Monitoreo remoto de sistemas en red para la auditoria informática

Ciolli María Elena, Porchietto Claudio, Rossi Roberto

Grupo de Investigación Instituto Universitario Aeronáutico, Córdoba, Argentina

Abstract. *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.

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.

No se ha encontrado ningún trabajo que analice el comportamiento de herramientas de código abierto en ambientes multiplataforma con conexión LAN, WAN o VPN, pero sí existen experiencias

desarrolladas en empresas con la utilización de aplicaciones propietarias.
En el primer caso las referencias encontradas son escasas y direccionan directamente a la página oficial de las herramientas consideradas o a los foros de consulta de las mismas.

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:

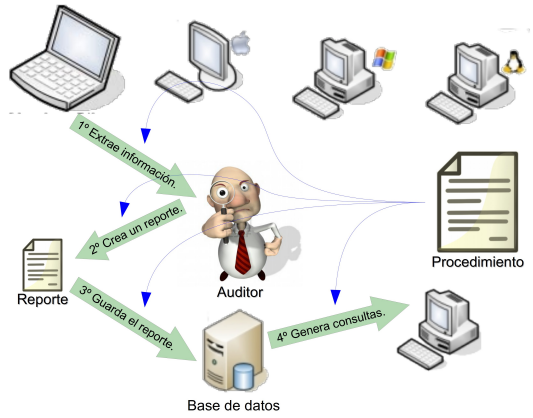

Figura 1: Auditoria estándar

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

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 es necesario realizar 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.

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].

Es pertinente aclarar que se contempla la posibilidad de que ninguna de las herramientas existentes cumpla con todo los requerimientos. Esto no plantea mayor

impedimento, siendo herramientas de código abierto se podrán adecuar a los requerimientos.

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

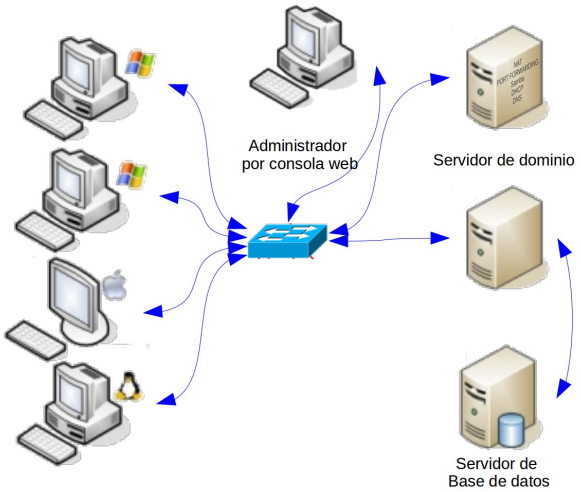

Figura 2: Estructura de la red virtual

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

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

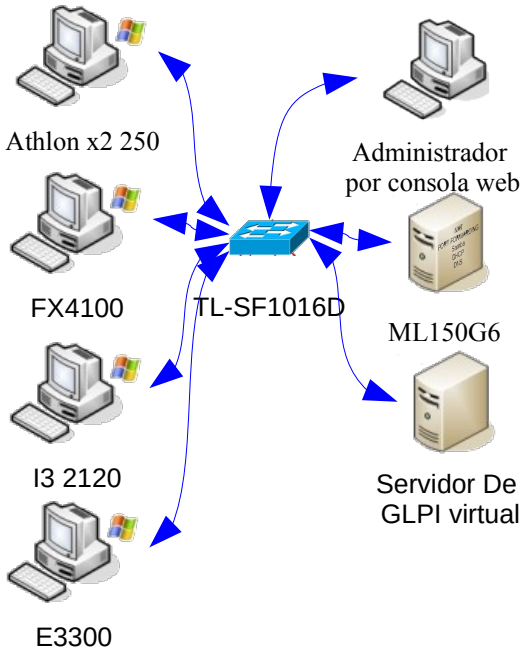

Figura 3: Topología de red real para entorno de pruebas

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.

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.

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)

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 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	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

• 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 OpenAudit es la herramienta que más se aproxima a los requerimientos de la norma ISO 27002, pero es necesario su mejora para lograr el objetivo planteado.

¿cómo funciona Open Audit para auditar un dominio?

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

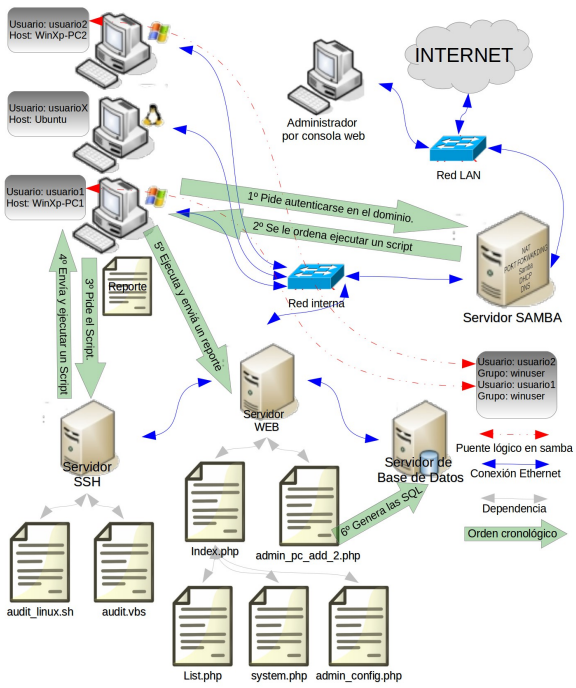

Figura 4: Auditoria de dominio

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?

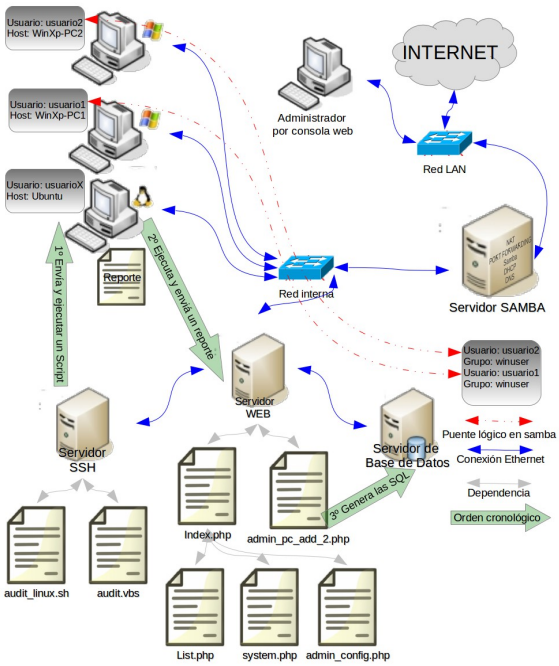

Figura 5: Auditoria fuera del dominio.

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. 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.

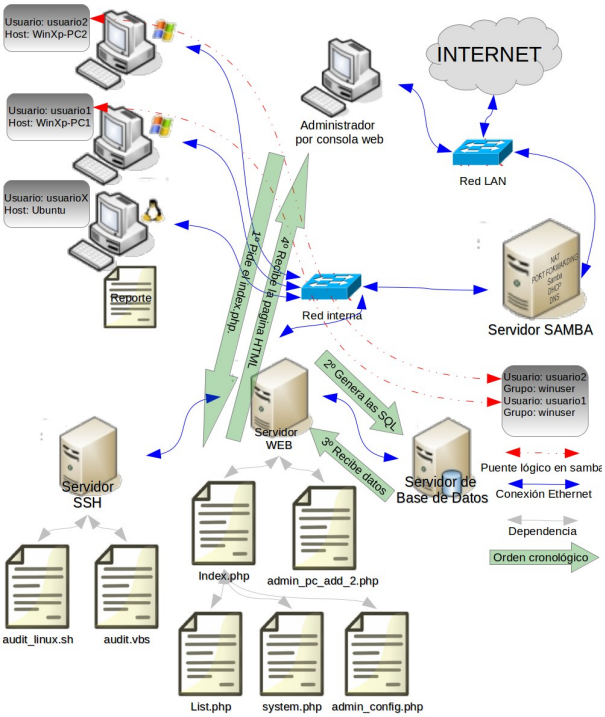

Figura 6: Consulta genérica

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.

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 OpenAudit. 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.

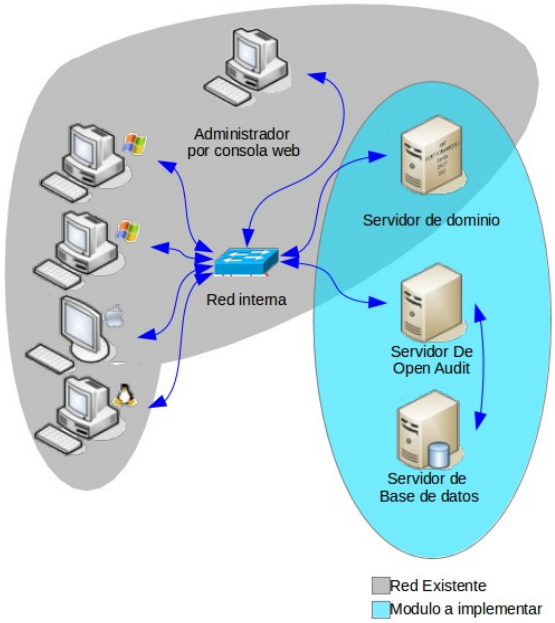

Figura 7: Modelo de implementación en red

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.

Discusión

La columna valoración de importancia que cuantifica a la tabla 1, fue creada arbitrariamente por un administrador de la red cuya pericia avala su contenido. No obstante esto podría ser aplicable solo a la red en la que pertenece dicho administrador.

Del relevamiento realizado en instituciones universitarias de la provincia de Córdoba, se concluyó sobre la no utilización de software del tipo GLPI para tareas de gestión global del parque informático. En este sentido se estima la utilidad de este trabajo a los fines de su implementación en otras áreas de gestión pública.

Conclusiones

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

Actualmente se continúa perfeccionando el código fuente de OpenAudit a fin de lograr la detección completa de todos los componentes mencionados por la norma, cuya valoración es visualizada en la tabla 1.

Este es uno de lo motivos de que se elijan herramientas de trabajo de código fuente libre.

El éxito de las pruebas tanto en el entorno virtual como real originó que este logro técnico esté documentado y a disposición de los otros proyectos del Ministerio de Defensa en ejecución en la actualidad.

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/

Datos de Contacto: Ciolli María Elena, Porchietto Claudio, Rossi Roberto
{mciolli,porchietto,roberto.rossi}@gmail.com

Anexos

Implementación del entorno virtual

Este proyecto se basa principalmente en el análisis de distintos sistemas de código abierto, por lo que es crucial tener una plataforma de pruebas que sea estable, aislada y donde se puedan implementar versiones fácilmente recuperables. Se optó por utilizar máquinas virtuales emuladas con VirtualBox y alojadas en una estación de trabajo con prestaciones suficientes para alojar a todos los componentes de una pequeña red.

Para la emulación se eligió VirtualBox por ser una herramienta con licencia GNU General Public License (GPL) versión 2, lo que permite el ahorro del gasto en licencias propietarias y, la posibilidad de utilizar la virtualización por hardware VT-x/AMD-V, tecnología que debe ser soportada por el micro procesador de la estación de trabajo anfitriona y permite una amplia mejora en el rendimiento.

Procesos realizados

- Construcción del entorno de trabajo. Consta de VM que representan estaciones de trabajo con Windows Xp, Windows 7 y VM que representan los servidores con Ubuntu server. Dicho entorno está configurado de tal manera que emula a la infraestructura existente en el IUA, en donde las estaciones de trabajo Windows dependen de controladores de dominio montados en servidores Linux con Samba.
- Luego de generado el ambiente, se procede a generar imágenes de cada máquina virtual con el fin de poder regenerar de manera simple y rápida un nuevo ambiente de prueba virgen.
- Despliegue sobre el espacio de trabajo de la primera de las herramientas a probar. Se generan informes en los que se detalla el proceso con la finalidad de que la experiencia sea fácilmente repetida al momento de implementarlo en un entorno real.
- Análisis del funcionamiento de la herramienta y generación de un informe estandarizado que facilite la comparación con otras dos herramientas.
- Se repiten los últimos dos puntos para las otras herramientas.
- Informe comparativo de las herramientas con el que se selecciona una y se enumeran las falencias de la misma según los requerimientos del proyecto para que posteriormente se cubran con otras herramientas.

Infraestructura requerida

Para alojar esta red informática virtual se requiere una estación de trabajo. Todos estos sistemas operativos deben funcionar simultáneamente en la PC que actúe como anfitriona.

Se debe dimensionar la PC que albergará el ambiente virtual para las pruebas.

Basados en documentación provista por Microsoft, Canonical y datos recogidos de Internet construimos la siguiente tabla.

Tabla 2: Estimación de los requerimientos de Hardware

Máquina virtual	Memoria por Máquina Virtual (Mbytes)	Frecuencia de CPU (MHz)	Cantidad de Máquinas Virtuales	Total Memoria (Mbytes)	Total CPU (MHz)
Microsoft Windows 7 X64	2048	1000	4	8192	4000
Windows Xp	128	300	4	512	1200
Ubuntu Desktop	1024	1000	2	2048	2000
Ubuntu server	512	500	3	1536	1500
				----------	----------
Total:				12288	8700

Se requiere un total de 12GB de RAM y un procesador de 8.7GHZ o los que es lo mismo dado que se puede paralelizar el cálculo un procesador de 4 núcleos a 2,2GHz. Se optó por un Intel i7 2600k de cuatro núcleos a 3.4 GHz y 16GB de RAM.

En los servidores es necesario calcular la memoria que consumirán ya que esta varía en función de los servicios y la cantidad de usuarios. Para calcular la memoria que consumirá el controlador primario de dominios, que es uno de los servidores del dominio virtual, es necesario saber la cantidad de usuarios que tiene la red. En la red virtual planteamos que sean 10. Este servidor corre un considerable número de servicios. Dicha situación se refleja en la Tabla 3.

Tabla 3: Requerimientos mínimos de memoria Servidor SAMBA

Nombre de aplicación	Memoria por usuario (Mbytes)	Cantidad de usuarios	Total (Mbytes)
DHCP (dhcpd3-server)	2,5	10	3,0
DNS	16	10	16
Samba (nmbd)	16	10	16
Samba (winbind)	16	10	16

Samba (smbd)	4	10	40
Basic OS	256	256	256
			---------- -
Total:			347

Por lo tanto se estima que con un total de 512 MB de RAM será suficiente para cubrir las necesidades de memoria en la simulación planteada con anterioridad.

Formulación y Valoración de Alternativas

La primera alternativa a utilizar VirtualBox es VMware que tiene funcionalidades muy parecidas pero exige el pago de licencias. Otra alternativa es la utilización de una red real con estaciones de trabajo y servidores reales pero esto tiene dos grandes desventajas, costos muy superiores y mayor dificultad para realizar el versionado.

Análisis de costo

La tabla 4 detalla los costos estimados de valorar las dos principales alternativas.

Si bien el costo de la estación de trabajo necesaria para alojar el entorno de trabajo virtual es elevado, el mismo es muy inferior al necesario para implementar el entorno real. Otro de los inconvenientes que se presenta es la no centralización de los sistemas, pues para implementar un control de versiones hay que realizar imágenes de cada disco duro haciéndolo máquina por máquina. En el entorno virtual es suficiente con clonar cada PC y etiquetarla con un nombre diferente.

Tabla 4: Estimación de los costos monetarios

	Cantidad	Costo unitario	Virtual	Cantidad	Costo unitario	Real
Estaciones de trabajo	1	13972,28	13972,28	10	2000	20000
Servidores	0	8437,99	0	2	8437,99	16875,98
switch	0	120	0	1	120	120
cableado	0	25	0	12	25	300
Total		13972,28			37295,98	