Práctica I.: Configuración básica (3 sesiones – 6h)

Prof. A. Santos del Riego
Legislación y Seguridad Informática (LSI)
Facultad de Informática (UDC)
Fecha propuesta.: junio-2002
Última revisión.: agosto 2023

El objetivo de esta práctica es comprender y probar el funcionamiento básico y configuración de su máquina de laboratorio. El alumno se "familiarizará" con los comandos y ficheros de configuración de un entorno Linux.

Se cerrará esta práctica con la configuración básica de servicios de red, como trabajo a desarrollar en grupos de dos alumnos.

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.)
b) ¿Qué distro y versión tiene la máquina inicialmente entregada?. Actualice su máquina a la última versión estable disponible.
c) Identifique la secuencia completa de arranque de una máquina basada en la distribución de referencia (desde la pulsación del botón de arranque hasta la pantalla de login). ¿Qué target por defecto tiene su máquina?. ¿Cómo podría cambiar el target de arranque?. ¿Qué targets tiene su sistema y en qué estado se encuentran?. ¿Y los services?. Obtenga la relación de servicios de su sistema y su estado. ¿Qué otro tipo de unidades existen?.
d) Determine los tiempos aproximados de botado de su kernel y del userspace. Obtenga la relación de los tiempos de ejecución de los services de su sistema.
e) Investigue si alguno de los servicios del sistema falla. Pruebe algunas de las opciones del sistema de registro journald. Obtenga toda la información journald referente al proceso de botado de la máquina. ¿Qué hace el systemd-timesyncd?.
f) Identifique y cambie los principales parámetros de su segundo interface de red (ens34). Configure un segundo interface lógico. Al terminar, déjelo como estaba.
g) ¿Qué rutas (*routing)* están definidas en su sistema?. Incluya una nueva ruta estática a una determinada red.
h) En el apartado d) se ha familiarizado con los services que corren en su sistema. ¿Son necesarios todos ellos?. Si identifica servicios no necesarios, proceda adecuadamente. Una limpieza no le vendrá mal a su equipo, tanto desde el punto de vista de la seguridad, como del rendimiento.
i) Diseñe y configure un pequeño "script" y defina la correspondiente unidad de tipo service para que se ejecute en el proceso de botado de su máquina.
j) Identifique las conexiones de red abiertas a y desde su equipo.
k) 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.
l) 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*?. Procure en este proceso no perder conectividad con su máquina. No se olvide que trabaja contra ella en remoto por ssh.
m) Existen múltiples paquetes para la gestión de logs (syslog, syslog-ng, rsyslog). Utilizando el rsyslog pruebe su sistema de log local. Pruebe también el journald.
n) Configure IPv6 6to4 y pruebe ping6 y ssh sobre dicho protocolo. ¿Qué hace su tcp-wrapper en las conexiones ssh en IPv6? Modifique su *tcp-wapper* siguiendo el criterio del apartado h). ¿Necesita IPv6?. ¿Cómo se deshabilita IPv6 en su equipo?

[SIGUE EN LA PÁGINA 2]

a) En colaboración con otro alumno de prácticas, configure un servidor y un cliente NTPSec básico.
b) Cruzando los dos equipos anteriores, configure con rsyslog un servidor y un cliente de logs.
c) Haga todo tipo de propuestas sobre los siguientes aspectos.: ¿Qué problemas de seguridad identifica en los dos apartados anteriores?. ¿Cómo podría solucionar los problemas identificados?
d) En la plataforma de virtualización corren, entre otros equipos, más de 200 máquinas virtuales para LSI. Como los recursos son limitados, y el disco duro también, identifique todas aquellas acciones que pueda hacer para reducir el espacio de disco ocupado.
e) Instale el SIEM splunk en su máquina. Sobre dicha plataforma haga los siguientes puntos.:
    a. Genere una query que visualice los logs internos del splunk
    b. Cargué el fichero `/var/log/apache2/access.log` y el journald del sistema y visualícelos.
    c. Obtenga las IPs de los equipos que se han conectado a su servidor web (pruebe a generar algún tipo de gráfico de visualización), así como las IPs que se han conectado un determinado día de un determinado mes.
    d. Trate de obtener el país y región origen de las IPs que se han conectado a su servidor web y si posible sus coordenadas geográficas.
    e. Obtenga los hosts origen, sources y sourcestypes.
    f. ¿cómo podría hacer que splunk haga de servidor de log de su cliente?

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