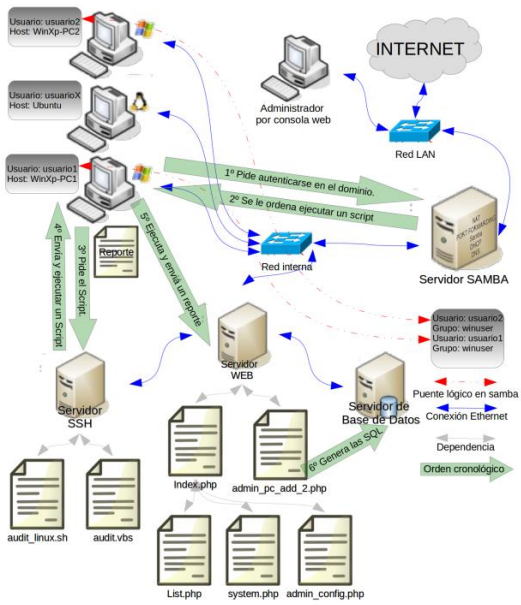

Figura 1 - Auditoria de dominio

Al iniciar sesión los usuarios del dominio se registran ante el PDC (controlador primario de dominio). En este caso particular es implementado por un servidor Samba, que instruye a ejecutar el Script de auditoría a las estaciones de trabajo. Dependiendo del sistema operativo el Script es diferente [7] [8] pero su reporte está estandarizado.

El Script para Linux está compuesto de una serie de sentencias de consola cuya salida es analizada, clasificada y segmentada por herramientas para procesar texto como awk.

En Windows se utiliza un Script semejante al de Linux que está codificado en Visual Basic Script y basado en instrucciones de WMI Service (Windows Management Instrumentation).

¿Cómo funciona Open Audit para auditar máquinas fuera del dominio?

Un servidor con un método de Polling [9] es el encargado de enviar el auditor. En la figura 2 se observa que aunque el segundo proceso de distribución parece más simple, no lo es, ya que es necesario cargar máquina por máquina en una lista con sus correspondientes nombres de usuario con privilegios de administrador.

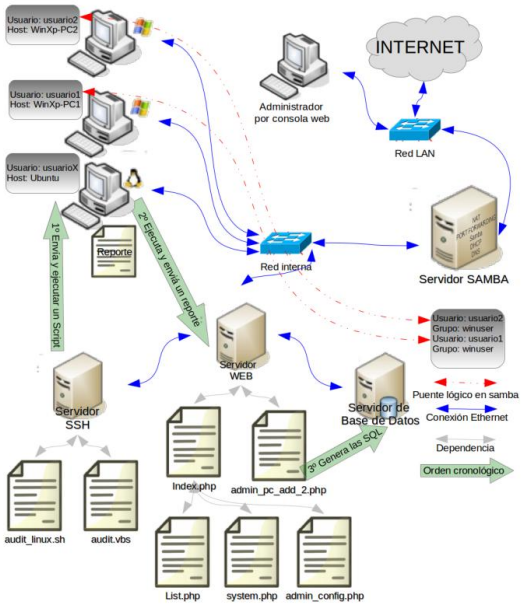

Figura 2 - Auditoria fuera del dominio

Todo esto conlleva a la necesidad de tener una gestión distribuida en la red y no concentrada.

¿Cómo almacenan la información?

Ambos Scripts guardan en cadenas de texto la información extraída que contiene un identificador de cabecera y caracteres especiales como separador de campos. Estas cadenas son almacenadas temporalmente en un archivo de texto (reporte) cuyo nombre es el de la máquina auditada. Una vez realizadas todas las consultas, el archivo de reporte es enviado vía html, previa autenticación, al servidor del Open Audit que se encarga de cargar los datos en el servidor de base de datos.

¿Cómo se genera un reporte del estado general de la red?

En la figura 3 se aprecia cómo es el flujo de información a la hora de realizar una consulta. No es necesario que las máquinas auditadas estén en línea al momento de realizar la consulta. Esto cumple con la disponibilidad de datos pedida por la normativa [10] [11] [6].

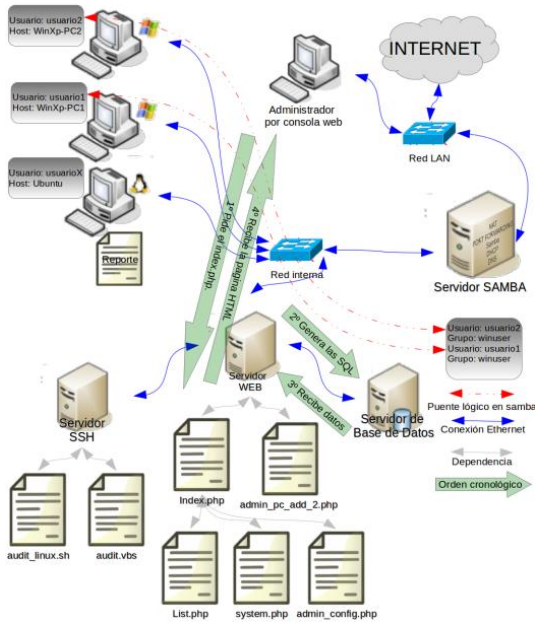

Figura 3 - Consulta generica

En concordancia con el modelo pre sistema, el rol del auditor es cambiado de una persona física a un Script, el reporte que se trasladaba y almacenaba manualmente ahora lo hace a través de la red LAN interna cuyo único requerimiento es que brinde conectividad entre las estaciones de trabajo y el servidor del Open Audit.

Los procedimientos estandarizados están almacenados en el controlador de dominio que es quien va a decidir qué máquinas son auditadas y cuándo. Para el caso de máquinas que no pertenecen a ningún dominio pero sí son parte de la zona auditada, el servidor de Open Audit efectúa una conexión mediante SSH con cada uno de los hosts que estén registrados.

¿Qué sucede con los Host intrusos?

Al no estar blindada la red, los usuarios pueden conectarse a la misma con sus ordenadores personales. Esto sucede por un tema de flexibilidad, ya que muchos usuarios quieren compartir archivos entre sus ordenadores y los ordenadores que se encuentran en la zona auditada.

Todos los hosts que no están en la lista de auditoría o se autentican contra un controlador de dominios o son considerados intrusos [12].

Los mismos si no son auditados presentan un riesgo para la seguridad de la red.

Una solución a esta situación fue integrar la herramienta Nmap a la suite de Open Audit. Con ella se puede detectar los hosts que están conectados a la red, todos ellos. A los mismos se les extrae información como la dirección MAC, la dirección IP, y el nombre de host. Estos datos son comparados en el servidor de Open Audit con la lista de estaciones de trabajo auditadas y de no corresponder a ninguna se los almacena como "host no auditado" representando una alerta de seguridad.

En la figura 4 se puede apreciar cómo es insertado el servidor Nmap al esquema de funcionamiento de la red.

Como en los casos anteriores en la implementación realizada en la zona auditada, el servidor de Nmap está implementado sobre el mismo servidor físico donde se encuentra instalado el Open Audit así como el servidor MySQL.

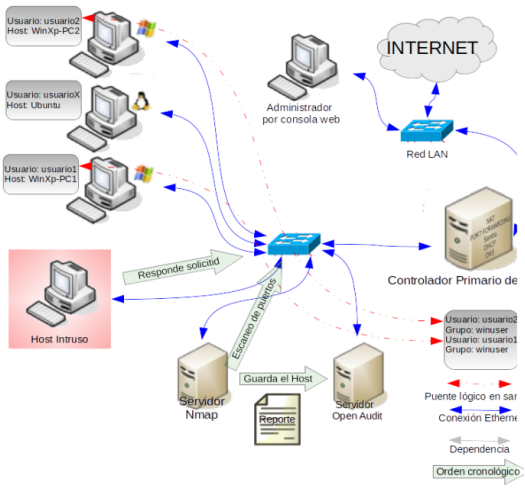

Figura 4 - Nmap

Gracias a la adición de Nmap al esquema de auditoría se puede tener un control más estricto del total de máquinas reales que contiene la red momento a momento. A pesar de ello no es todavía posible auditar los host intrusos.

METODOLOGÍA

En base a los resultados de las pruebas efectuadas, la herramienta Open Audit resultó seleccionada como plataforma base para continuar con el desarrollo en curso, tras la comparación cuantitativa de las auditorías realizadas.

Para cuantificar las plataformas se tomó como referencia la fidelidad de los datos, el volumen de tráfico de red y las facilidades que brinda la herramienta para poder ser desplegada. Todo esto fue introducido en la tabla 1 acompañado por un cuantificador de importancia dando como resultado una puntuación fácilmente comparable.

Cada elemento a auditar en el entorno de evaluación de la herramienta, posee características documentadas que sirven como base de comparación con las extraídas por el auditor. En base a cuan fiel es cada auditoria se le otorga un valor entre 1 y 5.

No todos los elementos auditables tienen el mismo grado de importancia. Conocer el número de serie de un ratón no es tan relevante como el de un disco duro o el de un software con licencia. Por ende es necesaria la introducción de una columna que pondere los valores de fidelidad. Los valores de dicha columna son arbitrarios y elegidos por un administrador de la red, ya que su experiencia valida su magnitud.

Finalmente la calificación está conformada como la suma del todos los valores de fidelidad ponderados. El rango se sitúa entre 88 y 17. Open Audit obtuvo 71.2, 70.2 y 63.8 en Windows XP, Windows 7 y Ubuntu respectivamente contra 68.2, 65 y 49.8 de OCS Inventory en el mismo orden.

El mismo método fue utilizado para controlar el avance de la plataforma Open Audit. Los nuevos resultados obtenidos se situaron en 78.8, 77.8, 66.0 y 69 para Windows XP, Windows 7, Ubuntu 14.04 y Windows 8.

Este método de cuantificación no contempla mejoras introducidas a la herramienta como la detección de intrusos. No obstante los cambios en el indicador garantizan que la herramienta está en proceso de evolución.

RESULTADOS

De la información recogida en la prueba y muestra efectuada, el total de estaciones de trabajo fueron de 91 y el total de servidores de dominio 3.

En la figura 5 se aprecia la estructura de red.

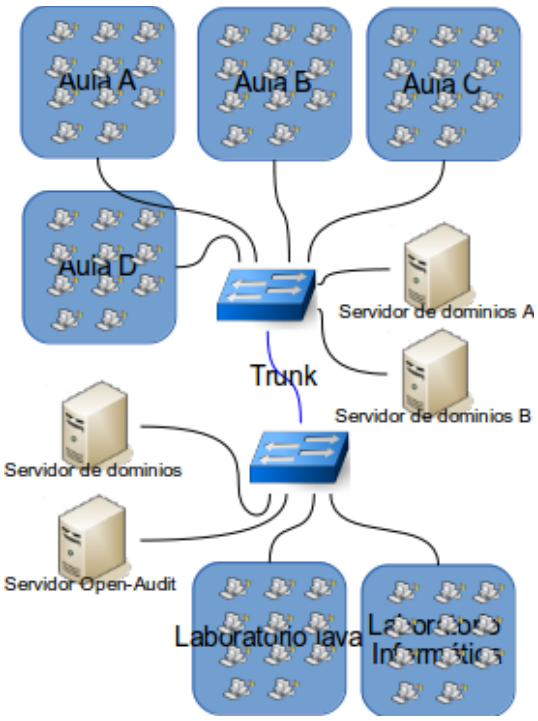

Figura 5 - Dominios donde se desplegó Open Audit

En el tiempo de prueba el sistema logró auditar 86 estaciones de trabajo y los tres servidores. Las restantes PC no se auditaron por no haber iniciado sesión en el dominio en el tiempo que lleva en funcionamiento el servidor.

Además se localizaron un total de 21 Host intrusos gracias a Nmap. Es de aclarar que todo dispositivo de red es detectado por un escaneo de puertos, tanto routers, como switchs administrables, etc. No obstante estos dispositivos de red no representan un problema para el sistema, dado que se le reporta la detección al administrador una vez y luego se procede a ignorarlos.

En cuanto a la performance del servidor, en la figura 6 se presenta un histograma del consumo de memoria y espacio libre en disco.

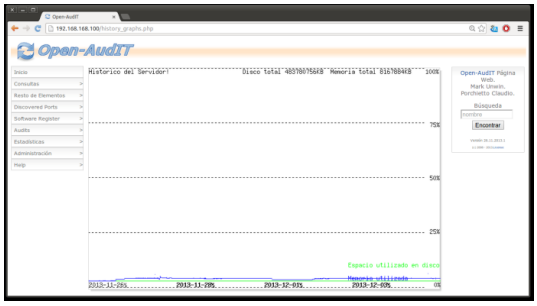

Figura 6 - Histograma

El impacto en el hardware es prácticamente inapreciable para el total de 91 estaciones de trabajo, lo que nos alienta a desplegarlo en un dominio de mayor dimensión. Los impactos en el hardware del servidor y en la red cableada son ínfimos comparados con el tráfico que genera el inicio de sesión en dominio de Windows.

El Sistema funciona sobre redes LAN, siendo posible su aplicación en redes WAN, pero en este caso es necesario modificar su estructura para tal integración.

Las figuras 7, 8, 9 y 10 presentan las distintas interfaces desplegadas por la herramienta.

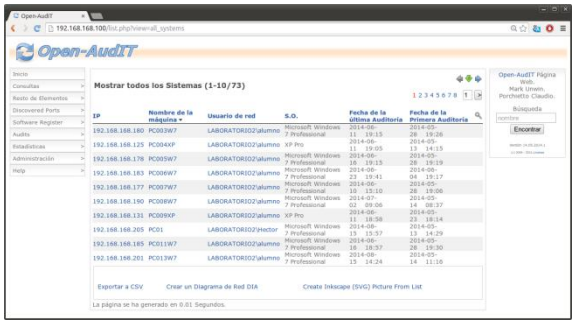

Figura 7 - Todos los Sistemas Auditados.

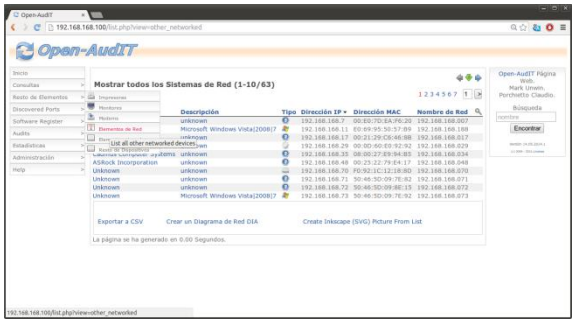

Figura 8 - Hosts descubiertos por Nmap.

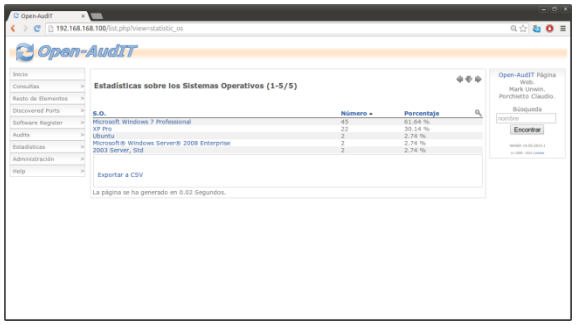

Figura 9 - Estadísticas sistema Operativo.

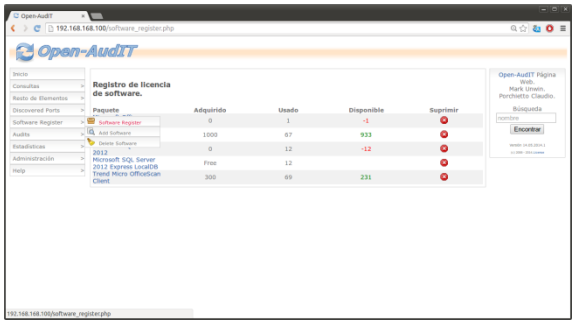

Figura 10 - Seguimiento de Software.

CONCLUSIONES

Con las mejoras realizadas a la suite Open Audit tanto en la depuración de los agentes auditores como en la integración con Nmap, se puede garantizar que el plantel de estaciones de trabajo se encuentra monitoreado de forma permanente, alertando ante la posible remoción de algún hardware en los equipos que se encuentren en la zona auditada como así también ante la instalación de nuevo software no autorizado. Además cualquier host conectado a la red es detectado procesado y notificado si no está auditado.

TRABAJOS FUTUROS

Actualmente se está trabajando en forzar la auditoría de las estaciones de trabajo que no están en un dominio ni en una lista, o sea los “hosts intrusos”. Esta nueva etapa es presentada como “Sistema de control de acceso discriminado para estaciones móviles”.

Es habitual que los usuarios de la red tengan sus propias estaciones móviles. Además estos quieren compartir archivos entre sus estaciones móviles y las estaciones de la institución. Es por ello que dichas estaciones ponen en riesgo la red si no son auditadas periódicamente.

Se está implementado un prototipo de Access Point (AP) WI-FI en el que se discrimine dispositivos de usuarios públicos y usuarios privados. De este modo el equipamiento móvil de los usuarios perteneciente a los usuarios con privilegios en la red puede acceder a la red cableada privada y los usuarios sin privilegios o invitados pueden tener acceso a una red pública. El usuario que desee conectarse a la red interna se deberá dar de alta ante el AP. En ese momento el AP comprobará que se ejecute el agente de auditoría.

Referencias

[1] MODx. (2013, Aug.) www.ocsinventory-ng.org. [Online]. http://www.ocsinventory-ng.org/en/

[2] Mark Unwin. (2013, May) open-audit.org. [Online]. http://www.open-audit.org/

[3] Porchietto Claudio. (2013, Oct.) www.unpl.edu.ar. [Online]. http://sedici.unlp.edu.ar/bitstream/handle/10915/31337/Documento_completo.pdf?sequence=1

[4] Jose Antonio Echenique Garcia, *Auditoria en Informática*.: Méjico - McGraw Hill, 2001.

[5] Chris Jackson, *Network Security Auditing*, Primera ed.: Cisco Press, 2010.

[6] Agustín López Neira. (2013, Oct.) www.iso27000.es. [Online]. http://iso27000.es/

[7] Mario Piattini Velthuis, *Auditoria de Tecnología y Sistemas de Información*, Primera ed.: Alfaomega, 2008.

[8] Abe Fettig, *Twisted Network Programming Essentials*, Segunda ed.: O'Reilly, 2013.

[9] Chris McNab, *Network Security Assessment: Know Your Network*, Segunda ed.: O'Reilly Media, 2007.

[10] Sarahol. (2013, Nov.) /www.17799.com. [Online]. http://www.17799.com/

[11] 123 Innovation Group, S.L. Auditoria Sistemas. [Online]. http://auditoriasistemas.com/estandares-ti/

[12] Jean-Philippe Martin-Flatin, *Web Based Management of IP Networks & Systems*, Primera ed.: Wiley, 2002.

[13] 123 Innovation Group S.L.. (2014, Mar.) auditoriasistemas. [Online]. http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/

[14] Barzan "Tony" Antal, *It Inventory and Resource Management with Ocs Inventory Ng 1.02*, 102nd ed., Barzan "Tony" Antal, Ed.: Packt Publishing , 2010.

ANEXO

Herramienta / *Atributo*	*Valoración de Importancia*	*OCS inventory Windows xp*		*OCS inventory Windows 7*		*OCS inventory Ubuntu*		*Open Audit Windows xp*		*Open Audit Windows 7*		*Open Audit Ubuntu*	
Software de base con licencia - Sistema Operativo	5	5	5	4	4		0	5	5	4	4		0
Actualizaciones de Sistema Operativo	3	5	3	5	3	5	3	5	3	5	3	5	3
Software de aplicaciones con licencia	5	4	4	4	4		0	5	5	5	5		0
Antivirus	4	4	3,2	4	3,2		0	5	4	5	4		0
Software gratuito	4		0		0	5	4		0		0	5	4
Inventario de Hardware			0		0		0		0		0		0
Motherboard	5	2	2	2	2	2	2	4	4	4	4	4	4
Procesadores	5	4	4	4	4	4	4	5	5	5	5	5	5
Memoria	5	4	4	4	4	4	4	4	4	4	4	4	4
Almacenamiento físico HDD	5	5	5	4	4	5	5	4	4	4	4	5	5
Almacenamiento físico (CD, pen, etc)	5	4	4	4	4	4	4	4	4	4	4	3	3
Almacenamiento lógico	5	5	5	5	5	5	5	5	5	5	5	5	5
Video	5	3	3	3	3	3	3	3	3	3	3	3	3
Sonido	3	3	1,8	3	1,8	3	1,8	3	1,8	3	1,8	3	1,8
Red	5	5	5	5	5	5	5	5	5	5	5	5	5
BIOS	5	4	4	4	4	4	4	4	4	4	4	5	5
Monitor	4	5	4	5	4	1	0,8	5	4	5	4	5	4
Dispositivos de entrada.	3	4	2,4	4	2,4	2	1,2	4	2,4	4	2,4	4	2,4
Impresoras	4	4	3,2	4	3,2		0	2	1,6	2	1,6	4	3,2
Impacto en red			0		0		0		0		0		0
Volumen de tráfico en la auditoría	4	3	2,4	3	2,4		0	3	2,4	3	2,4	3	2,4
Volumen de tráfico en el despliegue	1	1	0,2	1	0,2		0	5	1	5	1	5	1
Facilidades			0		0		0		0		0		0
Desligue	3	5	3	3	1,8	5	3	5	3	5	3	5	3
TOTAL			68,2		65		49,8		71,2		70,2		63,8

Tabla 1 - Tabla de valoraciones