Monitoreo remoto de sistemas y redes para la auditoria informática

María Elena Ciolli, Claudio Porchietto, Roberto Rossi, Juan Sapolski

Grupo de Investigación Instituto Universitario Aeronáutico, Córdoba, Argentina
{mciolli,porchietto,roberto.rossi}@gmail.com

Resumen. Esta ponencia presenta el resultado del análisis e implementación de herramientas para el control remoto del hardware y software de una red informática 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). Se realizó un estudio comparativo entre dos herramientas: OCS Inventory NG y Open Audit. Se tomaron como factores claves la identificación unívoca de hardware y el software del parque informático y asimismo se consideraron relevantes: el impacto en el tráfico de la red, las facilidades de las herramientas y la explotación de la base de datos resultante para su integración con otros sistemas de información.
Se pretende implementar un sistema de información automática de inventario que registre los cambios de la configuración de una red informática, aplicándose en primer término a la red interna del Instituto Universitario Aeronáutico que cuenta con un plantel de 1000 máquinas aproximadamente, repartidas entre dependencias del IUA central y centros de apoyo de Rosario y Buenos. Aires.

Palabras clave: OCS Inventory NG, Open Audit, GLPI, Auditoria, Monitoreo.

1 Introducción

Existen diversos estándares y prácticas [1] que definen cómo gestionar diferentes puntos de la función IT entre ellos :

- COBIT
- COSO
- ITIL
- ISO/IEC 27002
- FIPS PUB 200
- ISO/IEC TR 13335
- ISO/IEC 15408:2005
- TickIT
- TOGAF
- IT Baseline Protection Manual
- NIST 800-14

Fue seleccionada para esta investigación como base normativa la ISO/IEC 27002 [11],[12], por ser un estándar internacional en la cual los puntos de control son la clave para su implementación. En este proyecto se tomó de la misma el dominio 7, Gestión de activos, sección 7.1 ya que el mismo trata sobre Inventario de Activos y Directrices para su clasificación.

A los efectos de disponer de un estudio de campo que permita determinar el uso de aplicaciones GLPI en el entorno de las universidades tanto públicas como privadas de la ciudad de Córdoba Capital se ha realizado un relevamiento en distintas universidades, entre ellas la UNC y la UCC.

En este sentido se ha podido determinar que sólo en algunas áreas muy limitadas se utiliza software del tipo GLPI con fines de seguimiento de intervenciones sobre los equipos, como en el caso de soporte técnico, y no como gestión global de recursos informáticos, licencias de software o automatización del inventario.

En un diagrama como muestra la figura 1, pueden apreciarse los distintos roles que intervienen en una auditoría que realiza el control de activos informáticos:, a saber:

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

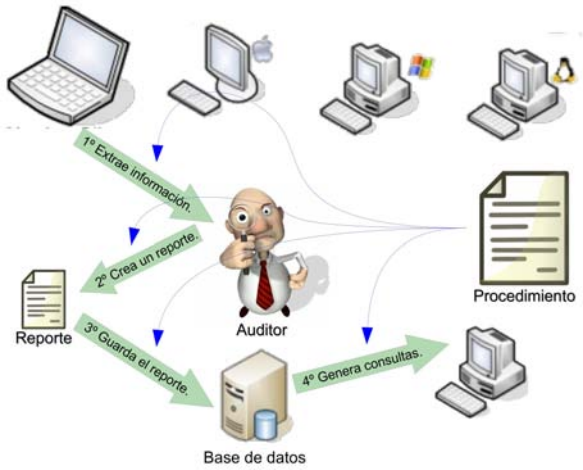

Figura 1. Auditoria estándar.

En la actualidad, en el organismo donde se realiza la investigación, el rol de auditor lo encarna una persona física apoyado por el software AIDA. El informe o reporte es transportado en un pendrive y la base de datos es una PC donde se guardan todos los informes. Todo esto se ejecuta en base a unos procedimientos internos estandarizados por normativas de la Fuerza Aérea Argentina, de la cual depende este instituto.

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

Se pretende, en síntesis, tener un control del inventario de la red informática tanto lógico como físico. Al realizarlo de manera autónoma, los períodos de actualización de la información resultan menores que cuando se realiza con un técnico que releva máquina por máquina en forma local y registra la información en una base de datos preexistente. Los beneficios más importantes son:

- Menor tiempo de actualización de la información.
- Disminución de la probabilidad de errores originados por el ingreso manual de los datos.
- Reducción de costos de mantenimiento.

2 Metodología

A la hora de implementar una solución al problema de la auditoría surgen distintas interrogantes, ¿qué Herramienta usar?, ¿cómo se implementa?, ¿qué datos se pueden extraer?, ¿qué datos son relevantes extraer?, entre otros.

Habiéndose analizado diferentes opciones para lograr este objetivo, se planteó un análisis de dos herramientas preseleccionadas de código abierto, a saber: OCS Inventory [2], [10] y Open Audit [9].

Con el fin de tener una primera aproximación al funcionamiento de las herramientas, este análisis fue llevado a cabo sobre un entorno de trabajo virtual. Posteriormente se realizó sobre una pequeña red LAN de arquitectura heterogénea

Nuestro esquema de funcionamiento está centrado en la auditoría de las máquinas que pertenecen a una red. En principio esta red está segmentada, con diferentes dominios, diferentes sistemas operativos, y diferentes usuarios. El primero de los interrogantes es ¿qué es necesario modificar o agregar a mi red para poder implementar el sistema de auditoría?

Luego surge la pregunta ¿cómo voy a enviar al auditor a cada estación de trabajo?.

Todas estas preguntas tienen un elemento en común que consiste en cómo factores externos a la herramienta afectan al despliegue de la misma [3]. De más esta decir que una herramienta de auditoría es netamente un sistema distribuido en toda la red.

Para responder estas preguntas es válida la utilización de un entorno de trabajo virtual.

El esquema de funcionamiento del sistema que se plantea se aproxima al que se muestra en la figura 2.

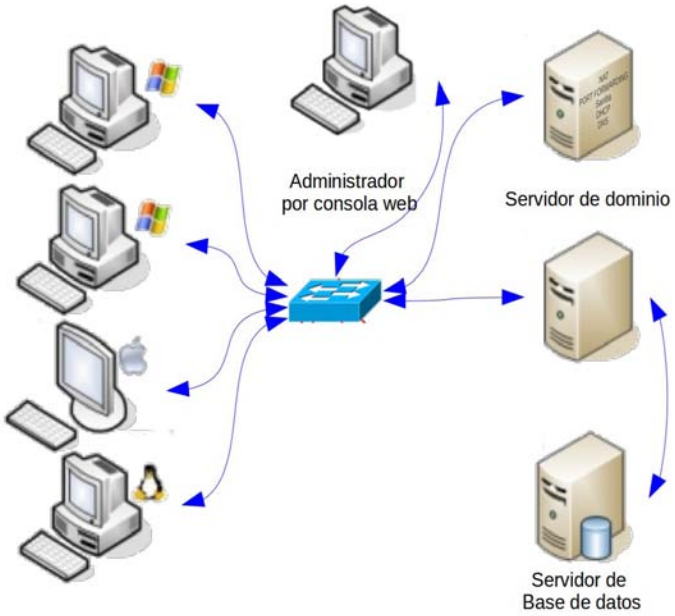

Figura 2. Estructura de la red virtual.

Esta estructura simula la red informática y se implementó en máquinas virtuales emuladas con Oracle VirtualBox.

¿qué datos se pueden extraer?

Al extraer datos tales como: usuarios, programas, configuraciones, etc, en general datos lógicos, la virtualización no presenta mayores inconvenientes, pero a la hora de extraer datos de los componentes físicos la misma no es suficiente.

De aquí surge la segunda etapa del proyecto, centrada en la fidelidad de los datos extraídos.

Nuestro nuevo entorno de trabajo es una pequeña red aislada, compuesta por 4 estaciones de trabajo todas de hardware diferente (distintos microprocesadores, placas madres, monitores, etc). Además cada estación de trabajo también contiene 4 sistemas operativos instalados. Si bien con solo 4 estaciones no se puede tener toda la diversidad de hardware que hay en una red de 1000 máquinas, esta configuración es una muestra representativa de un entorno real.

El esquema de funcionamiento del sistema que se plantea se aproxima al que se muestra en la figura 3.

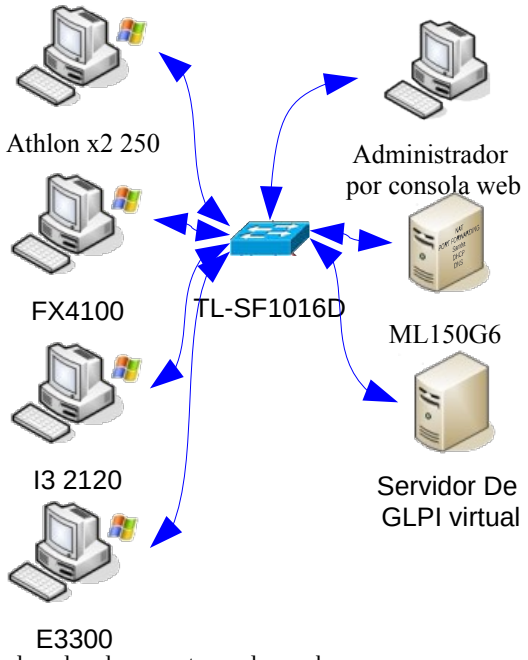

Figura 3. Topología de red real para entorno de pruebas.

Se puede apreciar en la figura 3 que el servidor de GLPI sigue siendo virtual. Esto no supone problemas a la hora de validar los datos ya que no es la máquina donde se alojan los servidores la que nos interesa auditar.

3 Resultados

De la primer etapa del proyecto surgen las guías de instalación y despliegue de las herramientas. Además se pudo estimar el impacto en la red para cada una de ellas. Se observó en un análisis de tráfico de red que el volumen de éste es directamente proporcional a la cantidad de máquinas. Esto nos permite estimar el tráfico total para la red de la institución. Con el fin de no congestionar a la red se programan los horarios y la velocidad de la auditoria. En la segunda etapa se realizó una comparación de la fidelidad de los datos extraídos, inspeccionando los informes de cada herramienta y verificando contra el hardware y software real de cada máquina.

Con todos estos informes se confeccionó la Tabla 1, donde se obtienen los siguientes indicadores, cuyos valores oscilan entre cero y cinco donde cinco es el máximo valor y cero el mínimo.

Tabla 1. Cuantificador numérico.

Herramienta, Atributo	*Valoracio de Importacia*	*OCS inventory Windows xp*		*OCS inventory Windows 7*		*OCS inventory ubuntu*	*Open Audit Windows xp*		*Open Audit Windows 7*		*Open Audit ubuntu*	
Inventario de Software												
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 fisico HDD	5	5	5	4	4	5	5	4	4	4	4	5	5
Almacenamiento fisico (CD, pen, etc)	5	4	4	4	4	4	4	4	4	4	4	5	5
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		65,8

Inventario de Software

- 5 corresponde a datos fidedignos y completos (nombre, versión, números de serie, licencia, etc,).
- 4 corresponde a datos fidedignos (nombre, versión, etc , pudiendo faltar algún número de serie o licencia pero auditando todo lo que tiene el sistema)
- 3 corresponde a datos parciales (ejemplo: No reconoce todo el software instalado o solo los nombres pero no las versiones)
- 2 corresponde a datos incompletos (Ejemplo: No detecta cierto software.)
- 1 corresponde a datos inciertos (Completa campos con nombres o números no significativos)

Inventario de Hardware

- 5 corresponde a datos fidedignos y completos (nombre, revisión, números de serie, etc,).
- 4 corresponde a datos fidedignos (nombre, modelo, pudiendo faltar algún número de serie, pero auditando todo lo que tiene el sistema)
- 3 corresponde a datos parciales (ejemplo: Reconoce cuanta memoria RAM tiene pero no el modelo.)
- 2 corresponde a datos incompletos (Ejemplo: No detenta un microprocesador, no detecta tarjetas de expansión.)
- 1 corresponde a datos inciertos (Completa campos con nombres o números no significativos)

Impacto de red

- 5 corresponde a volumen de tráfico excedente menor a la mitad al excedente promedio.
- 4 corresponde a volumen de tráfico excedente mayor a la mitad al excedente promedio.
- 3 corresponde a volumen de tráfico excedente cercano al excedente promedio.

• 2 corresponde a volumen de tráfico excedente menor al doble del excedente promedio.
• 1 corresponde a volumen de tráfico excedente mayor al doble del excedente promedio.

De la tabla 1 se puede concluir que Open Audit es la mejor elección.

¿cómo funciona Open Audit para auditar un dominio?

La figura 4 muestra un esquema general de auditoria de dominio con la herramienta Open Audit.

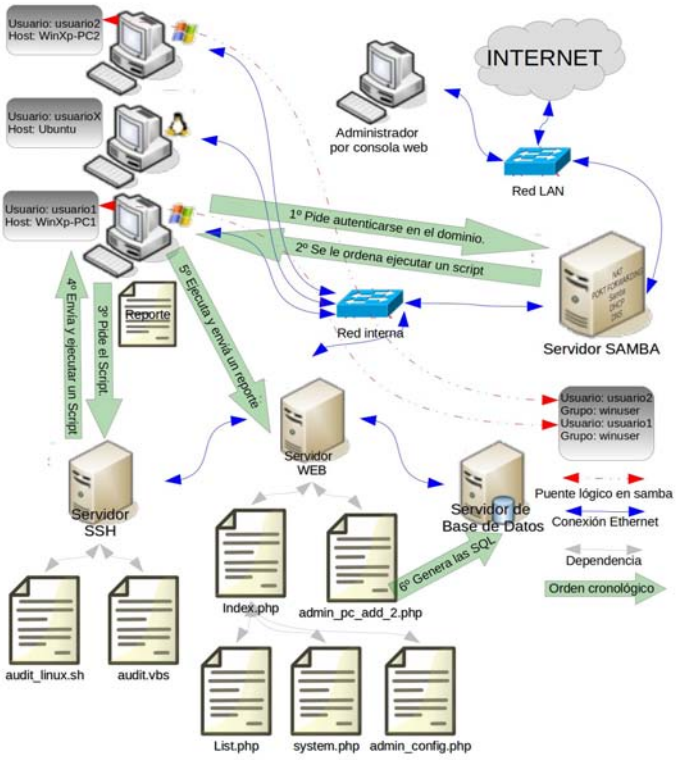

Figura 4. Auditoria de dominio.

Al iniciar sesión los usuarios del dominio se registran ante el PDC (controlador primario de dominio), que es implementado por el servidor Samba, que los instruye a ejecutar un Script de auditoria. Dependiendo del sistema operativo el Script es diferente.

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 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 es el encargado de enviar el auditor. En la figura 5 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.

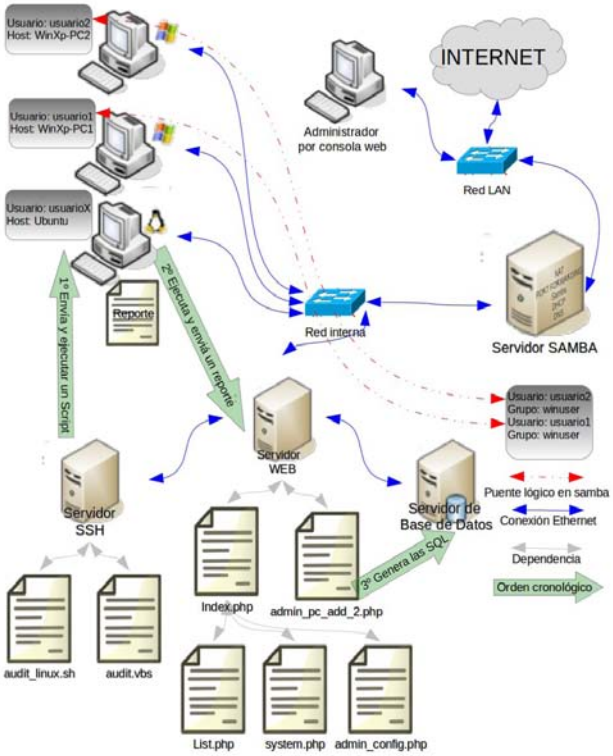

Figura 5. Auditoria fuera del dominio.

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 por html 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 6 se aprecia cómo es el flujo de información a la hora de realizar una consulta. No es necesario que las máquinas auditadas estén en linea al momento de realizar la consulta. esto cumple con la disponibilidad de datos pedida por la ISO.

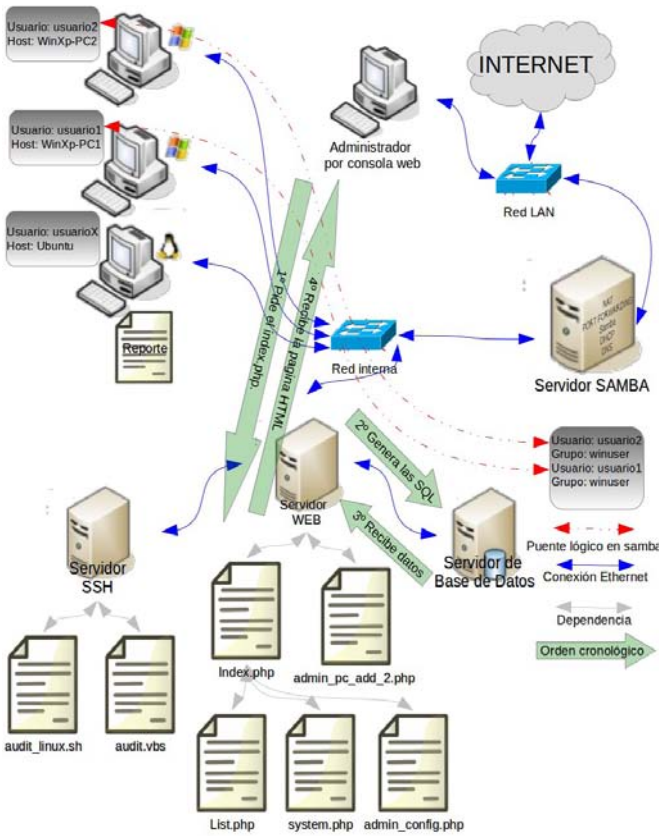

Figura 6. Consulta genérica.

En concordancia con el sistema actual, 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.

Esquema general

En la figura 7, se presenta un diagrama en bloques que muestra el esquema general que es necesario agregar a la red para implementar la herramienta.

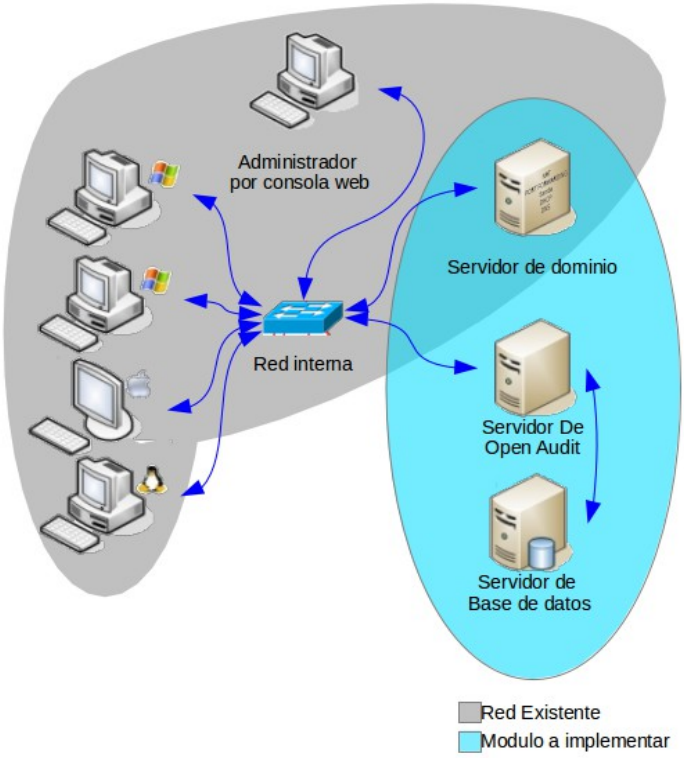

Figura 7. Modelo de implementación en red.

El área pintada de gris representa una red como la existente en el IUA, el área pintada de turquesa son los servidores que se incorporarán o modificarán.

Hay que destacar que hay un área compartida que es el servidor de dominio que al momento de implementar el sistema en la red real será necesario modificar su configuración. Por esto mismo es de vital importancia que estas configuraciones y modificaciones sean exhaustivamente probadas, a los efectos de evitar fallos en la red.

4 Conclusiones

Se generó un ambiente virtual donde se simuló un dominio real sobre el que se realizaron las pruebas de las herramientas de una forma controlada para poder medir bien sus facilidades.

El mismo está compuesto por máquinas virtuales emuladas con Oracle VirtualBox. Algunas de ellas actúan como servidores y otras como estaciones de trabajo, estas últimas fueron instaladas dentro de un mismo servidor, configurándolas en distintos ambientes operativos, para simular la situación real de la red del IUA, o de cualquier red informática con muchas estaciones de trabajo conectadas.

Además se generó un entorno de trabajo real que fue útil para verificar fidedignamente los datos que extraen las herramientas, el cual está compuesto por máquinas reales de hardware y software heterogéneo con el fin de tener una muestra más representativa del parque informático.

El éxito de estas pruebas originó que este logro técnico esté documentado y a disposición de los otros proyectos del Ministerio de Defensa en ejecución en la actualidad.

Las pruebas realizadas sobre el software demostraron que el mismo no es afectado por la topología de la red, ya que se parte de la presunción de que todas las máquinas tienen conectividad contra su servidor de dominios o la puerta de enlace a Internet, por lo que nos limitamos a simular solamente una subred: 10.0.0.x

Como se puede apreciar en la Tabla 1 la extracción de datos no cumple totalmente con lo requerido por la norma, por lo que es preciso continuar con el perfeccionamiento del código de Open Audit. Este es uno de lo motivos de que se elijan herramientas de trabajo de código fuente libre.

5 Trabajos futuros

Adaptación del frontend PHP que brinda la herramienta Open Audit con nuevas consultas SQL que faciliten la interacción con la información recolectada.

En la siguiente etapa se implementará una integración entre la base de datos de Open Audit y la base de datos de la institución a los fines de su convergencia a una única solución.

Referencias

1. http://auditoriasistemas.com/estandares-ti/
2. Barzan T. A. (2010). IT Inventory and Resource Management with OCS Inventory NG 1.02 , Ed. Packt Publishing.
3. Jackson C. (2010). Network Security Auditing. Ed. Cisco Press.
4. Fettig A. (2005). Twisted Network Programming Essentials. Ed. O'Reilly.

5. Philippe J. y Flatin M. (2002). Web Based Management of IP Network Systems. Ed. John Wiley & Sons.
6. McNab C. (2007). Network Security Assessment,
7. Echenique Garcia J. A.(2001). Auditoria en Informática. Ed. Compañía Editorial Continental.
8. Piattini V. M. y Del Peso N. E. (2008). Auditoria de Tecnologías y Sistemas de Información. Ed. Alfaomega Grupo Editor.
9. http://www.open-audit.org/
10. http://www.ocsinventory-ng.org/en/
11. http://www.iso27000.es/
12. http://www.17799.com/