Práctica II.: *Sniffing* et al. (parte II)

Prof. A. Santos del Riego
Protección y Seguridad de la Información (PSI)
Facultad de Informática. Universidade da Coruña

El objetivo de esta práctica, como complemento de los desarrollos con *sniffers*, se centra en diversos temas relacionados con el *scanning* de sistemas, la necesidad de integridad y disponibilidad en nuestros equipos, etc. Hemos tratado en las clases teóricas los conceptos fundamentales que deberán ser aplicados mediante pruebas. En la clase de prácticas se propondrán posibles herramientas a utilizar.

a) Pruebe distintas técnicas de *host discovey*, *port scanning* y *OS fingerprinting* sobre las máquinas del laboratorio de prácticas.
b) Seleccione y pruebe alguna utilidad para verificar la integridad de sus binarios.
c) Utilizando la herramienta `tripwire` defina un esquema seguro de chequeo de la integridad sobre su sistema.
d) Seleccione y pruebe alguna de las utilidades disponibles para chequear el sistema contra *rootkits*
e) Obtenga información "en tiempo real" sobre las conexiones de su máquina, así como del ancho de banda consumido en cada una de ellas. Establezca un sistema de *accounting* del subsistema de red de su máquina de laboratorio.
f) Seleccione alguna máquina de laboratorio de cualquier compañero de clase como objetivo y, pensando en una DoS de tipo *direct attack*, proceda a "darle caña". Repita la jugada pero pesando en una DoS de tipo *reflective flooding attack*. Trate de visualizar en todo momento las conexiones y, o, paquetería generada. ¿Cómo podría montar una arquitectura DDoS utilizando varias de las máquinas de laboratorio de sus compañeros?
g) ¿Qué haría si sospecha que su sistema ha sido comprometido?

Método de evaluación.: Como resultado de esta práctica, el profesor evaluará las habilidades adquiridas por el alumno mediante una sesión de trabajo en máquina.