PRÁCTICA II: Sniffing

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, que deberán ser aplicados mediante pruebas. Para ello se deberán seleccionar los *sniffers* a utilizar y el entorno de trabajo.

a) Instalar el *sniffer* o *sniffers* seleccionados, pensando tanto en redes de medio compartido como switched.
b) Identificar las posibilidades de la-s herramienta-s seleccionadas y probar las opciones más relevantes (captura de tráfico, edición, filtrado, etc.)
c) Pruebe alguno de los pluggin del ettercap
d) Capturar e *login* y el *password* de una sesión que utilice texto en claro.
e) ¿Qué permite un *sniffer* sobre la IP del *router* de tu segmento?
f) Capturar un paquete IP e indicar la funcionalidad de sus principales campos. Capturar un paquete ARP.
g) Indique 3 servicios que transmiten información sensible en claro.
h) Indique 3 servicios que transmiten información sensible cifrada.
i) Establecer y aplicar un esquema de *sniffing* mediante filtrado.
j) ¿Cómo podría obtener una relación de las direcciones MAC de los equipos de su segmento?.
k) ¿Cuál es la dirección IP de su equipo?. ¿Cuál es la dirección MAC de su equipo?
l) Instalar y probar alguna herramienta y técnica de detección de *sniffing*
m) Instale y configure el arpwatch. Registre pares IP-MAC de su segmento. Detecte algún cambio IP-MAC
n) ¿Cómo podría hacer *sniffing* sobre una máquina perteneciente a un segmento de red distintos al suyo?
o) ¿Qué posibles utilidades tiene un *sniffer*?
p) Instale y pruebe la utlidad md5sum para verificar la integridad de sus binarios
q) Utilizando el *Tripwire* defina un esquema de chequeo de la integridad sobre su sistema
r) ¿Qué hace el etherape?. Pruebe esta utilidad.
s) Instale un servidor web en la máquina virtual del otro grupo. Detecte e identifique de forma remota y activa el servicio instalado e intente identificar su versión. Identifique también todos los puertos abiertos y, si posible, la versión del sistema operativo.
t) Instale el paquete pads y detecte servicios de las conexiones de red de forma pasiva. ¿Qué implicaciones tiene una detección pasiva frente a una activa?
u) Abra una conexión de red contra su máquina virtual y "mátela"
v) Instale y pruebe algún detector remoto de interfaces en modo promis
w) ¿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.