

Técnicas y Herramientas para la Formación y Entrenamiento en Seguridad Informática

Gustavo Betarte Alejandro Blanco Marcelo Rodríguez

Grupo de Seguridad Informática
Instituto de Computación
Facultad de Ingeniería - Universidad de la República
Uruguay

Plan

- 1 Presentación del Grupo de Seguridad Informática
- 2 Laboratorio de Seguridad Informática
- 3 Capacitación CSIRTUY 2008
- 4 Trabajo en Curso
- 5 Resumen

Grupo de Seguridad Informática (GSI - FING)

- Formado a comienzos del año 2006
- Integrado por docentes y profesionales del InCo, IIE y la URI de la Facultad de Ingeniería
- Objetivos
 - Formación de RRHH (grado y posgrado)
 - Investigación
 - Asesoramiento especializado

Formación Curricular

Cursos

- Fundamentos de la Seguridad Informática
 - Curso opcional de grado (Ing. en Computación)
 - Curso de posgrado (Pedeciba Informática)
- Seguridad de Sistemas Informáticos
 - Curso del diploma de especialización del Centro de Posgrados y Actualización Profesional (CPAP)

Formación Curricular

Áreas de Estudio

- Criptografía aplicada
- IAA
- Control de acceso: modelos y políticas
- Sistemas Operativos
- Redes
- Aplicaciones
- Bases de Datos

Proyecto I+D

Hacia un CSIRT nacional

- Metodologías y herramientas para la gestión de incidentes de seguridad
- Diseño e Implantación de un CSIRT nacional
- Actividad específica en el contexto del convenio marco de cooperación entre ANTEL y FING-UdelaR
- Integrantes del proyecto
 - Gerencia de Seguridad de la Información, CSIRT (ANTEL)
 - Grupo de Seguridad Informática (FING)

Laboratorio de Seguridad Informática

Motivación

- Con el LaSI se busca brindar un ámbito que permita complementar la teoría con la experimentación
- Familiarizarse con técnicas y herramientas
- Características
 - Escenario complejo y altamente variable
 - Fácil replicación e independencia del hardware
 - Proteger al resto de las máquinas pertenecientes al laboratorio
 - Las máquinas involucradas (y vulnerables) no tienen que quedar expuestas
 - Ensayos multiplataforma

Laboratorio de Seguridad Informática

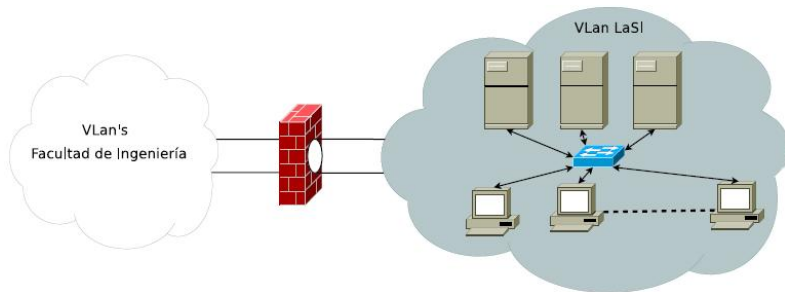
Diseño

- Propiedades
 - Aislado, Reconfigurable, Heterogéneo
 - Robusto, Realista
 - Mantenable, Escalable
- Restricciones
 - Reutilizar la infraestructura disponible en el Instituto de Computación (laboratorio con PCs)
 - Dicho laboratorio es compartido por múltiples usuarios
- Opciones de Arquitectura
 - PCs con múltiple booteo
 - Virtualización

Laboratorio de Seguridad Informática

Arquitectura

- Infraestructura basada en tecnología de máquinas virtuales
 - Servidores que soportan ambientes virtualizados
 - Se utilizan los PCs de la infraestructura existente como terminales de trabajo
- Conectividad, Vlans y firewalls



Laboratorio de Seguridad Informática

Características

- Aislado de la red de producción
- La virtualización permite definir ambientes de trabajo heterogéneos y realistas
- La clonación de máquinas virtuales facilita el armado de ambientes de trabajo
- Puede reponerse rápidamente a daños producidos por el uso

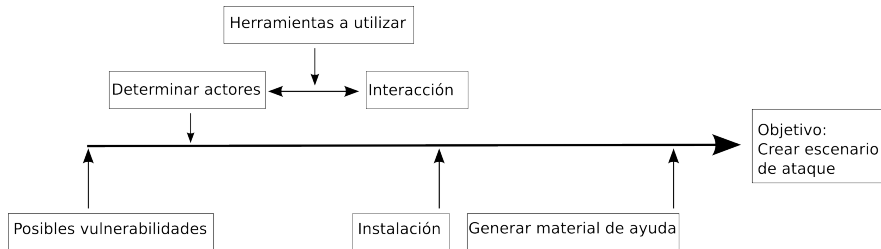
Metodología de Trabajo

Análisis de Escenarios

- Objetivo: crear escenarios para el laboratorio
- Identificar la problemática
 - Escenarios de ataque
 - Soluciones
- Generar material de ayuda (guías)
- Crear indicadores para evaluar resultados

Metodología de Trabajo

Escenario de Ataque



Metodología de Trabajo

Actores Involucrados

Víctimas



Sistemas operativos

Servicios mal configurados

Aplicaciones vulnerables

Canal de comunicación inseguro

Atacantes



Herramientas para realizar ataques

Exploits y diccionarios

Ataques a las comunicaciones

Metodología de Trabajo

Actores Involucrados

Víctimas



Sistemas operativos

Servicios mal configurados

Aplicaciones vulnerables

Canal de comunicación inseguro

Atacantes



Herramientas para realizar ataques

Exploits y diccionarios

Ataques a las comunicaciones

Metodología de Trabajo

Herramienta de especificación de escenarios

Antecedentes

- En un escenario se identifican componentes a los cuales se le pueden asociar atributos
- En el proceso de concepción de un escenario existen tareas repetitivas
- Se cuenta con repositorios

Primera etapa

- Se está trabajando en la definición de un lenguaje para especificar escenarios

Metodología de Trabajo

Herramienta de especificación de escenarios

Antecedentes

- En un escenario se identifican componentes a los cuales se le pueden asociar atributos
- En el proceso de concepción de un escenario existen tareas repetitivas
- Se cuenta con repositorios

Primera etapa

- Se está trabajando en la definición de un lenguaje para especificar escenarios

Capacitación CSIRTUY 2008

Objetivo de los módulos GSI - FING

- Desarrollado en colaboración con el CSIRT de ANTEL
- Marco teórico
 - ¿Qué es el Ethical Hacking?
 - Bases sobre los pasos y técnicas para llevar adelante un Ethical Hacking
 - Honey*
- Hands On
 - Uso de la herramienta Nmap y Nmap Scripting Engine (**NmapSE**)
 - Instalación y configuración de **honeyd**

Capacitación CSIRTUY 2008

Público Objetivo

- Profesionales e idóneos en seguridad en redes, informática e información
- Personal jerárquico con capacidad de decisión en dichas áreas, de Uruguay y del exterior
- Ámbito público y privado

Honey*

Definiciones

- Es un recurso utilizado como “cebo” o “carnada” con el objetivo de atraer a “atacantes”
- El valor de los Honeypot reside en cuán “atractivo” resulte la carnada para atraer “atacantes”
- Abstractamente se los puede ver como **SENSORES** recolectando información maliciosa
- No son sistemas en producción o reales
- Toda actividad dirigida hacia ellos es considerada sospechosa o maliciosa
- **No hay falsas alarmas**

Honey*

Motivación

- Herramienta de apoyo para la formación en el área de la Seguridad Informática
- Excelente herramienta para **emular objetivos de ataque**
 - Servicios, Computadoras, Redes de Datos
- **Sensibilización**
- **Aprender** de/sobre los atacantes
 - Conocer tendencias de los ataques
 - Mejorar el conocimiento de los atacantes y las herramientas usadas
 - Conocer las vulnerabilidades usadas para acceder o comprometer los sistemas
 - Reaccionar frente a ataques que se realizan sobre nuestros sistemas (alarmas)

Trabajo en Curso

Laboratorio

- Automatizar la creación de ambientes de experimentación
- Investigar diferentes técnicas de virtualización y evaluar la incorporación al LaSI (Paravirtualization, Virtualización on the OS level, Full virtualization)
- Investigar los diferentes productos de virtualización (Xen, UML, OpenVZ, Solaris Zones)
- Movilidad de la plataforma

Trabajo en Curso

Honey*

- Integración con **sistema de alarmas** o IPS
- **Formato de representación** y **modelo de datos** para la información recolectada
 - IDMef, HiDef [Hoep08]
- Uso de mecanismos de virtualización para la implementación de Honeypots
- Uso de Honeypot/Honeynet en cursos de formación en Seguridad Informática
 - Análisis Forense
 - Ethical Hacking
 - Instalación y Configuración de Honeypots de producción

Resumen

- Formación curricular de grado y posgrado
- Ambiente de experimentación y entrenamiento
- Desarrollo de líneas de investigación e innovación

Referencias



G. Betarte, M. Corti and M. Rodríguez

Concepción, Diseño e Implantación de un Laboratorio de Seguridad Informática.

4to Congreso Iberoamericano de Seguridad Informática, Mar del Plata, Noviembre 2007.



C. Hoepers, N.L. Vijaykumar, A. Montes

HIDEF: a Data Exchange Format for Information Collected in Honeypots and Honeynets.

Febrero 2008.