

Laboratorio virtual para la enseñanza de seguridad informática

Autores

Ing. Hugo Pagola, hpagola@fi.uba.ar

Ing. Alberto Dams, adams@fi.uba.ar

Juan Manuel Caracoche, jmcaracoche@gmail.com

Departamento de Electrónica, Facultad de Ingeniería, Universidad de Buenos Aires

Resumen

Adecuar un laboratorio de propósito general con computadoras PC, fácilmente disponible en cualquier ambiente educativo como el de nuestra Facultad para realizar prácticas de la materia Criptografía y Seguridad Informática. Lo ideal sería tener un laboratorio específico, pero la escasez de fondos no lo permite. Este artículo presenta una experiencia que estamos desarrollando en nuestro departamento para utilizar un sistema basado en un Linux (Sistema Operativo Libre) diseñado en forma específica como un bloque de construcción del laboratorio virtual. El CD permite construir ambientes complejos con redes de computadoras sin requerir hardware especial y contiene las herramientas necesarias para realizar los diversos trabajos de seguridad informática.

Palabras claves: Laboratorio de Seguridad Informática, tecnología en educación,

INTRODUCCION

El objetivo principal del trabajo es desarrollar una herramienta de uso educativo que permita a nuestro departamento disponer de un laboratorio de seguridad informática versátil y de bajo costo.

La meta del proyecto es construir un laboratorio donde los alumnos puedan desarrollar las actividades prácticas de nuestra materia “Criptografía y Seguridad Informática”, la cual es electiva tanto para los alumnos de Ingeniería Electrónica como para los alumnos de Ingeniería Informática de la FIUBA (Facultad de Ingeniería de la Universidad de Buenos Aires).

Entendemos importante que el estudiante sea capaz de atacar un problema, realizar la síntesis del mismo, elaborar una solución e implementarla con el apoyo del medio tecnológico que esta a su disposición.

Para desarrollar en todos ellos una “actitud científica” [3] acorde con nuestra profesión de ingenieros. La velocidad de cambios tecnológicos que tiene el área de conocimiento hace imprescindible abordar el aprendizaje de esta manera.

La mejor solución sería disponer de un laboratorio especial de uso exclusivo de la materia o de uso compartido con las materias de redes que nos permita interconectar varias redes. La falta de espacio y recursos impiden dicha opción. Sin embargo hay varios laboratorios de propósito general con computadoras conectadas a la red de la FIUBA. Estos laboratorios pueden ser usados pero no se permite en los mismos introducir cambios en los equipos ni en su conectividad.

Actualmente los SO permiten implementar redes virtuales, y la existencia de distribuciones Linux que inician desde CD nos acercó a la solución que adoptamos para el uso de dichos laboratorios.

OBJETIVOS

- Simplicidad de configuración del aula para un laboratorio: la configuración del aula debe poder ser llevada a cabo en pocos minutos para permitir que los estudiantes se focalicen en el aprendizaje y la resolución de problemas.

- No se debe modificar ni alterar la configuración de las computadoras del laboratorio: Permitiendo de esa manera no modificar el ambiente usado por las otras materias.
- Errores de configuración introducidos por otras materias en las computadoras no debe afectar a nuestro laboratorio.
- Simple de usar: Pero no facilitar totalmente su uso, ya que esta destinado a estudiantes de Ingeniería electrónica e Informática.
- Que los alumnos puedan replicar fácilmente las experiencias en otros ambientes como su casa.
- Posibilidad de implementar redes complejas sin modificaciones físicas de magnitud en el aula

POR QUE SE SELECCIONO EL LINUX

EL SO Linux fue seleccionado dada su versatilidad y su facilidad de cambio y que aportaba lo que estábamos necesitando, la libertad de adaptarlo específicamente para nuestro uso, disponibilidad de numerosas herramientas, la facilidad de incorporar placas de red virtuales con comandos simples del SO y el licenciamiento abierto que nos permite adaptarlo sin restricciones [2].

Por ejemplo utilizando comandos del SO una configuración simple de computadoras (fig1)

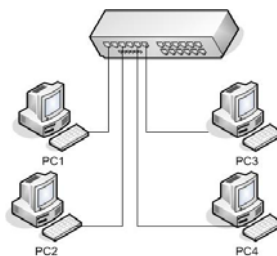


Fig 1

Mediante la configuración de placas Virtuales en dos de las maquinas y la configuración de direcciones IP en cada PC se puede simular un ambiente con tres redes.

La red virtual configurada es:

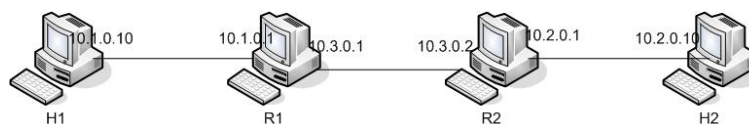


fig. 2

De esta manera se consigue una topología de tres redes con los componentes físicos disponibles.

COMO ES EL CD: CryptoCD

Un LiveCD [5,8,10] es un sistema operativo con un conjunto de aplicaciones almacenado en un medio extraíble, tradicionalmente un CD o DVD, que puede ejecutarse desde éste sin necesidad de ser instalado en el disco duro del ordenador, para lo cual usa la memoria RAM como disco duro virtual.

Una característica fundamental de los mismos es que permite ejecutar un ambiente computacional completo sin modificar el disco rígido de la computadora utilizada.

El CD es desarrollado en forma abierta en el disco de un ambiente LINUX donde se incorporan los programas, scripts y documentos que se necesiten. Por último se compilan usando scripts desarrollados por los diseñadores del proyecto knoppix [13].

Toda la información y las herramientas están compiladas en un CD LINUX autónomo. Cuando la PC se inicia desde el CD el equipo es reconfigurado en un ambiente especialmente pensado para el curso (Sin afectar la información de los Discos Rígidos).

El “CryptoCD” contiene el software instalado y scripts (secuencia de comandos del SO) especialmente diseñados para desarrollar los diferentes prácticos de la materia. En el mismo los estudiantes tienen acceso al material didáctico, notas del curso y a tutoriales de los laboratorios.

Cuando un estudiante o grupo finaliza con su trabajo, el CD permite guardar el estado del trabajo en un diskette para ser enviado para su evaluación a la cátedra o para continuar posteriormente el trabajo. Esto les permite realizar el trabajo parcialmente en su casa y terminarlo en la FIUBA o viceversa.

Para mayor detalle del uso y descripción del CryptoCD referirse al artículo [1] o ver el WEB de la materia [4].

USO EN EL AULA

El sistema permite adaptar con rapidez el aula para su uso por los estudiantes. Simplemente se encienden las computadoras y se inserta el CD en las mismas.

Al iniciarse cargan el SO personalizado e inician su trabajo desde el mismo accediendo a las guías de trabajos incorporadas al mismo.

La guía de trabajos prácticos le presenta el problema al alumno, lo lleva paso a paso en la solución al problema planteado y le presenta variantes no triviales a ser analizadas y resueltas en clase con la supervisión de los docentes.

Durante las prácticas en la interacción con el alumnado se busca afianzar sus conocimientos informativos de seguridad, pero en mayor medida se trata de guiarlos en un proceso que los conduzca a la construcción de su propia solución al tema bajo estudio.

La mejor manera de afianzar una nueva capacidad es poniéndola en práctica primero en situaciones conocidas (descriptas en detalle por los docentes) y luego en variaciones que presenten desafíos.

Ejemplo de Laboratorio Desarrollado: IPSEC

Un ejemplo de trabajo de laboratorio que los alumnos pueden desarrollar con nuestro CD es la configuración de un túnel “IPSEC” [5, 6, 7, 9] entre dos redes. (La guía del TP está disponible en el WEB de la materia [4])

Este ejemplo permite que dos grupos de tres estudiantes trabajen en forma mancomunada en configurar un ambiente muy similar a un caso real de trabajo.

Los estudiantes son divididos en grupos y cada dos grupos se asignan 4 computadoras las cuales son conectadas por los alumnos en el esquema virtual de la figura 2.

Esta división en grupos fomenta la cooperación entre los estudiantes de cada grupo y los otros grupos involucrados para delinear los temas más difíciles y encontrar soluciones interactuando.

La meta del laboratorio es construir el siguiente esquema:

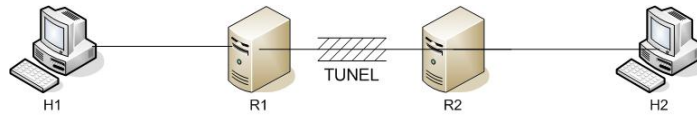


Fig 6

La red de prueba le permite a nuestros estudiantes trabajar con dos PC actuando como enrutadores de tráfico e implementar un túnel IPSEC entre las dos redes y simular el caso real de dos redes LAN conectadas por INTERNET. Para mayor descripción de los pasos utilizados para configurar el túnel IPSEC referirse al artículo [1].

NUEVOS DESARROLLOS SOBRE EL MATERIAL

Actualmente se está trabajando en incorporar la funcionalidad que permitirá una mayor versatilidad al momento de la actualización del ambiente y la corrección del trabajo de los alumnos.

La primera mejora propuesta es incorporar un módulo que permita a los estudiantes publicar su trabajo en nuestro servidor, para luego ser recuperado por el plantel docente en la evaluación posterior y permitir llevar una bitácora de cada grupo.

Otra mejora en estudio es la capacidad de actualización dinámica del ambiente desde el servidor de la materia al momento de iniciar el CD, esto permitiría no tener que distribuir una nueva versión del CD durante el cuatrimestre si se encuentra un error menor en el mismo.

CONCLUSION

El CryptoCD le permite a nuestra materia disponer de un laboratorio virtual extensible de rápida configuración en un aula con computadoras.

Dicho sistema fue usado y verificado con éxito en nuestra materia, facilitando y acelerando el trabajo en el aula. Hemos tenido una muy buena recepción del material por los alumnos quienes han sugerido numerosos cambios y mejoras. Es muy importante recalcar que el material permitió que los estudiantes desarrollen las configuraciones de los laboratorios en forma más rápida y con mejores resultados.

Antes de disponer del CD nos encontrábamos con que debíamos verificar las computadoras del curso antes y después de cada clase para ver que las mismas estén en condiciones operativas para su uso. De esta manera, nos independizamos de la configuración que tengan las PC y trabajamos sobre un ambiente perfectamente conocido y estable.

REFERENCIAS

- [1] Hugo Pagola, Alberto Dams, Juan Caracocha "An Educational Linux Live Cd For A Versatile Information Security Laboratory", International Conference of Engineering Education, Jul 2006
- [2] Franco Diaz, Viviana Harari, Claudia Mariana Banchoff Tzancoff "Ventajas del Software Libre en las Escuelas. Casos de Estudio", JEITICS 2005.
- [3] L. Sanjurjo, M. Vera "Aprendizaje significativo y enseñanza en los niveles medio y superior", Ed. HomoSapiens, 2003

- [4] Web de la materia Criptografía en FIUBA, <http://cactus.fi.uba.ar/crypto/>
- [5] Web de wikipedia <http://es.wikipedia.org/wiki/Knoppix> y <http://es.wikipedia.org/wiki/IPSEC>
- [6] William Stallings , PRENTICE HALL, "Cryptography and Network Security, Third Edition".
- [7] ipsec, <http://www.ietf.org/html.charters/ipsec-charter.html>
- [8] Knoppix Homepage <http://www.knoppix-es.org/>
- [9] OpenSwan Homepage <http://www.openswan.com/>
- [10] morphix live CD <http://www.morphix.org/autobuilds/>