Concepción, Diseño e Implantación de un Laboratorio de Seguridad Informática

María Eugenia Corti, Marcelo Rodriguez, and Gustavo Betarte

Grupo de Seguridad Informática, Instituto de Computación, Facultad de Ingeniería, Universidad de la República
J. Herrera y Reissig 565, Montevideo, Uruguay
[mcorti,marcelor,gustun]@fing.edu.uy
http://www.fing.edu.uy/inco

Resumen El creciente interés, tanto a nivel académico como industrial, por la seguridad de la información, y en particular en la seguridad informática, repercute en la necesidad y demanda de programas educativos y proyectos de investigación abocados a esta temática. Un componente importante de soporte a estas actividades es contar con un laboratorio apropiadamente diseñado e implantado donde se puedan realizar prácticas y experimentos.
Este artículo describe en detalle las opciones analizadas así como la metodología utilizada para el diseño, implantación y explotación del Laboratorio de Seguridad (LaSI) implementado por el Grupo de Seguridad Informática (GSI) de la Facultad de Ingeniería de la Universidad de la República (Uruguay).

Keywords: Laboratorio de Seguridad Informática, Seguridad de la Información, Virtualización.

1. Introducción

En estos últimos años se ha incrementado en forma sustancial el interés en la seguridad de la información en general y en particular de la seguridad informática. Esto incentiva la realización de programas educativos y proyectos de investigación en esta área.

Un aspecto importante de implementar un programa de formación, capacitación e investigación en seguridad informática es brindar a los involucrados un ámbito donde poner en práctica los conceptos aprendidos, refinar las habilidades, realizar pruebas adecuadas y experimentar con tecnologás y aplicaciones. Un lugar equipado para la experimentación, observación, práctica y prueba usualmente requiere, entre otros aspectos, una inversión significativa en hardware, dispositivos de red, cableados y equipamiento informático en general.

Por otro lado, para un laboratorio de estas características es necesario disponer de una infraestructura aislada de los sistemas en producción, donde poder experimentar sin interferir con el funcionamiento normal de otros sistemas. La plataforma a utilizar debe permitir la instalación, configuración, funcionamiento

y evaluación de herramientas de seguridad informática, así como el análisis en condiciones controladas, de vulnerabilidades y ataques a los sistemas operativos y servicios.

Según se especifica en [1], las características mínimas que debe cumplir un laboratorio apropiadamente diseñado son las siguientes:

- *Reconfigurable:* Diferentes temas a investigar o prácticas a realizar requieren diferentes configuraciones, ya sea de sistemas operativos o topologías de red. Debe ser posible modificar la configuración del laboratorio de forma fácil y eficiente.
- *Heterogéneo:* Debe involucrar diferentes plataformas de diferentes proveedores.
- *Escalable:* Debe poder crecer fácilmente y debe soportar un número importante de usuarios sin que la performance se vea degradada.
- *Rentable:* El costo de configuración y mantenimiento debe ser considerablemente menor al costo de lo que se está intentando simular.
- *Robusto:* Debe poder soportar y reponerse rápidamente de daños producidos por los usuarios o por las propias instalaciones o pruebas que se estén realizando.
- *Mantenible:* Debe ser fácil de mantener. Tareas como respaldos, aplicación de parches o actualizaciones deben ser fáciles de realizar y lo más automatizadas posibles.
- *Realista:* Debe proveer escenarios que sean lo más próximos posibles a la realidad.
- *Aislado:* Las actividades del laboratorio no deben afectar a otras instalaciones.

Este artículo evalúa diferentes opciones de arquitecturas para implementar laboratorios de seguridad y describe la arquitectura y metodología utlizada en la implementación del Laboratorio de Seguridad Informática (LaSI) del Grupo de Seguridad Informática (GSI) de la Facultad de Ingeniería de la Universidad de la República (Uruguay). La idea inicial de diseñar e implantar un laboratorio de seguridad surge en el marco de un convenio con la Administración Nacional de TELecomunicaciones (ANTEL), con el objetivo de contribuír en el análisis de la viabilidad de organizar, instalar y desarrollar un Computer Emergency Response Team (CERT) nacional. El LaSI ha sido concebido en una primera instancia como centro de concentración de las actividades de formación e investigación en los aspectos relacionados a la seguridad informática.

El resto de este artículo esta estructurado como se describe a continuación. La sección 2 describe y analiza diferentes diseños posibles para la implantación de un laboratorio de seguridad informática. La sección 3 describe el diseño y tecnología adoptados por el GSI para consolidar la implantación del laboratorio. En la sección 4 se reseña el enfoque metodológico utilizado para el desarrollo de experimentos sobre el ambiente provisto por el LaSI. La sección 5 concluye y describe trabajo futuro.

2. Criterios para el Diseño de un Laboratorio de Seguridad

Existen diversos trabajos [2,3,4,5] que abordan la temática de la implementación de laboratorios de enseñanza e investigación en el área de seguridad informática. Varios de estos trabajos resaltan la importancia de considerar un diseño de laboratorio aislado y heterogéneo. Por las características de las prácticas a realizar es posible que se requiera de variados sistemas operativos para un mismo ejercicio. Asimismo, factores como la generación de flujos de tráfico elevados, así como la utlización de herramientas especializadas, podría perjudicar el normal funcionamiento de una red. Como se menciona en [3] el objetivo para los investigadores en el uso de laboratorios de seguridad es poder utilizarlos como un campo de experimentación sin preocuparse por las consecuencias negativas.

A continuación discutiremos las ventajas y desventajas de algunas opciones de diseño de laboratorios de seguridad.

2.1. Opciones de arquitectura

Existen diferentes opciones de arquitectura para un laboratorio de seguridad teniendo en cuenta las configuraciones de hardware y software necesarias. A continuación se describen algunas de ellas y se exponen las ventajas y desventajas de las mismas.

PCs potenciados y servidores. Esta es una arquitectura donde se cuenta con un número de PCs con una configuración de hardware que no represente una limitación a la hora de ejecutar las aplicaciones o sistemas operativos necesarios, y un conjunto de servidores que faciliten el acceso a archivos o imágenes.

Esta aquitectura presenta varias desventajas desde el punto de vista de un laboratorio de seguridad informática. Un laboratorio de estas características necesita tener diversidad de sistemas operativos ejecutándose para una misma práctica. Con esta arquitectura, se necesitaría un PC por cada sistema operativo a ejecutar, con el aumento en los costos que esto significa. Necesitando además, una configuración con booteo múltiple ya sea utilizando múltiples particiones o discos extraíbles, dificultando las tareas de mantenimiento y recuperación.

Si bien existen herramientas que permiten emular la ejecución en diferentes sistemas operativos, esto solamente permitiría la ejecución de algunas aplicaciones, limitando la variedad de configuraciones que se pueden simular. Por otro lado la escalabilidad de la infraestructura se ve limitada a la compra de más PCs.

PCs estándares y Terminal Servers. Una arquitectura utilizando Terminal Servers permite reducir el costo de recursos en los PCs aumentando el de los servidores, que deben ser potenciados. En esta arquitectura los PCs clientes visualizan en forma remota diferentes sesiones iniciadas en el servidor.

Una de las ventajas de esta arquitectura, además de la disminución de los costos de la configuración de los PCs, es la posibilidad de trabajar con diferentes sistemas operativos en un mismo PC. Por otro lado las tareas de reconfiguración y mantenimiento se limitan a las asociadas a los servidores donde se ejecuta el Terminal Server. Una desventaja de esta solución es que los diferentes usuarios compiten por los recusos del servidor, sin posibilidad de asignarlos en forma independiente. Esto requiere una planificación previa adecuada, en el caso de tener múltiples usuarios, para no disminuír la performance del laboratorio y que las prácticas efectuadas por diferentes usuarios interfieran unas con otras.

PCs estándares y Máquinas Virtuales. En esta arquitectura varios PCs actúan como clientes visualizando o interactuando con máquinas virtuales que se ejecutan en el servidor. Las máquinas virutales pueden configurarse con diferentes sistemas operativos.

Esta solución permite ejecutar en un mismo cliente varias máquinas con diferenes sistemas operativos, permitiendo heterogeneidad, con consumo de recursos únicamente en el servidor. Otra ventaja de esta arquitectura es la facilidad para reconfigurar y mantener. Una máquina se instala y configura por única vez con el sistema operativo y software necesario y puede luego ser distribuída sin necesidad de volver a reinstalar. Además, si la máquina es dañada o destruída en alguna de las prácticas, la tarea de configurar nuevamente la máquina o el escenario, se limita a la copia de archivos. Por otro lado, en un servidor con recursos suficientes, múltiples máquinas pueden ejecutarse simultáneamente permitiendo flexibilidad y escalabilidad en el diseño de escenarios de trabajo. Se suma a lo anterior la facilidad con la que se pueden armar diferentes escenarios con configuraciones de red complejas, como la presentada en la Figura 1.

2.2. Opciones de conectividad

Debido a que usualmente las herramientas y aplicaciones que se ejecutan en un laboratorio de seguridad, pueden perjudicar el funcionamiento de los equipos o la red a la que están conectados, es conveniente que el mismo esté lo más aislado posible.

Una primera opción podría ser que el mismo se encontrara desconectado totalmente de la red de producción. De esta forma, se tiene total certeza que las prácticas que se lleven acabo en el mismo no serán perjudiciales. Esto puede limitar algunas operaciones necesarias durante las prácticas como sería el acceso a Internet o a algún otro recurso de la red. En estos casos una solución es utilizar un firewall para controlar el tráfico saliente o entrante al laboratorio. Un acceso controlado y continuamente monitoreado permite conectar la red del laboratorio a la red de producción minimizando los niveles de riesgo. Por otro lado, el laboratorio de seguridad debe contar con una política de seguridad que establezca claramente los accesos permitidos y el buen uso del mismo.

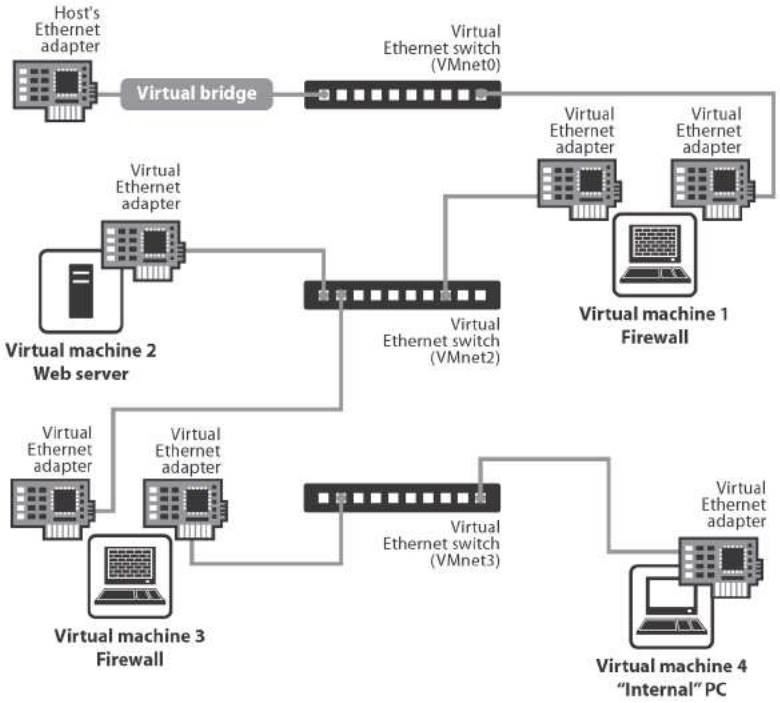

Figura 1. Red Virtual usando VMWare Server [6]

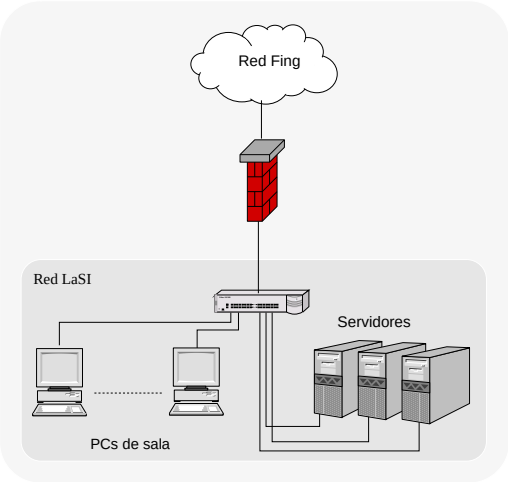

Figura 2. Arquitectura del LaSI

3. Diseño e implementación del LaSI

El objetivo principal que ha guiado la creación del LaSI es que éste sirva de ambiente para el desarrollo de actividades de experimentación, investigación y enseñanza de la seguridad informática. Un requerimiento básico es además que este laboratorio opere aislado de los sistemas de producción. A estos requerimientos se agrega la condición que los servicios que provee el laboratorio puedan ser explotados desde una sala de laboratorio de uso compartido del Instituto de Computación (InCo) de la Facultad de Ingeniería. Esta sala es compartida por múltiples actividades docentes y estudiantiles, lo que implica que cualquier modificación de configuración que se realice directamente sobre la infraestructura informática de la misma podría afectar las otras actividades allí realizadas.

En este contexto, se decidió que el modelo de laboratorio de seguridad a implantar seguiría los lineamientos de la arquitectura *PCs estándares y Máquinas Virtuales* descripta en la sección anterior. Más precisamente, la solución adoptada consiste en utilizar la infraestructura física (PCs, switches, cableado, etc) provista por el salón de uso compartido para desde allí acceder a la red de máquinas virtuales que realmente conforman el laboratorio.

En las siguientes secciones se describe la arquitectura y los componentes de hardware y software del LaSI.

3.1. Arquitectura

Las PCs de la sala de uso compartido conforman la base física a través de la cual los estudiantes o investigadores se conectan a las máquinas virtuales del laboratorio. Tres servidores se encargan de soportar el entorno donde se

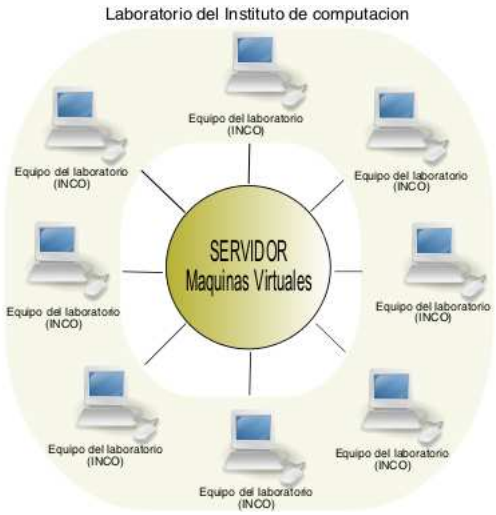

Figura 3. Arquitectura virtual del LaSI

ejecutan las máquinas virtuales. La infraestructura informática del laboratorio está conformada por los servidores, las máquinas virtuales y los PCs de la sala.

Los PCs se comportan como simples terminales para la ejecución de las máquinas virtuales. Servidores y PCs se encuentran en una misma subred, mientras que las máquinas virtuales están contenidas en una red virtual. La red de servidores y PCs es separada de la red de producción por un firewall que controla los accesos desde y hacia los mismos. La Figura 2 y la Figura 3 ilustran la arquitectura del LaSI, mostrando la primera la conectividad con la red de producción y la segunda la interacción entre la red virtual y el conjunto de PCs.

3.2. Componentes de hardware

Los componentes de hardware se dividen en dos grupos: los servidores y los PCs del salón estudiantil.

Los servidores son tres unidades Sun Fire X2100 x64 Server equipados con 2GB de memoria. Los PCs, cuya única función es comportarse como puestos físicos de trabajo para cumplir el rol de clientes del laboratorio virtual, son equipos Pentium IV con 512 MB de memoria cada uno.

3.3. Componentes de software

Los servidores del LaSI ejecutan el sistema operativo CentOS versión 4.4. Sobre este sistema se alza la infraestructura de máquinas virtuales utilizando Vmware Server [6]. Vmware Server fue elegido entre otras herramientas de similares características, como Microsoft Virtual PC [7] and Virtual Server [8],

QEMU [9] y Xen [10], por su portabilidad y capacidad para crear redes virtuales totalmente independientes.

Además de los anteriores, existe otro producto llamado Vmware Player [11], totalmente compatible con la versión Server, que permite ejecutar en forma independiente una máquina virtual. Esto resulta útil en caso de querer distribuir alguna de las instalaciones o para generar un ambiente en el cual no se cuenta con un servidor que fuera capaz de soportar la carga de trabajo.

En lo que respecta a la portabilidad, Vmware Server puede ser instalado tanto en Windows como en Linux y las máquinas virtuales generadas se ejecutan indistintamente sobre cualquiera de estos sistemas operativos. La elección del sistema operativo de los servidores se vio influenciada por el software de virtualización seleccionado (Vmware Server). No existen versiones de estos productos para Solaris, esto limita la elección del sistema operativo base a Windows o Linux. La distribución del sistema operativo base seleccionado (CentOS) está pensada para servidores, está basada y es totalmente compatible con RedHat Enterprise Server y es distribuida en forma libre.

La configuración del software instalado en los PCs de la sala informática depende de la Unidad de Recursos Informáticos (URI) de la Facultad de Ingeniería. Los únicos requerimientos solicitados a la URI fueron la creación de usuarios para poder ingresar a los equipos de trabajo y la instalación del producto vmware-server-client. De esta manera el impacto generado sobre estas estaciones de trabajo por las diferentes prácticas es mínimo y no perjudica a los otros usuarios del laboratorio. El vmware-server-client es la herramienta que permite conectarse al Vmware Server y seleccionar las máquinas virtuales en las que se va a trabajar.

3.4. Principales características del LaSI

La utilización de virtualización permite particionar un único servidor físico en múltiples máquinas virtuales, que pueden definirse con variadas características de hardware y en las que se pueden instalar diversos sistemas operativos y aplicaciones. Esto se convierte en una plataforma ideal para los objetivos del laboratorio de proveer una infraestructura que permita el testeo y evaluación de sistemas y aplicaciones diversas y el dictado de cursos y talleres en el área de seguridad. Esto permite cumplir con la característica de *heterogeneidad* deseada.

La implementación de máquinas virtuales permite un mejor aprovechamiento del hardware y brinda la flexibilidad necesaria para permitir la experimentación con un costo no demasiado excesivo. Esto lo convierte en *rentable*.

La posibilidad de poder crear una máquina virtual y realizar varias copias de la misma, facilita el armado de prácticas de cursos y talleres de formación y la rápida repetición de los mismos y de cualquier experimentación o práctica que se desee realizar, satisfaciendo así la característica de *robusto* y *mantenible*.

Mediante la configuración de switches virtuales es posible soportar hasta 10 redes totalmente independientes entre sí. A su vez, cada uno de estos switches pueden conectar 32 maquinas virtuales en forma simultánea. Esto ofrece una gran potencia al momento de planificar los entornos de trabajo para cada una

de las prácticas. Estas características contribuyen a que el ambiente sea *realista*, *escalable* y *reconfigurable*.

Por otro lado, la utilización de un firewall que controla el acceso desde y hacia la red de producción, garantiza que las prácticas que se realicen no interfieran con otras actividades, lo que refleja la característica de *aislado* del laboratorio.

De esta forma el diseño seleccionado para la implementación del LaSI cumple con las principales características requeridas en [1] para un laboratorio de seguridad.

4. Metodología de trabajo

En esta sección se describe brevemente la metodología de trabajo utilizada para el diseño, armado y ejecución de las prácticas que han sido definidas en el contexto del dictado de un curso introductorio a la Seguridad Informática. Se describe además en detalle una de estas prácticas, específicamente la que le permite al estudiante entender cómo funciona un ataque de *Man in the Middle*. El objetivo es ilustrar el framework conceptual y metodológico que posibilita la infraestructura del laboratorio.

4.1. Contexto de trabajo

El equipo de trabajo responsable del curso está dividido en dos grupos: uno encargado de la planificación y dictado de la parte teórica del mismo y un segundo grupo a cargo de la parte práctica.

Como se mencionó en la sección anterior tres servidores componen el LaSI. Uno de ellos es utilizado como plataforma de desarrollo de laboratorios y los otros dos como plataforma de producción. La plataforma de desarrollo es accedida solamente por los miembros del grupo asignado a la planificación e implementación de las prácticas, mientras que la plataforma de producción puede ser accedida por todos los participantes del curso en el momento de la práctica.

Para facilitar la definición de las diferentes prácticas se crearon máquinas virtuales base con variados sistemas operativos. Esto permite disponer fácilmente de dichos sistemas operativos sin tener que instalarlos desde cero. Para la elaboración de una práctica simplemente se seleccionan las máquinas necesarias del conjunto ya disponible y se las prepara según las necesidades de la misma.

En la actualidad se cuenta con máquinas base con los siguientes sistemas operativos:

- Windows 98
- Windows XP
- Windows 2003
- Linux OpenSuse
- Linux Read-Hat 8
- Linux Fedora Core 4
- Linux Fedora Core 5

4.2. Preparación de una práctica

Para una mayor claridad dividiremos la metodología utilizada para la preparación de una práctica en diferentes etapas, que cubren desde la planificación hasta la ejecución de las mismas.

Etapa 1- Planificación En esta etapa los integrantes del grupo encargado de las prácticas estudian el tema a desarrollar, previamente definido, y se discuten las posibles prácticas a desarrollar para los diferentes temas abordados en el teórico. Se estudian las herramientas disponibles, se plantea el escenario en el cual se desarrollará la práctica y se evalúa la infraestructura necesaria para montar el mismo. Se determinan cuántas máquinas virtuales serán necesarias, qué sistema operativo deben tener y qué software deben ejecutar. Se asignan, además, las diferentes tareas que deberá realizar cada integrante del grupo.

Etapa 2- Preparación Una vez establecida la infraestructura, cada integrante procede a preparar las máquinas virtuales que se utilizarán en la práctica que tiene asignada (puede ser más de una máquina). Para ello toma del conjunto de máquinas base las adecuadas y las acondiciona instalándole las herramientas necesarias, particulares de la práctica, que no se encuentran en la instalación base. Estas actividades se llevan a cabo sobre la plataforma de desarrollo.

Etapa 3- Prueba y armado Cuando se tiene preparado el ambiente se procede a testear la práctica y a escribir la documentación que servirá de guía a los participantes. Luego de afinados todos los detalles, se procede a replicar el ambiente preparado en la plataforma de producción para que quede disponible para trabajar. El mismo escenario es replicado tantas veces como sea necesario, dependiendo de la cantidad de asistentes a la práctica y de forma de que sea mínimo el número de participantes que deberán trabajar sobre el mismo a la vez.

Etapa 4- Ejecución Luego de que todos los escenarios están replicados y todo está configurado se procede a la ejecución de la práctica. Se entrega a cada participante la documentación que lo guiará, el encargado de la práctica realiza una breve introducción en el tema, explicando en que consistirá la práctica y cuales serán los resultados esperados.

4.3. Prácticas del curso de Fundamentos de la Seguridad Informática

En el primer semestre del año 2007 el GSI dictó una asignatura opcional [12] del plan Ingeniero en Computación. La metodología de enseñanza utilizada consiste en presentaciones teóricas y prácticas desarrolladas en el ambiente provisto por el LaSI.

El contenido teórico de este curso ha sido estructurado en los siguientes módulos:

- **Introducción:** Se realiza una breve introducción a los conceptos básicos de seguridad informática.
- **Criptografía aplicada**: Se introducen conceptos básicos de criptografía, se resaltan los aspectos de seguridad asociados a la misma y se ven algunos ejemplos de criptografía aplicada.
- **Seguridad de Sistemas**: Se muestran los mecanismos de seguridad utilizados en los sistemas operativos más utilizados y cómo los mismos intentan garantizar la integridad y confidencialidad de la información.
- **Seguridad en Redes**: Se describen los principales problemas de seguridad asociados a las redes de datos. Se visualizan algunas soluciones implementadas.
- **Seguridad en las Aplicaciones**: Se señalan las principales vulnerabilidades de las aplicaciones y se muestran algunas buenas prácticas de programación y configuración.
- **Seguridad en Bases de Datos**: Se reseñan los diferentes modelos de control de acceso implementados en RDBMs comerciales y de investigación. Se introducen los vectores de ataques en Bases Estadísticas.

A continuación se describen brevemente las prácticas diseñadas y ejecutadas para algunos de estos módulos.

Criptografía aplicada Esta práctica está compuesta de cuatro partes. La primera de ellas está dedicada a ataques del tipo Man in the Middle (MitM). Tiene como objetivo generar conciencia sobre cómo afectan los mismos a la confidencialidad de los datos transmitidos y cómo la utilización de algoritmos criptográficos logra mitigar el riesgo asociado. La segunda parte está orientada a revisar el concepto de algoritmos de hash, en particular MD5. Se enfatiza el tema de las colisiones producidas en este algoritmo. Se muestra en forma práctica como a partir de un texto y un valor de hash, se puede generar un texto diferente con el mismo valor de hash. En la tercera parte se ponen en práctica los conceptos de infraestructura de clave pública (PKI). Sobre una entidad certificadora, instalada para este fin, se realizan prácticas de solicitud, generación e instalación de certificados. Se pretende familiarizar al practicante con los diferentes servicios y componentes de una infraestructura de clave pública. Por último se ven ejemplos de croptografía aplicada sobre el servicio de correo electrónico. Se utilizan dos tecnologías diferentes (PGP y S/MIME) para transmitir correo electrónico seguro entre dos partes, poniendo en práctica los conceptos de criptografía simétrica y asimétrica, junto a la noción de firma digital.

Seguridad de Sistemas El propósito de las prácticas asociadas a este módulo es introducir a los asistentes en los problemas relacionados con la seguridad de los sistemas informáticos y luego estudiar algunas herramientas que proponen

soluciones. Asociado a los problemas se realizaron prácticas que ilustran técnicas para el crackeo de contraseñas y técnicas para escalar privilegios. Relacionado a las soluciones que se pueden implementar para disminuir los riesgos asociados a problemas de seguridad en los sistemas, se configuraron prácticas que permiten visualizar herramientas que contribuyen al fortalecimiento de contraseñas. Además se trabaja en la configuración de sistemas de detección de intrusos en los hosts (HIDS), que permiten entre otras cosas, verificar la integridad de los archivos y detectar cuando los mismos han sido modificados. Por último se muestra en forma práctica los sistemas operativos que integran módulos de seguridad pensados para proteger la integridad y confidencialidad de los datos que manejan, se ve el funcionamiento y la configuración de los mismos.

Seguridad en Redes Las prácticas asociadas a este módulo introducen herramientas para prevenir y detectar ataques vinculados a las redes de datos. Como parte de las mismas se instala y configura un sistema de detección de intrusos en la red (NIDS), se visualiza cómo este tipo de herramientas permite detectar ataques como la denegación de servicios y aquellos realizados a vulnerabilidades específicas de algunos servicios. Se configura además un firewall utilizando herramientas de configuración gráficas. Por otro lado se ponen en práctica los conceptos de certificados digitales con la configuración de una red privada virtual (VPN) entre dos equipos, utilizando el protocolo SSL/TLS.

Seguridad en las Aplicaciones En este módulo las prácticas definidas tienen como objetivo introducir a los participantes en los problemas de seguridad asociados a vulnerabilidades en las aplicaciones. Se practican ataques a vulnerabilidades del tipo Buffer Overflow. Además, se instaló y configuró la herramienta WebGoat que permite a los participantes practicar diferentes formas de ataque como ser: SQL injection, Cross-Site Scripting, Injection Flaws, etc. Ilustrando de esta forma las vulnerabilidades más comunes de las aplicaciones. Por último se montó la infraestructura necesaria para poner en funcionamiento la herramienta Hacme Bank [13], la cual simula en forma real una aplicación de banca online. Esta aplicación fue construida conteniendo, de forma intencional, vulnerabilidades comunes y conocidas. Utilizando la misma los participantes logran comprender en la práctica los ataques que se realizan sobre este tipo de aplicaciones Web.

4.4. Discusión de una práctica: *Man in the Middle*

Man in the middle (MitM) es un ataque donde el atacante intenta entrometerse, sin ser detectado, en una comunicación entre dos equipos pertenecientes a una red (víctimas) con el fin de obtener y/o modificar la información que éstas intercambian.

Con la definición anterior en mente, el grupo encargado de planificar y preparar la práctica se propone crear un ambiente en el cual se puedan utilizar las herramientas tcpdump [14], ethereal [15] y ettercap [16] para realizar el ataque.

Además se plantea que las máquinas víctimas no se encuentren en el mismo dominio de colisión (red con switch) para que los participantes tengan que efectuar necesariamente un ataque de *ARP Spoofing* [17] para poder tener éxito en el *MitM*.

En este contexto, el escenario resultante consta de tres hosts o máquinas: **atacante**, **víctima1** y **víctima2**. Para crear el atacante se toma, del repositorio de máquinas base, una de las máquinas virtules linux y se le instala las herramientas necesarias. Las víctimas son generadas apartir de una máquina con una instalación mínima, la víctima1 será el servidor de una comunicación cuyo protocolo no utilizará criptografía para que el atacante tenga éxito (por ejemplo: telnet, pop3, http, etc) y la víctima2 será el cliente de dicha comunicación. También se crean *scripts* para que la comunicación entre las víctimas se realice automáticamente y sin intervención de usuarios.

Luego de replicado el escenario, tantas veces como participantes realicen la práctica, se les brinda acceso a las máquinas atacantes y se les plantea el desafío de encontrar un mensaje que se transmite entre las dos víctimas asignadas.

Claramente un inconveniente de este enfoque se encuentra en que son necesarias tres máquinas por cada participante, se puede llegar a utilizar el mismo servidor (víctima1) para todos los participantes, pero de todas maneras son necesarias por lo menos dos máquinas para cada uno. Sin duda, esta limitante acota el número de participantes que puede realizar la práctica en forma simultánea, delimitando dicho número a la capacidad de procesamiento y el espacio en disco de los servidores del laboratorio.

5. Conclusiones y Trabajo Futuro

Si bien el diseño original del LaSI consideraba que los usuarios del mismo accederian a los servicios provistos por el laboratorio utilizando terminales, el incremento en el número de estudiantes a los cursos, la premisa de no aumentar el número de estudiantes por grupo y la arquitectura de las prácticas llevó a que se necesitaran utilizar los PCs del salón como parte del laboratorio.

Por otro lado, para las prácticas implementadas para el curso, el número de máquinas virtuales utilizadas es directamente proporcional al número de grupos de estudiantes que participan de las mismas, situación que es necesaria revertir.

La problemática, planteada oportunamente en el ejemplo de *Man in the middle*, de multiplicar las máquinas virtuales (VMs) para crear el escenario de cada participante es inherente a la técnica de virtualización utilizada por la herramienta VMware. Dicha herramienta emula una plataforma de hardware real y el sistema operativo que se instala sobre la plataforma no se entera quese está ejecutando sobre una VM.

Existes otras técnicas de virtualización como son la *paravirtualización* y la *virtualización a nivel del sistema operativo* [18]. La virtualización a nivel de sistema operativo permite fácilmente compartir recursos entre diferentes VMs, algo similar ocurre en la paravirtualización. Compartir recursos entre diferentes

VMs genera la posibilidad de no tener que multiplicar la máquina ante una nuevo participante y de esta manera optimizar la utilización de los recursos.

Surge entonces como trabajo futuro, a corto plazo, el estudio y la aplicación en el laboratorio de productos que implementen virtualización a nivel del sistema operativo (por ejemplo *OpenVZ* [19]) y paravirtualización (por ejemplo *User Mode Linux* [20]). Se plantea analizar cada uno de los paradigmas de virtualización y los productos relacionados para integrarlos en un mismo laboratorio y de esta manera aprovechar las ventajas de cada uno de ellos.

A largo y mediano plazo se plantea el estudio y la concepción de un *framework* que facilite y automatice la creación de nuevas prácticas de laboratorio, dicho framework contemplaría también los mecanismos de evaluación de cada práctica. Una iniciativa similar a ésta se plantea en el proyecto *Tele-Lab* [21], desarrollado por el departamento de ciencias de la computación de la Universidad de Trier en Alemania.

Referencias

1. T. Andrew Yang, Kwok-Bun Yue, Morris Liaw, George Collins, Jayaraman T. Venkatraman, Swati Achar, Karthik Sadasivam, and Ping Chen. Design of a distributed computer security lab. *J. Comput. Small Coll.*, 20(1):332–346, 2004.
2. Herbert J. Mattord and Michael E. Whitman. Planning, building and operating the information security and assurance laboratory. In *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development*, pages 8–14, New York, NY, USA, 2004. ACM Press.
3. John M. D. Hill, Jr. Curtis A. Carver, Jeffrey W. Humphries, and Udo W. Pooch. Using an isolated network laboratory to teach advanced networks and security. *SIGCSE Bull.*, 33(1):36–40, 2001.
4. Harry Bulbrook. Using Virtual Machines to Provide a Secure Teaching Lab Environment. http://www.infosecwriters.com/text_resources/pdf/Virtual_Machines_HBulbrook.pdf, (última visita Agosto 3, 2007).
5. Alec Yasinsac, Jennifer Frazier and Marion Bogdanov. Developing an Academic Security Laboratory. In *6th National Colloquium for Information Systems Security Education*, 2002).
6. Inc. VMware. Virtual Machine Guide. Vmware Server 1.0. http://www.vmware.com/pdf/server_vm_manual.pdf, (última visita Agosto 3, 2007).
7. Microsoft Corporation. Microsoft Virtual PC 2007. http://www.microsoft.com/windows/virtualpc/default.mspx, (última visita Agosto 3, 2007).
8. Microsoft Corporation. Microsoft Virtual Server. http://www.microsoft.com/windowsserversystem/virtualserver/default.aspx, (última visita Agosto 3, 2007).
9. Fabrice Bellard. Open Source Processor Emulator. http://fabrice.bellard.free.fr/qemu/, (última visita Agosto 3, 2007).

10. University of Cambridge. Xen. http://www.cl.cam.ac.uk/research/srg/netos/xen/, (última visita Agosto 3, 2007).
11. Inc. Vmware. VMware Player. http://www.vmware.com/products/player, (última visita Agosto 3, 2007).
12. Grupo de Seguridad Informática-Facultad de Ingeniería. Fundamentos de la Seguridad Informática. http://www.fing.edu.uy/inco/cursos/fsi, 2007.
13. Shanit Gupta. Foundstone Hacme Bank v2.0. Software Security Training Aplication, (última visita Agosto 3, 2007).
14. Van Jacobson, Craig Leres and Steven McCanne. Tcpdump. http://www.tcpdump.org/, (última visita Agosto 8, 2007).
15. Alberto Ornaghi and Marco Valleri. Ettercap. http://ettercap.sourceforge.net/index.php, (última visita Agosto 8, 2007).
16. Ethereal Inc. Ethereal. http://www.ethereal.com/, (última visita Agosto 8, 2007).
17. G. Pulido, M. Niño, D. Lizarazo, G. Peñuela and L. Varela. Principios Básicos de ARP Spoofing: Arpoison, un primer paso para la incomunicación del servicio. http://www.criptored.upm.es/descarga/arppoisoning.zip, (última visita Agosto 9,2007).
18. Robert Rose. Survey of System Virtualization Techniques. http://citeseer.ist.psu.edu/rose04survey.html, (última visita Agosto 9, 2007).
19. SWsoft. OpenVZ. http://openvz.org, (última visita Agosto 9, 2007).
20. Jeff Dike. User Mode Linux. http://user-mode-linux.sourceforge.net/, (última visita Agosto 9, 2007).
21. Ji Hu, Christoph Mainel and Michael Schmitt. Tele-Lab IT Security: An Architecture for Interactive Lessons for Security Education. http://www.hpi.uni-potsdam.de/fileadmin/hpi/FG_ITS/papers/SIGCSE04.pdf, (última visita Agosto 9, 2007).