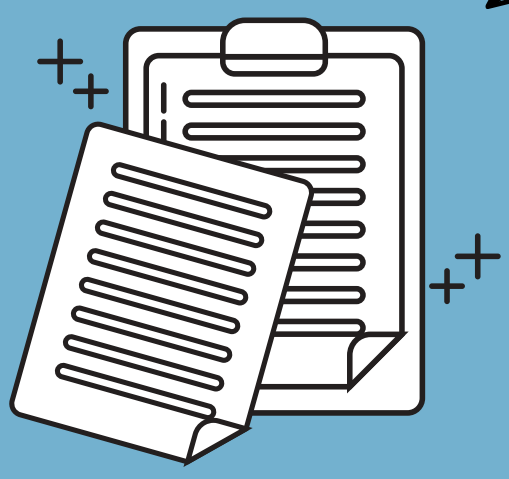
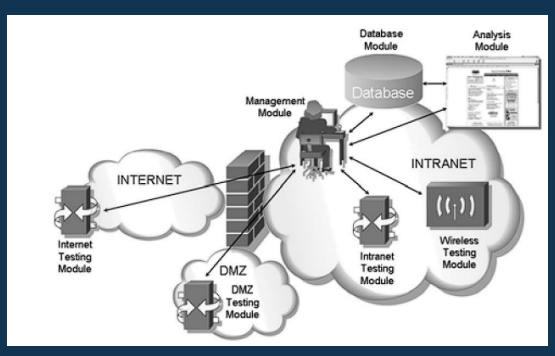
A DISTRIBUTED VULNERABILITY DETECTION SYSTEM FOR AN INTRANET

Brandon Meza - 3CV11

Existen muchas herramientas para detectar vulnerabilidades, pero no siempre dan un panorama general de toda la red. Se propone el sistema de detección de vulnerabilidades que facilita la ejecución de tests basados en el OSSTMM automatizando procedimientos



CONSENSUS SYSTEM



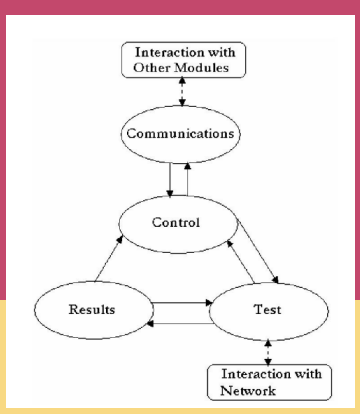
CONSENSUS es un sistema de testeo de vulnerabilidades que consta de módulos interactivos. Este sistema automatiza mecanismos referentes a testeo de vulnerabilidades para minimizar el tiempo que se necesita para llevar a cabo un testeo de seguridad OSSTMM. Este sistema es una interfaz web donde los usuarios interactúan de manera sencilla.

El módulo intranet

Es el encargado de realizar testeos desde la red interna, esto significa que este módulo debe estar integrado en la infraestructura de la red corporativa. Esto minimiza el impacto que implica tener un dispositivo de testeo en la intranet.

Especificaciones del módulo de intranet

El sistema base corre Debian 2.6.9 y es el núcleo del resto de los módulos. Este sistema operativo fue customizado para proveer un sistema estable, configurable y eficiente que ocupa poco espacio. Todas las herramientas de testeo embebidas deberán ser open-source y estas herramientas no necesitan una interfaz gráfica.



Diseño del módulo de intranet

El sistema tiene 4 bloques. El bloque de comunicaciones comunca solo el módulo de administración. El sistema usa su propio protocolo de comunicación. El bloque de control maneja los parametros de testeo y supervisa el performance del test. El bloque de testeo corre herramientas de seguridad.

Implementación del testeo de intranet

La meta de la recopilaciópn de vulnerabilidades es verificar y entender debilidades y vulnerabilidades de un host o una red. La fase de testeo de aplicaciones verifica la confianza de las apps. Las herramientas usadas son capaces de descubrir más de 3000 vulnerabilidades. La fase de ruteo esta diseñada para asegurar que aquel que esta permitido será aceptado en la red. Cuando finaliza los resultados se guardan en un archivo XML que se inserta en la base de datos.