Diseño de un entorno virtualizado para la docencia práctica de Seguridad en Sistemas de Información

Francisco José Ribadas Pena, Francisco Mario Barcala Rodríguez, Víctor Manuel Darriba Bilbao, Juan Otero Pombo

Departamento de Informática

Universidade de Vigo

Edificio Politécnico, Campus As Lagoas S/N

32004 Ourense

{ribadas,barcala,darriba,jop}@uvigo.es

Resumen

La posibilidad de que los alumnos de materias relacionadas con la seguridad informática puedan realizar sin restriciones prácticas sobre sistemas y redes reales tiene un valor pedagógico indudable, ya que les permite enfrentarse a situaciones reales y resolver problemas que en las clases teóricas apenas se llegan siquiera a describir. Sin embargo, estas actividades conllevan una serie de dificultades técnicas y de disponibilidad de recursos, junto con otras derivadas de la propia disposición del alumno a la hora de enfrentarse a ellas.

En este trabajo describimos un entorno de prácticas basado en el uso de equipos y redes virtualizadas y en el empleo de herramientas de seguridad de código abierto, que supera parte de los problemas inherentes a la realización de ejercicios sobre sistemas reales. Presentamos también el diseño y desarrollo de una serie de actividades de laboratorio que hacen uso del entorno descrito y que pretenden promover el trabajo autónomo en la resolución de problemas relacionados con la seguridad y la protección de sistemas.

1. Introducción

En multitud de ocasiones existen limitaciones de tipo material o administrativo que dificultan realizar ciertas actividades prácticas que desde un punto de vista pedagógico serían deseables o necesarias. Un caso paradigmático de este tipo de problemas es la docencia de determinados contenidos relacionados con la seguridad informática [5, 7].

Se pretende que los estudiantes conozcan las amenazas típicas a la integridad y la seguridad de los datos y los sistemas de información y que adquieran una experiencia que les permita ser capaces de enfrentarse a ellas e implantar las medidas necesarias para evitarlas, detectarlas y contrarrestarlas. Asegurar el éxito en la adquisición de este tipo de habilidades es particularmente difícil, ya que requiere la práctica directa sobre un entorno similar a los que se puedan encontrar en el mundo real. Por ello, la situación ideal sería aquella en la cual cada alumno dispusiese de un entorno de red real sobre el que experimentar y poder manejar libremente distintas herramientas de seguridad, enfrentándose a casos de estudio cercanos a la realidad.

Sin embargo, plantear este tipo de aproximaciones en los laboratorios de prácticas disponibles en nuestros centros supone un reto. Por cuestiones de coste y de administración del equipamiento, es habitual que los laboratorios docentes sean compartidos por distintas materias. En ese

contexto es necesario tener presente que buena parte de los ejercicios relacionadas con la seguridad, como simulación de intrusiones y ataques o la instalación de cortafuegos y medidas de protección, causarían numerosos problemas en un laboratorio compartido. Otro problema es el riesgo implícito de las actividades desarrolladas en una clase práctica de seguridad. Es necesario que los alumnos trabajen con privilegios de administrador y que realicen tareas potencialmente peligrosas, que pueden afectar a la integridad de los recursos del laboratorio, perturbando la docencia de otras materias. Incluso, dada la naturaleza de ese tipo de ejercicios, es posible que de forma intencionada o no, el alcance de las molestias o los daños causados vaya más allá de un laboratorio concreto, del centro o de la red de la propia universidad.

Otra cuestión que plantea dificultades a la hora de abordar este tipo de prácticas sobre entornos reales está relacionada con las capacidades del alumnado. Enfrentarse a ejercicios prácticos de seguridad requiere disponer de unos conocimientos básicos sobre Sistemas Operativos (S.O.) y Redes de Computadores, así como de la soltura necesaria para ponerlos en práctica al realizar tareas avanzadas de administración de equipos y redes. En el caso concreto de la docencia de *Seguridad en Sistemas de Información*[1] que impartimos en la Escuela Superior de Ingeniería Informática de la Universidad de Vigo, las diferencias en cuanto a las capacidades previas del alumnado si suponen un obstáculo serio. En nuestro centro, *Seguridad en Sistemas de Información* se oferta como materia de libre elección, con un alumnado muy variado en cuanto a sus conocimientos previos, ya que en un mismo grupo de prácticas puede haber estudiantes desde segundo hasta quinto curso. Como contrapartida, al tratarse de una materia elegida por el alumno, su motivación y su interés por los temas relacionados con la seguridad suele ser bastante alto.

[1] `http://ccia.ei.uvigo.es/docencia/SSI`

Tomando en consideración todos estos condicionantes previos, proponemos una aproximación basada en el uso software de virtualización. Pretendemos ofrecer al alumno, dentro de una única máquina, un entorno virtual con múltiples computadores conectados formando pequeñas redes. Conseguimos con ello aislar los problemas de administración y los riesgos mencionados anteriormente dentro de un entorno independiente del resto del laboratorio docente. En nuestro caso, proponemos un entorno diseñado específicamente para la docencia de seguridad informática, junto con una colección de actividades prácticas, diseñadas con la premisa de mitigar los problemas derivados de las diferencias en cuanto a formación y experiencia previa que se dan en nuestro caso concreto.

2. Requisitos previos y alternativas

Según la propuesta de Logan [6], el esquema ideal para desarrollar un curso de seguridad informática requeriría la inversión en un laboratorio específico, con una red cerrada, dispositivos de red propios y un conjunto de servidores y herramientas software con las que experimentar. Esta autora parte de la base de que un aspecto crítico en cursos que requieran ejercicios reales es la disponibilidad de un laboratorio de uso exclusivo, debido a la naturaleza de las herramientas empleadas y a la necesidad de reconstruir y reconfigurar la red durante el desarrollo del curso, concluyendo que un laboratorio destinado a este tipo de docencia de la seguridad informática no debería estar disponible a estudiantes ajenos a ese curso.

Como hemos mencionado, esta propuesta no es aplicable en la mayoría de los casos. Aún así, nuestro objetivo principal sigue siendo que los estudiantes pongan en práctica sus conocimientos de seguridad informática en sistemas reales, usando herramientas de seguridad reales y resolviendo problemas prácticos del mundo real. Como objetivos secundarios, pretendemos minimizar el

coste y la carga de trabajo que requeriría el mantenimiento de un laboratorio de seguridad dedicado. También buscamos maximizar el aprovechamiento del tiempo de prácticas, ofreciéndo al alumno un entorno preconfigurado y adaptado específicamente a cada una de las actividades prácticas que se le propongan, donde el tiempo y el trabajo extra necesario para su puesta en marcha sea lo más reducido posible.

Para conseguir estos objetivos proponemos hacer uso de técnicas de virtualización, siguiendo una aproximación similar a la descrita en [2] y [3]. Estas herramientas nos permiten crear un entorno para la docencia de seguridad informática que simule dentro de un equipo anfitrión una pequeña red de máquinas reales, que contarán con un conjunto rico y variado de herramientas de seguridad.

2.1. Aspectos generales de virtualización

En la virtualización de sistemas nos encontramos con un equipo anfitrión sobre el cual un software específico permite ejecutar uno o más sistemas huésped de forma simultánea. En [4] y [2] se ofrece un repaso de las técnicas de virtualización y una revisión del software más significativo. A modo de resumen, distinguimos cuatro grandes técnicas de virtualización.

Emulación También llamada recompilación dinámica, en la cual se simula el hardware completo del sistema huésped. Es la aproximación más lenta y costosa y permite trabajar con hardware y sistemas operativos diferentes de los del anfitrión.

Virtualización completa El huésped se ejecuta directamente sobre la CPU anfitrión, la máquina virtual sólo simula el hardware necesario para que el S.O. huésped se ejecute sin modificaciones. La arquitectura del huésped, y ocasionalmente su S.O., han de coincidir con los del anfitrión. Obtiene velocidades cercanas a las nativas.

Paravirtualización La máquina virtual no simula la totalidad del hardware, se limita a ofrecer un API especial. Require modificaciones en el S.O. huésped para poder usar ese API, a cambio se consigue una velocidad equiparable a la nativa.

Virtualización a nivel de S.O. Se ofrece virtualización a varios servidores sobre el S.O. anfitrión, que se ejecutan dentro de entornos propios e indepedientes. El S.O. del huésped coincide con el del anfitrión.

Actualmente la virtualización es un campo en auge, debido a las posibilidades que ofrece como mecanismo para la compartición y el aprovechamiento de recursos hardware. También se usa ampliamente en entornos de experimentación y como mecanismo para la difusión e instalación de soluciones preconfiguradas para funciones específicas, conocidas como *appliances*. Existen repositorios[2] de imágenes de máquinas virtuales que permiten contar casi inmediatamente con un entorno listo para ser usado. Otro ejemplo de uso efectivo de las técnicas de virtualización con fines educativos y divulgativos es el reto SAURON del SG6-Lab[3], donde se ofrece un entorno virtual para practicar intrusiones en sistemas, consistente en la imagen QEMU [1] de un servidor Web sobre GNU/Linux.

Desde el punto de vista de la docencia, los entornos virtualizados proporcionan numerosas ventajas [8]. Las máquinas virtuales son fáciles de crear y son muy seguras, ya que es posible aislarlas totalmente de la red de docencia y del exterior. Permiten configurar una vez y distribuir las imágenes a los alumnos, ahorrando tiempo de configuración. Son razonablemente fiables y la recuperación ante catástrofes es sencilla, basta con retomar las imágenes iniciales para reconstruir el entorno de prácticas. Además, ofrecen grandes facilidades para diseñar ejercicios específicos destinados a desarrollar habilidades concretas, mediante

[2] http://www.vmware.com/appliances
[3] http://www.sg6.es/labs/

Huésped ligero (`ligero.img`)
Debian Etch con kernel 2.6.18 Sin entorno gráfico
Servicios (desactivados por defecto): servidor web (Apache 1.3) servidor ssh (openSSH) servidor telnet, servidor ftp
Herramientas de seguridad: escáner de puertos NMAP
Software general: clientes telnet, ftp y ssh navegador web modo texto *Lynx* editores: vi, nano, jed
Tamaño de la imagen: aprox. 450 MB

Tabla 1: Configuración del huésped ligero.

el uso de imágenes de sistemas virtuales preconfigurados listos para desarrollar esa actividad, del mismo modo que se desarrollan y distribuyen *appliances*.

En el caso que nos afecta, la docencia práctica de *Seguridad en Sistemas de Información*, las técnicas de virtualización ofrecen la posibilidad de que cada alumno cuente con un entorno de red completo en un laboratorio docente compartido, o incluso en su propio equipo personal, con todas las ventajas mencionadas anteriormente y sin riesgo para el equipo anfitrión o para la red docente del centro.

3. Descripción del entorno de prácticas propuesto

Una vez presentados nuestros objetivos y las ventajas que ofrecen las aproximación basadas en entornos virtualizados, dedicaremos esta sección a describir los aspectos más destacados del software de virtualización que hemos empleado en nuestro caso, QEMU [1], y presentaremos los detalles técnicos de los componentes del entorno virtualizado que proponemos para la docencia práctica de *Seguridad en Sistemas de Información*.

3.1. Software de virtualización QEMU

En nuestro entorno de virtualización para la docencia de seguridad informática hemos decidido emplear la herramienta QEMU [1], desarrollada por Fabrice Bellard bajo licencia GPL. Este software puede funcionar en modo emulador, empleando recompilación dinámica, ó, mediante el uso del módulo KQEMU, puede proporcionar virtualización completa sobre sistemas anfitrión x86, con menor consumo de recursos y una velocidad cercana a la nativa. El sistema está disponible para GNU/Linux, Windows y MacOS X y permite emular diferentes arquitecturas(x86, x86-64, PowerPC, ARM, SPARC-32/64), junto con sus correspondientes dispositivos de E/S (tarjeta de red, gráfica, sonido, etc...), sobre los que se pueden instalar diversos S.O.

Además de tratarse de una alternativa de software libre, con todas las ventajas que esto conlleva, la principal razón a la hora de habernos decido por el uso de QEMU frente a otras herramientas de virtualización privativas[4] o libres[5], es la gran versatilidad que ofrece a la hora de construir y emular redes entre los equipos virtualizados. QEMU puede simular varias interfaces de red en un mismo huésped, que se pueden conectar con las de otros huéspedes o con el propio equipo anfitrión, formando lo que en terminología QEMU se llama una *Virtual-LAN*(VLAN). Cada una de estas VLAN conforma un dominio de colisión, a modo de concentrador o *hub* virtual, donde se conectan diferentes instancias de equipos huésped, que se ejecutan en el mismo o en diferentes anfitriones. Cada uno de los interfaces de red asociados a un anfitrión puede ser configurado de diversas formas, para definir el tipo de conexión que se establecerá y su comportamiento.

Modo usuario El anfitrión establece en cada VLAN una red del rango 10.0.2.0/24 y la provee de un cortafuegos y de servidores DNS y DHCP. A dicha red se incorporan los huéspedes configurados en modo usuario. No requiere privilegios de administrador y no permite tráfico hacia el anfitrión o hacia el exterior.

[4] VMWare: `http://www.vmware.com`
[5] VirtualBOX: `http://www.virtualbox.org`

Conexión a VLANs Es posible conectar varias instancias de máquinas huésped dentro de una misma VLAN a través de un puerto TCP o UDP. El primer huésped establece la conexión[6] a la cual se pueden conectar otros huéspedes de esa VLAN[7]. No es preciso que todos los huéspedes se ejecuten en el mismo anfitrión. Una vez conectados compartirán un mismo segmento de red virtual.

Conexión TAP QEMU crea un dispositivo de red virtual TAP[8] en el anfitrión a través del cual los huéspedes se pueden comunicar con él. Convenientemente configurado, permite la salida al exterior desde los huéspedes de una VLAN. Este tipo de conexión requiere privilegios de administrador y configuración previa.

En nuestro caso trabajamos exclusivamente con la red de QEMU en modo usuario y usaremos la conexión a VLANs para construir redes arbitrariamente complejas entre huéspedes. No emplearemos las conexiones TAP, dado que no deseamos que nuestros huéspedes tengan acceso a redes externas. Este aislamiento total del mundo exterior, junto al hecho de que la creación de estas redes en modo usuario no requiere privilegios de administrador, nos permite contar con un entorno de experimentación muy robusto y seguro, que puede ser perfectamente empleado en un laboratorio compartido sin riesgo de perturbar a la docencia de otras materias.

3.2. Estructura de los equipos y de la red virtualizada

Una vez descrita la herramienta de virtualización utilizada en nuestra propuesta, junto con el modo en que la hemos empleado para asegurar un entorno de prácticas sin riesgos, pasamos a mostrar los componentes concretos de nuestra propuesta de entorno virtual, sobre los que se desarrollarán las actividades prácticas descritas en la sección 4.

Huésped pesado (`pesado.img`)
Debian Etch con kernel 2.6.18 Entorno gráfico ligero *fluxbox*
Servicios (desactivados por defecto): servidor web (Apache 1.3) servidor ssh (openSSH) servidor telnet, servidor ftp
Herramientas de seguridad: analizador de protocolos WIRESHARK escáner de vulnerabilidades NESSUS escáner de puertos NMAP sistema de detección de intrusiones SNORT cortafuegos: netfilter/iptables interfaces iptables: Firestarter, Shorewall
Software general: clientes telnet, ftp y ssh navegador web modo texto *Lynx* editores: vi, nano, jed
Tamaño de la imagen: aprox. 750 MB

Tabla 2: Configuración del huésped pesado

Hemos pretendido simplificar al máximo las tareas de puesta en marcha de cada una de las actividades prácticas. Para ello, se ha creado un conjunto de imágenes de sistemas Debian preconfigurados con las herramientas de seguridad que se emplearán en los ejercicios instaladas y listas para ser usadas. Una restricción importante, que condiciona en gran medida el desarrollo de las prácticas es la carga computacional asociada a la virtualización. Para mitigar estos problemas las imágenes utilizadas contienen sistemas GNU/Linux mínimos, en unos casos con entornos gráficos con un consumo mínimo de recursos y en otros, exclusivamente en modo texto. Todos ellos con los servicios desactivados por defecto.

En nuestra propuesta hemos empleado únicamente dos tipos de imágenes, descritas en las Tablas 1 y 2, con las que se lanzarán los huéspedes que formarán parte de las redes virtuales a utilizar en los ejercicios prácticos. Hemos optado por configurar un *huésped pesado*, dotado de un entorno gráfico sencillo, donde están disponibles la mayor parte de herramientas de seguridad, como analizadores

[6] `-net socket,vlan=X,listen=anfitrion:puerto`
[7] `-net socket,vlan=X,connect=anfitrion:puerto`
[8] Interfaz de red simulado por software.

de protocolo, escáner de vulnerabilidades o interfaces para `netfilter`. Sobre estos huéspedes los alumnos realizarán la mayor parte de sus ejercicios. Contamos además con un *huésped ligero* con aplicaciones en modo texto, que, por su menor consumo de recursos, se empleará para crear el grueso de equipos que conformarán las redes virtualizadas.

Ambos tipos de huéspedes se combinarán para dar forma a los entornos de red empleados en las actividades propuestas. Las tareas a realizar por el alumno en cada sesión de prácticas serán las siguientes:

1. Replicar las imágenes de partida, según sea conveniente.
2. Lanzar los huéspedes en el orden adecuado, empleando los parámetros `connect` y `listen` para configurar la topología de las VLANs a emplear.
3. Configurar manualmente la red de cada huésped (dirección IP, nombre y rutas).
4. Iniciar en los huéspedes que correspondan los servicios a utilizar en el ejercicio.
5. Desarrollo del ejercicio propuesto, empleando las herramientas indicadas.

4. Propuesta de ejercicios y actividades prácticas

Una vez descritos los componentes del entorno virtual que proponemos, presentaremos una perspectiva general del tipo de actividades prácticas que permite desarrollar y la finalidad y objetivos concretos que perseguimos con las mismas. En nuestro caso, el uso que hemos dado a lo largo de los últimos años a las herramientas de virtualización ha ido aumentando el nivel de complejidad de los ejercicios propuestos, a la vez que el grado de implicación exigido a los alumnos en la realización de los mismos iba creciendo.

4.1. Uso demostrativo

El primer uso que hicimos de entornos virtualizados en la docencia de *Seguridad en Sistemas de Información* fue meramente

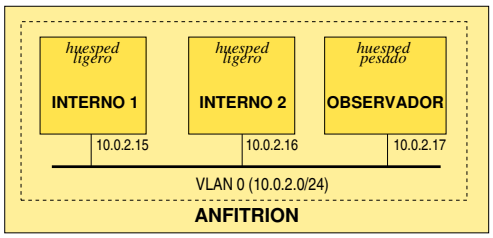

Figura 1: Configuración de red para demostración y escaneo de puertos

demostrativo. Esto sirvió a los docentes de la materia como primer contacto con estas técnicas y puso de manifiesto las enormes posibilidades pedagógicas de estas herramientas, en las que hemos ido profundizando con el paso del tiempo. En la Figura 1 se muestra un escenario en el cual hemos realizado estas actividades de demostración. En concreto, se ponen a prueba las vulnerabilidades de servicios como `telnet` y `ftp`, empleando el analizador de protocolos WIRESHARK[9] en el equipo *observador*, para capturar este tipo de tráfico entre los huéspedes *interno1* e *interno2*, haciendo evidente que un flujo de información no cifrado es extremadamente vulnerable. Para reafirmar esta conclusión, se repite el ejercicio empleando conexiones `ssh`, cuyo intercambio de datos no es visible para el huésped *observador*.

4.2. Desarrollo de prácticas guiadas

La evolución natural de las actividades anteriores supone dar a los alumnos las indicaciones oportunas para que sean ellos quienes experimenten sobre el entorno virtualizado. En nuestro caso, contamos con la dificultad añadida de que nos enfrentamos a una materia de libre elección, en la cual los alumnos cuentan con unos conocimientos de partida sobre administración de redes y S.O. muy variables. Esto requiere por parte del profesorado un ejercicio de planificación

[9] `http://www.wireshark.org`

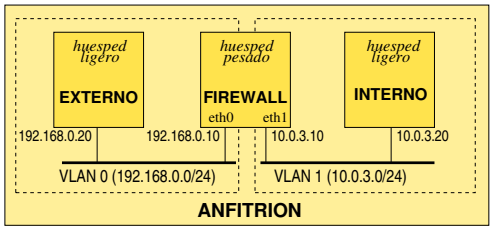

Figura 2: Configuración de red para prácticas simples con cortafuegos

y estructuración de las actividades prácticas que guíe paso a paso al alumno en las distintas tareas a realizar. Afortunadamente, el tipo de entorno que hemos creado se adapta fácilmente a este tipo de actividades guiadas. El grueso de las tareas de configuración de los huéspedes ya fue realizado de antemano y la intervención del alumno se limita a iniciar esas imágenes y trabajar con ellas.

En nuestro caso, además de adaptar la actividad anterior de intercepción de mensajes para su desarrollo por parte del alumno, hemos propuesto otras dos actividades guiadas. En una de ellas, empleando el mismo esquema de red de la Figura 1, se describe paso a paso una sesión de escaneo de puertos utilizando la herramienta NMAP[10], tanto desde el punto de vista del equipo que realiza el análisis, como desde la visión del equipo analizado. La otra actividad guiada realizada es mucho más extensa, y aborda las técnicas básicas de configuración de cortafuegos en GNU/Linux. Se emplean dos VLANs con la topología mostrada en la Figura 2, donde las tareas de cortafuegos son realizadas por un *huésped pesado*, que separa la red interna de la externa. En esta actividad los alumnos experimentan con varias opciones de configuración para un cortafuegos de borde, analizando el uso de políticas restrictivas (*denegar por defecto*) y permisivas (*aceptar por defecto*), para comprobar la dicotomía entre facilidad de administración *vs.* protección.

[10] http://www.nmap.org

4.3. Desarrollo de proyectos autónomos

Un paso más en el uso de entornos virtualizados en la docencia de la seguridad informática pasa por proponer ejercicios más complejos, donde los alumnos cuenten con mayor autonomía para experimentar y proponer sus propias alternativas y soluciones. En el presente curso planeamos añadir a las actividades guiadas, otras de carácter opcional mucho más abiertas y donde es necesaria una mayor implicación del alumno. Nuestra intención es plantear entornos de red más complejos, aprovechando la posibilidad que ofrece QEMU de establecer VLANs entre huéspedes ubicados en distintas máquinas anfitrión. De modo que varios estudiantes podrán trabajar en equipo. Sobre ese contexto se plantean dos posibles trabajos prácticos:

- Análisis de vulnerabilidades, usando la herramienta NESSUS[11], y propuesta de subsanación de las amenazas detectadas. El huésped analizado ejecutará *Damm Vulnerable Linux*[12], una distribución extremadamente insegura, con componentes software no actualizados y configuraciones por defecto inseguras; diseñada como banco de pruebas para trabajos de seguridad.
- Implementación de topologías complejas de cortafuegos. Se propone la definición de *zonas desmilitarizadas (DMZ)* mediante el uso de cortafuegos dobles, sobre los cuales se podrán evaluar distintas configuraciones y verificar la vulnerabilidad de los diferentes dominios de seguridad establecidos en la red frente a ataques procedentes del exterior.

5. Evaluación y conclusiones

El entorno propuesto persigue cubrir una parte de las necesidades de la docencia práctica de seguridad informática que, en el caso de nuestro centro, entendemos

[11] http://www.nessus.org
[12] http://www.damnvulnerablelinux.org/

que no estaban totalmente cubiertas. En concreto, pretendemos permitir que los alumnos ejerciten de un modo controlado sus habilidades técnicas y de gestión para implantar y administrar sistemas de red complejos. Antes de la adopción de este tipo de entornos virtualizados, la única opción posible era la realización de estos ejercicios sobre equipos reales del laboratorio docente. Lo que acarreaba múltiples dificultades y quejas por parte de otros usuarios, que nos llevaron a desistir y a que durante varios cursos se omitieran este tipo de actividades.

Nuestra experiencia con el uso de estas aproximaciones es altamente satisfactoria y aunque en un principio fue muy limitada, con un uso meramente demostrativo, ha sido relativamente fácil extenderla al modelo de prácticas guiadas y los resultados obtenidos por el alumnado han sido positivos. La experiencia con prácticas autónomas aún está en sus inicios y las dificultades previsibles son muchas, sobre todo las derivadas de contar con un entorno deliberadamente aislado, que no permite la conexión con el exterior y dificulta la instalación de nuevas aplicaciones o el intercambio de ficheros de configuración.

Desde el punto de vista del alumno, la gran ventaja de este método es que le permite enfrentarse a entorno casi real, donde la posibilidad de experimentación sin riesgos favorece la curiosidad y fomenta su trabajo independiente. En nuestro caso concreto, al tratarse de una materia de libre elección, el disponer de un entorno preconfigurado y el plantear prácticas guiadas, permite que alumnado con poca experiencia en redes y S.O. realice un acercamiento "apacible" a los temas relacionados con la administración segura de sistemas. Por otro lado, se ha constatado un mejor aprovechamiento del tiempo de docencia práctica y una buena predisposición por parte del alumnado, debido principalmente al tipo de prácticas propuestas, que suelen resultan atractivas para buena parte de nuestros estudiantes.

Por último, en cuanto a la posible evolución futura de la aproximación descrita en este trabajo, además de promover el trabajo autónomo, una propuesta especialmente interesante es la de fomentar que los alumnos elaboren y compartan sus propias prácticas guiadas. Estos trabajos versarían sobre temas que resultaran de interés para el alumno y tendrían como finalidad la construcción de un repositorio de imágenes QEMU y de guías de prácticas que hicieran uso de ellas.

Referencias

[1] F. Bellard, *Virtualización* QEMU +KQEMU, `http://fabrice.bellard.free.fr/qemu/`

[2] H. Bulbrook, *Using virtual machines to provide a secure teaching lab environment*, whitepaper, Durham Technical Community College.

[3] J.A. Gil, F.J. Mora *et al.*, *Entorno de red virtual para la realización de prácticas realistas de administración de sistemas operativos y redes de computadores*, XI Jornadas de la Enseñanza Universitaria de la Informática, JENUI'2005, 2005.

[4] P. Gómez, *Maquinas virtuales en las clases de informática*, XII Jornadas de la Enseñanza Universitaria de la Informática, JENUI'2006, 2006.

[5] J. Hu, D. Cordel, C. Meinel, *A virtual laboratory for IT security education*, Proc. of EMISA'2004, Luxemburgo.

[6] P.Y. Logan, *Crafting an undergraduate information security emphasis within information technology*, Journal of Information System Education, Vol. 13(3), 2002

[7] P.Y. Logan, *Teaching students to hack: Curriculum issues in information security*, Proc. of SIGCSE 2005, Vol. 37(1), 2005.

[8] K. Wong, T. Wolf, S. Gorinsky, J. Turner, *Teaching experiences with a virtual network laboratory*, Proc. of 38th Technical Symposium on Computer Science Education, 2007.