Tecnologías de red

Práctica 4 (1ª parte)

Despliegue de mecanismos de seguridad: Snort

Duración prevista: 1 sesiones

Objetivo	Instalación, configuración y evaluación de un sistema de detección de intrusos. Se utilizará Snort (http://www.snort.org).
Material	▪ Snort ▪ Herramientas de ataque y escaneo (nmap y hping3).
Fundamentos	Los fundamentos serán presentados en clase por el profesor al inicio de la sesión.
Realización práctica	➢ **Preliminares** Para la realización de la presente práctica es necesario arrancar el equipo en Ubuntu. Para ello, en el menú de arranque, seleccione "Redes->Ubuntu 12.04". De esta forma se arranca el equipo en "modo aislado", es decir, no se tiene acceso a Internet. Una vez se haya identificado como "administrador" (clave: finisterre), pase a modo superusuario ejecutando el comando: #sudo su La contraseña es "finisterre". Para configurar el servidor del aula (eihal) como repositorio para poder instalar paquetes de Ubuntu, accedemos a http://192.168.33.21 y descargamos un archivo de comandos (extensión .sh) de los denominados repository_ubuntu_precise.sh. Lo ejecutamos como administrador: #sudo sh <archivo.sh> A partir de este momento puede instalar paquetes a partir del servidor mediante el comando #sudo apt-get install <paquete> *NOTA: Es posible que algunos de los programas necesarios se instalen automáticamente al actualizar el repositorio.* ➢ **Ejecución** 1. Instale el paquete Snort. Especifique la interfaz eth2 (red de gestión) como la interfaz a monitorizar. 2. Configure adecuadamente Snort. Para ello, edite el archivo

	/etc/snort/snort.conf 3. Ejecute Snort mediante el comando: #sudo snort –c /etc/snort/snort.conf 4. El resultado del análisis (alertas) se almacena en /var/log/snort 5. Analice las alertas que se generan en los siguientes casos: a. En un ataque de denegación de servicio (DoS) a partir de ping. Para ello, instale el paquete hping3 b. En un escaneo de puertos. Para ello instale el paquete nmap. Debe realizar los ataques a algunos de sus compañeros para que sean capturados por Snort. 6. Cree una regla de prueba que almacene una alerta por cada paquete que se reciba en el puerto 80. 7. (Opcional) Instale y configure Snort Report para visualizar las alertas a través de web. Puede descargar las instrucciones desde www.snort.org, en la sección de documentación (http://www.snort.org/assets/158/snortinstallguide293.pdf).
Informe	Muestre los resultados del análisis al profesor.