Importante: En la segunda semana de diciembre de 2009 deben sí o sí presentar lo que tengan hecho hasta el momento. De no ser aprobado el TP en dicha instancia, deben recuperarlo antes del 28 de diciembre de 2009.

Tp de Investigación

Seguridad en virtualización

A medida que las nuevas tecnologías de virtualización se emplean cada vez más en las organizaciones, sobre todo para la consolidación de equipos y servicios, la ilusión de que cada máquina virtual está aislada de las demás pero a la vez contenida dentro del equipo físico provee una sensación de seguridad. Sin embargo, el hecho de que estas tecnologías de virtualización contengan diversas vulnerabilidades presentan nuevos desafíos sobre la seguridad de la información manejada por las máquinas virtuales que se instalan.

En este trabajo deberán describir qué es la virtualización, los distintos enfoques disponibles (virtualización, para-virtualización, emulación), el soporte por hardware para virtualización disponible en ciertos procesadores, investigar los potenciales problemas de seguridad existentes y detallar distintas vulnerabilidades encontradas hasta el momento. Incluir investigación relacionada con el uso de canales encubiertos, y la detección por parte de una aplicación de la forma de saber si se está corriendo en un entorno virtual.

Entregables TP de Investigación.
Una presentación con transparencias a dar para todos los alumnos y una versión preliminar del Informe, la 2da semana de diciembre.
Un informe al final del cuatrimestre de por lo menos 30 páginas, en letra arial 10, espaciado simple. El informe debe contener referencias bibliográficas relevantes.

TP Implementación

Desarrollo de Aplicación web con vulnerabilidades.

Se debe desarrollar una aplicación web que contenga diversas vulnerabilidades, con distinto grado de dificultad, que sirva para un entorno de capacitación para el dictado de la materia. Basarse en las vulnerabilidades descriptas en el OWASP TOP 10, e implementar por lo menos:

2 vulnerabilidades distintas relacionadas con SQL injection
1 XSS
1 Manipulación de cookies
1 Information leakage y mal manejo de errores
1 failure to restrict url access

La aplicación debe simular una aplicación real, como puede ser un sitio de impresión de fotografías, y se busca que los problemas sean originales, y que no dependan solo de un problema de implementación sino también de problemas de diseño y de operación.
Pueden tomar como referencia la herramienta webgoat y las herramientas hacme de foundstone. Es deseable que el software tenga mínimos requerimientos de disco y memoria, para que pueda correr en una maquina virtual en una PC con 2gb de RAM.

Implementación: Sniffer http Proxy

Parte 1:
Implementar una herramienta que captura mediante sniffing de la red pedidos http y https que son dirigidos a un Proxy (es el mismo proxy para todos los pedidos), y almacenarlos en una base de datos SQL. Se debe almacenar ip origen, fecha y hora, método http, URL. De ser posible, almacenar los Headers de la respuesta, incluyendo código de respuesta¸ tamaño de la misma y content-type.
Es muy importante poder capturar y registrar las solicitudes realizadas con el método connect.

Parte 2:
Se deberán poder generar reportes de anomalías (ejemplo: pedidos fuera del horario laboral). La lista de reportes será definida junto el docente antes del 15/11, en base a los avances de la parte 1.

IPS WEB

Desarrollar un IPS para el protocolo HTTP (tipo mod_security) que permita la definición de filtros configurables sobre un Request HTTP de manera tal de que sea posible tomar decisiones sobre si dicha solicitud deba o no ser redirigido al servidor web.
Se espera que reciba los pedidos en un puerto dado, y en caso de que el pedido sea aceptado, genere una nueva conexión retransmitiendo el pedido al puerto en el que escucha el servidor web y, una vez obtenida la respuesta, devolviéndosela al cliente original.
Se debe poder filtrar por distintos tipos de encabezados, haciendo hincapié en el método, el url, y los parámetros.
Además, debe generar un log histórico de todas las conexiones analizadas, mostrando información detallada sobre el Request original, el filtro aplicado y la acción llevada a cabo.

Entregables Tp de Implementación
Una presentación con transparencias y demo en vivo a dar durante la segunda semana de diciembre.
Un informe al final de cuatrimestre de por lo menos 10 carillas, en letra arial 10, espaciado simple (no incluye código fuente), indicando funcionalidad implementada, herramientas utilizadas, forma de instalación, configuración y uso, limitaciones de la aplicación.. El código fuente de la aplicación desarrollada.