

Práctica I: Configuración básica

Prof. A. Santos del Riego
Protección y Seguridad de la Información (PSI)
Facultad de Informática. Universidad de A Coruña
Fecha propuesta.: junio-2002
Última revisión.: febrero-2011

El objetivo de esta práctica es comprender y probar el funcionamiento básico y configuración de su máquina-computador de laboratorio. Hemos tratado en las clases teóricas los conceptos fundamentales, así como los principales comandos y ficheros de configuración de un entorno Linux.

- a) Configure su máquina virtual de laboratorio con los datos proporcionados por el profesor. Analice los ficheros básicos de configuración (`interfaces`, `hosts`, `resolv.conf`, `nsswitch.conf`, `sources.list`, etc.). ¿Qué nivel de arranque por defecto tiene su sistema?. Identifique la secuencia y acciones de arranque de su máquina Linux.
- b) Identifique y cambie los principales parámetros del interface de red mediante el comando `ifconfig`. Configure un segundo interface lógico.
- 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) Identifique los servicios de red proporcionados por el sistema. ¿Son necesarios dichos servicios?. En caso negativo, ...
- e) Instale un servidor `ssh`. Abra una conexión contra dicho servidor e identifíquela mediante el comando `netstat`.
- f) Nuestro sistema es el encargado de gestionar la CPU, memoria, red, etc., como soporte a los datos y procesos. Monitorice en “tiempo real” la información relevante de los procesos del sistema y los recursos consumidos. Monitorice en “tiempo real” las conexiones de su sistema.
- g) Un primer nivel de filtrado de servicios los constituyen los *tcp-wrappers*. 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*?
- h) Existen múltiples paquetes para la gestión de logs (`syslog`, `syslog-ng`, `rsyslog`). Utilizando el `rsyslog` configure y pruebe su sistema de log local.
- i) Configure IPv6 6to4 y pruebe `ping6` y `ssh6`. ¿Qué hace su *tcp-wrapper* en las conexiones `ssh` en IPv6?. ¿Qué hace su *firewall* ante tales conexiones?. Modifique su *tcp-wapper* siguiendo el criterio del apartado g). ¿Necesita IPv6?

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

Práctica I.: Configuración básica (opcional)

Prof. A. Santos del Riego

Protección y Seguridad de la Información (PSI)

Facultad de Informática. Universidad de A Coruña

Fecha propuesta.: junio-2002

Última revisión.: febrero-2011

- j) En colaboración con otro grupo de prácticas, configure un servidor y un cliente NTP.
- k) Cruzando los dos equipos anteriores, configure con rsyslog un servidor y un cliente de logs.
- l) ¿Qué problemas de seguridad identifica en los dos apartados anteriores?. ¿Cómo podría solucionar los problemas identificados?