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

Práctica propuesta.: enero 2005. Última revisión.: marzo 2012
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*.

a) Instale el ettercap y pruebe las opciones básicas en línea de comando (captura de tráfico, filtrado, etc.)
b) Capture paquetería de una sesión no segura.
c) Capture un paquete TCP e identifique los principales campos de cabecera.
d) Capture un paquete IPv6 e identifique los principales campos de cabecera.
e) Indique 3 servicios que transmiten información en claro. Indique 3 servicios que transmiten información cifrada.
f) Obtenga la relación de las direcciones MAC de los equipos de su segmento.
g) Obtenga la relación de las direcciones IPv6 de su red.
h) Mediante *arpspoofing* entre una máquina objetivo (víctima) y el *router* del laboratorio obtenga todas las URL HTTP visitadas por la víctima. Trate de visualizarlas directamente en su navegador.
i) Haga pruebas para tratar de hacer un MITM en IPv6.
j) Utilizando un filtro `ettercap` modifique las imágenes de las páginas http visitadas por una determinada máquina del laboratorio.
k) Utilizando el ettercap-gtk trate de capturar el password de una sesión https.
l) Pruebe alguna herramienta y técnica de detección del *sniffing.*
m) 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.