Práctica II.: Ejemplos de categorías de ataque et al. (3 sesiones – 6h)

Prof. A. Santos del Riego
Legislación y Seguridad Informática (LSI)
Facultad de Informática. Universidade da Coruña
Fecha propuesta.: enero 2003
Última revisión.: julio 2012

El objetivo de esta práctica es comprender y probar el funcionamiento de los *sniffers*, los ataques [D]DoS, así como diversos temas relacionados con lo que hemos llamado la trilogía ("host discovery", "port scanning" y "fingerprinting"). En las sesiones prácticas se propondrán posibles herramientas a utilizar.

a) Instale el ettercap y pruebe sus opciones básicas en línea de comando.
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 y otros 3 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 segmento.
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 un MITM en IPv6 y visualice la paquetería.
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) Pruebe distintas técnicas de *host discovey*, *port scanning* y *OS fingerprinting* sobre las máquinas del laboratorio de prácticas.
n) Realice alguna de las pruebas de *port scanning* del apartado anterior sobre IPv6. ¿Coinciden los servicios prestados por un sistema con los de IPv4?.
o) 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.
p) Seleccione alguna máquina de laboratorio de cualquier compañero de clase como objetivo y, pensando en una DoS de tipo *direct attack*, haga las pruebas que estime oportunas. 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.
q) Considerando que todos los sistemas del laboratorio tiene autoconfiguración de la pila IPv6, ¿cómo podría tratar de tirar abajo todos los sistemas? Haga también pruebas de *flooding* en IPv6. ¿Cómo podríamos protegernos?.
r) Ataque un servidor apache para provocarle un DoS. ¿Cómo podría proteger dicho servicio ante este tipo de ataque? ¿Y si se produce desde fuera de su segmento de red? ¿Cómo podría tratar de saltarse dicha protección?

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