GESTIÓN AVANZADA DE SISTEMAS OPERATIVOS
(5º Ingeniero en Informática) /
ADMINISTRACIÓN AVANZADA DE SISTEMAS OPERATIVOS
(4º Grado en Ingeniería Informática)

PRÁCTICAS DE LA ASIGNATURA
CONVOCATORIA DE JUNIO/2012

Mayo de 2012
Dpto. Ingeniería y Tecnología de Computadores
Universidad de Murcia

PRÁCTICAS DE GESTIÓN/ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

Convocatoria de Junio

Fecha de entrega de las prácticas: Martes 5 de Junio de 2012

REQUISITOS DE ENTREGA

- Memoria impresa, que incluya, para cada uno de los dos supuestos prácticos resueltos:
  - Portada con el título del supuesto y los componentes del grupo.
  - Índice.
  - Resumen inicial del trabajo realizado.
  - Introducción de aquellos conceptos que sean necesarios para entender la memoria.
  - Descripción detallada del trabajo realizado, incluyendo, en su caso, los scripts o programas realizados, así como los ficheros de configuración que haya sido preciso crear o actualizar.
  - Ejemplos de prueba.
  - Posibles propuestas de mejora.
  - Grado de cumplimiento de los controles relativos al estándar internacional sobre sistemas de gestión de seguridad de la información (ISO 27002).
  - Bibliografía, si la hubiere.
- Se adjuntará a la memoria un disquete de $3^{1/2}$ con el historial de órdenes ejecutadas para resolver cada supuesto, junto con sus respectivas salidas por pantalla. El disquete debe ir rotulado con el nombre de los componentes del grupo.

ASIGNACIÓN DE SUPUESTOS

- Los ocho supuestos ofrecidos quedan agrupados en cuatro conjuntos de dos supuestos, asignándose a cada grupo, por sorteo, alguno de estos conjuntos.
- Los cuatro conjuntos de supuestos son los siguientes:
  - Conjunto 1: supuestos 6 y 7.
  - Conjunto 2: supuestos 3 y 4.
  - Conjunto 3: supuestos 2 y 5.
  - Conjunto 4: supuestos 1 y 8.

VALORACIÓN DE LAS PRÁCTICAS

- La nota de las prácticas se valorará de 0 a 10, y supone el **60 %** de la calificación global de la asignatura.
- Cada uno de los dos supuestos es el **50 %** de la nota de prácticas.

EVALUACIÓN

- La memoria técnica se evaluará en función del grado de cumplimiento de los objetivos propuestos y de las normas de estructuración de contenidos antes expuestas. La nota de la memoria constituye la mitad de la nota de prácticas, y es una calificación compartida por ambos miembros del grupo.
- Además de la memoria, cada miembro del grupo habrá de mantener una entrevista individual con el profesor. Esta entrevista tendrá lugar en el laboratorio 2.7, y durante su transcurso el alumno deberá resolver en los equipos del citado laboratorio uno de los dos supuestos asignados, de acuerdo con un sorteo que se llevará a cabo el mismo día de la entrevista [1]. La nota de esta entrevista es el 50 % de la calificación de las prácticas, y puede ser diferente para cada miembro del grupo.
- La resolución de los supuestos prácticos debe ejecutarse, obligatoriamente, en el laboratorio 2.7, con los sistemas operativos Linux Fedora 15 y/o Windows Server 2008 y/o Windows XP, según proceda.

[1] En la entrevista individual estará permitido consultar la memoria técnica elaborada por el grupo.

SUPUESTO Nº 1: Administración básica de sistemas operativos

Contexto

Dos equipos, S y C, que actúan, respectivamente, como servidor y estación de trabajo. S es un servidor Linux Fedora 15, desde el que se ofrece un conjunto de servicios, y C es el puesto de trabajo habitual del administrador de S, quien cuenta con un Windows XP para desarrollar sus tareas habituales.

El equipo S tiene habilitadas sus funciones de red, pero no su terminal gráfico.

Ejercicios

1. Implantar el contexto arriba indicado, respetando *todas* las condiciones expuestas. Explicar, y probar, de qué modo el administrador de S puede conectarse desde su oficina al centro de datos de S utilizando el protocolo seguro *SSH*. Pese a que el servidor no tiene activada su interfaz gráfica, se desea que el administrador pueda ejecutar aplicaciones gráficas desde su equipo.

2. Desinstalar la actual versión del explorador de archivos *Nautilus*, e instalar, mediante *yum*, la versión más antigua de *Nautilus* que esté disponible en los repositorios a los que se tenga acceso desde S.

3. Con el fin de incrementar la seguridad de *SSH*, cámbiese en S su puerto de escucha, manteniendo la posibilidad de conexión a S desde C.

4. El administrador de S desea delegar en otro usuario, *masterseg*, las tareas de control y seguimiento de la seguridad telemática de S (en particular, la configuración del cortafuegos y el seguimiento de los accesos al sistema). Llévese a cabo esta delegación de tareas sin alterar el permiso de ningún fichero, y sin modificar el *uid* ni el *gid* de *masterseg*.

5. Imponer que la conexión a S por *SSH* sólo se pueda realizar si quien se autentica es el usuario *masterseg*, y si, además, lo hace desde C.

SUPUESTO Nº 2: Instalación de sistemas operativos

Contexto

Una máquina "limpia", sobre la que se pretenden instalar los siguientes sistemas operativos: Microsoft Windows Server 2008, Linux Ubuntu 11.04 y Linux Fedora 15 [2]

Ejercicios

1. Instalar los tres sistemas operativos, ateniéndose a las siguientes consideraciones:

   a) El espacio en disco debe quedar repartido, de modo razonablemente equitativo, entre los tres sistemas operativos.

   b) Se debe respetar en los tres casos un área *swap* acorde con la RAM física disponible.

   c) Debe existir una partición separada para el arranque, en donde esté el kernel Fedora y los ficheros de configuración de GRUB.

   d) Debe existir una partición que sirva de copia de seguridad de la partición de arranque.

   e) En las dos distribuciones Linux el espacio para ficheros temporales no debe superar las 5 GB.

   f) Las dos distribuciones Linux deben poder acceder a la partición NTFS de datos de Windows Server 2008.

   g) Las dos distribuciones Linux deben compartir:

   - El espacio para ficheros temporales.
   - Una partición común *Ext3* de 20 GB.

   Todas estas exigencias deben satisfacerse nada más arrancar el equipo, con cualquiera de los tres sistemas operativos. Se valorará, como mejora adicional, que, además, el acceso a la red y otros servicios básicos estén correctamente configurados.

2. Después de hacer una copia de seguridad de la partición de arranque, eliminarla con *fdisk* y posteriormente restaurarla, comprobando que todos los sistemas operativos funcionan correctamente.

[2] Se permite instalar, en vez de Windows Server 2008, cualquier otro sistema operativo de Microsoft que admita sistemas de ficheros NTFS. Por otra parte, la ejecución de este supuesto requiere la utilización de un lector de DVD con interfaz USB; en caso de no disponer de él, el profesor facilitará uno sólo durante las sesiones de prácticas en el laboratorio 2.7.

SUPUESTO Nº 3: Gestión de copias de seguridad

Contexto

Un equipo Linux, *H*, con una partición dedicada a copias de seguridad.

Ejercicios

1. Habilitar el espacio no usado de *H* como partición Linux destinada a servir de soporte para copias de seguridad.
2. Crear, en la partición dedicada a Ubuntu, el directorio `/root/backupfedora`, y permitir que desde Fedora se pueda acceder a él en cualquier momento (también inmediatamente después de reiniciar el equipo).
3. Programar la realización de copias de seguridad diarias de:

   a) Todos los directorios de inicio de los usuarios de Fedora, y
   b) Todos los archivos de configuración de Fedora cuyo propietario sea *root*

   en, respectivamente, los archivos `home_<AAAAMMDD>_<HHMM>.cpio` y `rootfiles_<AAAAMMDD>_<HHMM>.cpio`, donde `<AAAAMMDD>` y `<HHMM>` representan la fecha y hora actuales. Estos archivos deberán estar, obligatoriamente, en el directorio `/root/backupfedora` de la partición Ubuntu.
4. Implementar, mediante *dump*, la siguiente política de copias de seguridad sobre la partición Ubuntu completa, utilizando como destino la partición de copias de seguridad:

   - A las 01:00 AM del primer día de cada mes, realizar una copia de seguridad completa.
   - A las 03:00 AM del primer día de cada semana, realizar una copia de seguridad incremental de primer nivel.
   - A las 05:00 AM de cada día, realizar una copia de seguridad incremental de segundo nivel.
5. Simular una ejecución de la anterior política de copias a lo largo del tiempo, forzando, en primer lugar, una copia mensual; a continuación, una copia semanal y, por último, dos copias diarias (probar y documentar los cambios en el contenido de la partición Ubuntu entre cada dos copias).
6. Hacer una copia mensual de la partición Ubuntu (copia completa) y, a continuación, eliminar con *fdisk* la partición Ubuntu. Por último, recuperarla a partir de la copia de seguridad mensual.

SUPUESTO Nº 4: Gestión de versiones con Subversion

Contexto

Un host Linux, S, que actúa como servidor Subversion, un cliente Subversion bajo Linux, C_1, y otro cliente Subversion bajo Windows Server 2008, C_2.

Ejercicios

1. Instalar y configurar en S todo el software necesario para poner en marcha un servidor Subversion, teniendo en cuenta, además, los siguientes requerimientos:
   a) En caso de reiniciar S, ha de ponerse en marcha automáticamente el demonio Subversion.
   b) El cortafuegos debe permanecer activo.
2. Crear en S el repositorio `/root/repos/ejemplo`, y a continuación importar ficheros y/o directorios ubicados en otro directorio de S.
3. Configurar el acceso al repositorio de acuerdo con las siguientes exigencias:
   a) Los usuarios deben quedar divididos en dos categorías: **editores** y resto de usuarios (accesos anónimos).
   b) Dentro del grupo **editores** estarán los usuarios de Subversion *editor01* y *editor02*.
   c) Sólo los usuarios pertenecientes al grupo **editores** tendrán permiso para alterar el contenido del repositorio, previa introducción de sus correspondientes credenciales de acceso. El resto de usuarios podrá descargarse para su consulta el repositorio completo, sin necesidad de introducir contraseña alguna.
4. Realizar y documentar, al menos, las siguientes pruebas desde C_1 y C_2 (en este caso, con C_2 también bajo Linux):
   a) Descarga del repositorio, tanto por parte de usuarios anónimos como por parte de alguno de los editores.
   b) Actualización del repositorio (altas, modificaciones y supresiones).
   c) Obtención de un listado con el historial de versiones de los distintos directorios del repositorio.
   d) Eliminación de la caché del repositorio.
   e) Recuperación de una versión anterior de un fichero.
5. Reiniciar C_2 para que ahora funcione con Windows Server 2008, e instalar un cliente Subversion, comprobando su correcto funcionamiento.

SUPUESTO Nº 5: Infraestructura como servicio

Contexto

Implementación de una nube privada que sea proveedora de equipos virtuales. Mediante el hipervisor *Virtualbox* se pretende ofrecer, desde una máquina anfitriona Linux, dos máquinas virtuales accesibles para cualquier usuario que conozca sus respectivas direcciones IP y contraseñas de administración.

Estas dos máquinas virtuales, V_{cen} y V_{fed}, deben tener instalado:

- V_{cen}: Linux Centos 6.2 de 32 bits.
- V_{fed}: Linux Fedora 16 de 32 bits.

Ejercicios

1. Habilitar el espacio no usado del equipo anfitrión (unas 140 GB) como partición *Ext4* destinada a contener V_{cen} y V_{fed}.
2. Instalar las máquinas virtuales, dedicando a cada una de ellas 30 GB. Establecer en ambos casos la RAM mínima necesaria para que puedan funcionar.
3. Integrar en la red *155.54.225.0/26* las dos máquinas virtuales. Cambiar los nombres de host de V_{cen} y V_{fed} a *virtualcentos* y *virtualfedora*, respectivamente, y modificar también las contraseñas de *root*, haciendo que sean *practicascentos* y *practicasfedora*.
4. Probar las conexiones a V_{cen} y V_{fed} por *SSH*, tanto desde clientes Linux como Windows. Comprobar también que la copia telemática segura de archivos entre clientes y máquinas virtuales funciona correctamente.
5. Imponer, mediante el protocolo que resulte más adecuado, que todas las máquinas, tanto las virtuales como la anfitriona, estén sincronizadas entre sí.
6. Explicar de qué modo el administrador de la nube podría implementar un sistema tarifario basado en el tiempo de conexión, la RAM consumida y los cores utilizados.

SUPUESTO Nº 6: Autenticación Kerberos

Contexto

Tres equipos Linux, *KDC*, C_1 y C_2. El primero es el servidor Kerberos, y los otros dos son equipos clientes en los que se pretende implantar un sistema seguro de autenticación centralizada tipo *single sign-on*.

Ejercicios

1. Hacer que *KDC* sea un servidor DNS para el dominio *lab27.aso*, compuesto por todos los equipos de la red *155.54.225.0/24*. Configurar *KDC* de tal modo que, además, también sea capaz de resolver direcciones IP externas.

2. Configurar C_1 y C_2 para que su único servidor DNS sea *KDC*. En estos equipos se tiene que mantener el acceso a Internet, y, además, ha de asegurarse una perfecta sincronización horaria entre ellos y *KDC*.

3. Instalar y configurar en *KDC* todo lo necesario para crear el reino *LAB27.ASO*, asociado al dominio *lab27.aso*.

4. Implementar todas las medidas necesarias para que sea posible una autenticación SSH basada en Kerberos, en los tres equipos. A continuación, crear el principal *alumno* (de tipo usuario) y comprobar el correcto funcionamiento de la configuración realizada.

5. Hacer posible una autenticación Kerberos a la hora de abrir cualquiera de los terminales. Crear varias cuentas de usuario sin password local, junto con sus respectivos principales, para comprobar la corrección de la configuración implantada.

NOTA: *KDC* debe proveer todos los servicios automáticamente justo después de ser arrancado. El cortafuegos, por otra parte, ha de permanecer activo, aplicándose, en cualquier caso, las reglas imprescindibles que permitan prestar todos los servicios indicados.

SUPUESTO Nº 7: NFS y autenticación Kerberos para HTTP

Contexto

El punto de partida es el reino *LAB27.ASO* creado en el supuesto anterior. Además, ahora se habilitará C_1 como servidor web *Apache*, creándose una página de acceso libre y otra de acceso restringido que requiera autenticación Kerberos. También se habilitarán accesos NFS que hagan viable una edición web remota.

Ejercicios

1. Instalar el servidor web *Apache* en C_1, y crear las páginas *http://<nombre_ C_1>/lab27.aso* y *http://<nombre_ C_1>/lab27.aso/privado*, con un contenido simple que permita distinguirlas. No imponer, de momento, ninguna restricción de acceso.

2. "Kerberizar" HTTP en C_1, permitiendo el acceso libre a la página *http://<nombre_ C_1>/lab27.aso*, y un acceso limitado a *http://<nombre_ C_1>/lab27.aso/privado*, para únicamente aquellos usuarios que formen parte del reino *LAB27.ASO*.

3. Configurar en C_1 y C_2 el navegador web *Mozilla Firefox* para que soporte autenticación Kerberos.

4. Reconfigurar C_1 para permitir solamente a un usuario determinado el acceso a la web privada.

5. Exportar vía NFS los directorios en donde se encuentran los archivos HTML de las dos páginas, de tal modo que al usuario *webmaster*, que también formará parte del reino *LAB27.ASO*, le sea posible la edición de las mismas desde C_2. Además, en C_2 deben estar visibles, nada más arrancar, los directorios exportados desde C_1, y únicamente el usuario *webmaster* debe poder realizar ediciones web.

NOTA: C_1 debe proveer todos los servicios automáticamente justo después de ser arrancado. El cortafuegos, por otra parte, ha de permanecer activo, aplicándose, en cualquier caso, las reglas imprescindibles que permitan prestar todos los servicios indicados.

SUPUESTO Nº 8: Microsoft Active Directory

Contexto

Tres equipos el dominio **empresaprueba.es**, con las siguientes funciones:

- H_1: controlador de dominio con Windows Server 2008.
- H_2: servidor miembro con Windows Server 2008; se utiliza como servidor de archivos.
- H_3: servidor miembro con Windows XP; se utilizan como lugar de trabajo habitual de cualquiera de los empleados de la empresa.

Ejercicios

1. Implantar el dominio **empresaprueba.es** en los tres equipos, de acuerdo con los requisitos planteados.
2. Establecer la siguiente estructura organizativa:
   - Unidad organizativa **GERENCIA**: formada por el usuario **jefe**.
   - Unidad organizativa **COMERCIAL**: formada por los usuarios **com01** y **com02**.
   - Unidad organizativa **DESARROLLO**: formada por las unidades organizativas **TESTEO** y **PROGRAMACION**.
   - Unidad organizativa **TESTEO**: formada por el usuario **test01**.
   - Unidad organizativa **PROGRAMACION**: formada por los usuarios **prog01** y **prog02**.

   Se desea delegar el control sobre la unidad organizativa **COMERCIAL** en el usuario **com01**, y el de la unidad organizativa **DESARROLLO** sobre el usuario **prog01**.
3. Instalar en todos los servidores miembro las herramientas administrativas de Active Directory.
4. En H_2:
   a) Crear las carpetas `C:\empresaprueba\confidencial`, `C:\empresaprueba\promociones` y `C:\empresaprueba\programas`.
   b) Asignar a los usuarios del dominio permisos sobre los anteriores recursos, del siguiente modo:
      - `C:\empresaprueba\confidencial`: lectura-escritura únicamente para el usuario **jefe**.
      - `C:\empresaprueba\promociones`: lectura-escritura para **jefe** y **com01**. Sólo lectura para **com02**.
      - `C:\empresaprueba\programas`: lectura-escritura para **jefe**, **prog01** y **prog02**. Sólo lectura para **test01**.

   Dar de alta las tres carpetas dentro del dominio, con los nombres **docgerencia**, **doccomercial** y **fuentes**, respectivamente.
5. Impedir que ningún usuario, salvo los programadores, puedan hacer uso del panel de control.
6. Probar y comentar las funcionalidades ofrecidas por la utilidad *ldifde*, así como su relación con el protocolo *LDAP*. Dar de alta, mediante esta utilidad, los usuarios **prog03**, **prog04** y **com03** en sus correspondientes unidades organizativas.