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

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

El objetivo de esta práctica es comprender y probar el funcionamiento de los *sniffers*. Hemos tratado en las clases teóricas los conceptos fundamentales de estas herramientas y sus principales técnicas, que deberán ser aplicados mediante pruebas.

a) Instalar el *sniffer* o *sniffers* seleccionados, pensando tanto en redes de medio compartido como conmutadas.
b) Identificar las posibilidades de la-s herramienta-s seleccionada-s y probar las opciones más relevantes (captura de tráfico, edición, filtrado, etc.)
c) Capturar el *login* y el *password* de una sesión que utilice texto en claro.
d) ¿Qué permite un *sniffer* sobre la IP del *router* o *proxy* de tu segmento?
e) Capturar un paquete TCP e indicar sus principales campos de cabecera.
f) Indique 3 servicios que transmiten información sensible en claro.
g) Indique 3 servicios que transmiten información sensible cifrada.
h) Obtener la relación de las direcciones MAC de los equipos de su segmento.
i) ¿Qué posibles utilidades tiene un *sniffer*?
j) Mediante *arpspoofing* entre una máquina objetivo (víctima) y el *proxy* del laboratorio obtener todas las URL HTTP visitadas por la víctima y visualizarlas directamente en vuestro navegador.
k) Utilizando un filtro `ettercap` modificar las imágenes de las páginas http visitadas por una determinada máquina del laboratorio.
l) Y si quiero capturar un *password* de una sesión https, ¿qué opciones tengo?
m) Instalar y probar alguna herramienta y técnica de detección del *sniffing*
n) Abra una conexión desde una máquina remota contra la suya y "mate" dicha conexión en su equipo.

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