Práctica I.: Redes básica

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 básico del subsistema de red de un computador. Hemos tratado en las clases teóricas los conceptos fundamentales del subsistema, así como los principales comandos y ficheros de configuración de un entorno Linux.

a) Identificar y cambiar los principales parámetros del interface de red mediante el comando `ifconfig` con los parámetros proporcionados para cada máquina de laboratorio.
b) Identifique los servicios del sistema y las conexiones establecidas mediante el comando `netstat`. Abra una nueva conexión e identifíquela.
c) ¿Qué rutas (*routing*) están definidas en su sistema?. Modifique con el comando `route` la ruta *default*. Incluya una nueva ruta estática a una determinada red.
d) Analice e identifique los servicios de red en arranque del sistema. Identifique alguno de los servicios potencialmente inseguros y haga que deje de dar servicio. ¿Funcionaría su sistema si elimina el proceso `inetd`?. ¿Qué supone esta acción?. ¿Coincide la relación de servicios `inetd` con la totalidad de los proporcionados por su sistema?. ¿Qué es el `xinetd`?
e) ¿Qué nivel de arranque por defecto tiene su sistema?
f) Identifique la secuencia y acciones de arranque de su máquina Linux de laboratorio.
g) ¿Qué hacen las herramientas `top`, `iptraf` y `tcptrack`?
h) Analice los ficheros básicos de configuración (`interfaces`, `hosts`, `resolv.conf`, `nsswitch.conf`, etc.)
i) Analice y pruebe la configuración del *syslogger* del sistema. ¿Cómo puede enviar la salida de información de *log* de un conjunto de sistemas a uno remoto?. ¿Qué es el `syslog-ng`?
j) Envíe información de *log* utilizando una "tubería" sobre una conexión SSH a un sistema remoto.
k) Un primer nivel de filtrado de servicios los constituyen los *tcp-wrapper*. Configure el *tcp-wrapper* de su sistema (basado en los ficheros `hosts.allow` y `hosts.deny`) para permitir conexiones SSH a un determinado conjunto de IPs y denegar al resto. ¿Qué política general de filtrado ha aplicado?. ¿Es lo mismo el *tcp-wrapper* que un *firewall*?

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