

Framework para el Entrenamiento en Seguridad Informática

Juan Diego Campo Marcelo Rodríguez

Grupo de Seguridad
Instituto de Computación
Facultad de Ingeniería - UdelaR

Jueves 24 de Junio, 2010



Plan

- 1 Introducción
 - Motivación
 - Objetivos
 - Metas Cumplidas
- 2 Diseño de la herramienta
 - Arquitectura
 - Diseño
 - Componentes
 - Prestaciones
- 3 Trabajo en Curso
- 4 Demostración



Plan

- 1 **Introducción**
 - Motivación
 - Objetivos
 - Metas Cumplidas
- 2 **Diseño de la herramienta**
 - Arquitectura
 - Diseño
 - Componentes
 - Prestaciones
- 3 **Trabajo en Curso**
- 4 **Demostración**



Motivación

- El Laboratorio de Seguridad Informática es un ámbito que permite complementar la enseñanza teórica con la experimentación.
- Administrar y mantener la infraestructura de estos laboratorios es costoso.
- Aparece la necesidad de diseñar una plataforma que asista en la definición y ejecución de las prácticas de seguridad.



Objetivos

- Los objetivos de este trabajo son diseñar, desarrollar e implantar una plataforma para el entrenamiento en Seguridad Informática.
- Requerimientos:
 - Reconfigurable
 - Escalable
 - Rentable
 - Robusto
 - Mantenable
 - Realista
 - Aislado
- Surge naturalmente la *virtualización* como mecanismo a utilizar en la plataforma.



Metas Cumplidas

- Definición de la metodología para la elaboración de entrenamientos en SI.
- Investigación de diferentes técnicas y productos de virtualización
 - Paravirtualization, OS level virtualization, Full virtualization
 - Xen, UML, OpenVZ, Solaris Zones, VirtualBox
- Implementación de una primera versión de la herramienta (basada en UML) para asistir en la creación de ambientes de entrenamientos.

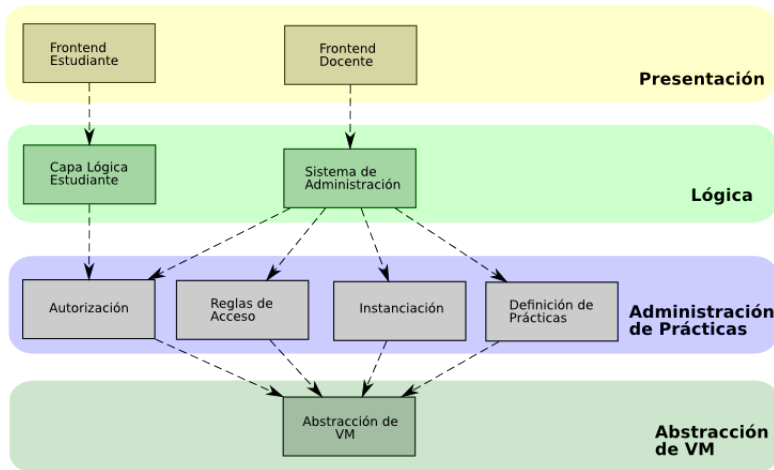


Plan

- 1 Introducción
 - Motivación
 - Objetivos
 - Metas Cumplidas
- 2 Diseño de la herramienta
 - Arquitectura
 - Diseño
 - Componentes
 - Prestaciones
- 3 Trabajo en Curso
- 4 Demostración



Arquitectura de la herramienta



Diseño de la herramienta

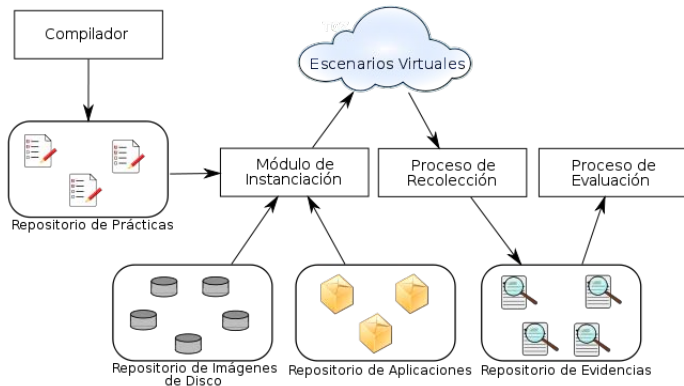
- Hasta ahora, se concentró en el módulo de definición de escenarios
- Para este módulo se creó un lenguaje de especificación de escenarios (LisLAB)

Lenguaje LisLAB

- Constituye el core del framework
- Permite abstraerse de la tecnología de virtualización e instanciación



Componentes de la herramienta



Prestaciones de la herramienta

- Definición de escenarios en forma abstracta
- Reducción del tiempo de instanciación y configuración de varias horas a minutos
- Puesta en producción en cursos de seguridad con buen desempeño
- Reducción en la utilización de recursos de hardware



Plan

- 1 Introducción
 - Motivación
 - Objetivos
 - Metas Cumplidas
- 2 Diseño de la herramienta
 - Arquitectura
 - Diseño
 - Componentes
 - Prestaciones
- 3 Trabajo en Curso
- 4 Demostración



Trabajo en Curso

- Extensión del lenguaje de especificación de escenarios
- Especificación un lenguaje para la administración de entrenamientos.
- Identificación de nuevos actores con roles diferentes
- Definición e implantación de mecanismos de control de acceso
- Implementación de una capa de abstracción de recursos de Hardware

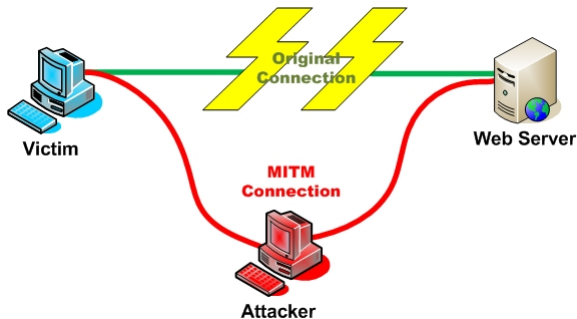


Plan



- 1 Introducción
 - Motivación
 - Objetivos
 - Metas Cumplidas
- 2 Diseño de la herramienta
 - Arquitectura
 - Diseño
 - Componentes
 - Prestaciones
- 3 Trabajo en Curso
- 4 Demostración



Man in the Middle Attack



Referencias

-  G. Betarte, M. Corti, M. Rodríguez
Concepción, Diseño e Implantación de un Laboratorio de Seguridad Informática.
4to Congreso Iberoamericano de Seguridad Informática, Mar del Plata, Noviembre 2007.
-  A. Blanco, J. D. Campo, L. Escanellas, C. Pintado, M. Rodríguez
Generación de Ambientes para Entrenamiento en Seguridad Informática .
5to Congreso Iberoamericano de Seguridad Informática, Montevideo, Noviembre 2009.



¿Preguntas?

