SEP-03

Los entornos gráficos típicos en los entornos UNIX son los sistemas de ventanas X (*X Window*). Estos entornos están construidos sobre una arquitectura cliente-servidor.

a). ¿Qué elemento hace el papel de servidor y cuáles son sus responsabilidades?
b). ¿Qué elementos pueden hacer de clientes?
c). El Gestor de Ventanas (*Window Manager*) ¿qué servicios proporciona?, ¿hace el papel de cliente o de servidor?
d). ¿Cómo se puede hacer que el sistema arranque en módo gráfico (es decir mostrando una ventana de login gráfico)?

FEB-04

Asocie los siguientes servicios o mecanismos con el concepto o aplicación para el cual están diseñados o pueden servir. **NOTA**: Cada entrada (de la izquierda y de la derecha) puede tener, ninguna, una o varias líneas que la asocien con entradas en la otra columna.

1- NFS	a- Dispositivos de almacenamiento redundantes
2- NIS	b- Ventana de *login* gráfico de acceso al sistema
3- SSH	c- Mecanismo aplicable a la gestión de usuarios y *passwords*
4- FDDI	d- Compartición de sistemas de ficheros (UNIX-UNIX)
5- Shadow	e- Compartición de sistemas de ficheros (UNIX-Win)
6- RAID	f- *Login* remoto con cifrado de conexión
7- X11	g- Servicio de tipo RPC
8- XDM	
9- Samba	

JUN-04

Construya 5 sentencias que sean **verdaderas** en lo referente a los conceptos de administración de sistemas UNIX (y estrictamente relacionados con ella). Cada sentencia se podrá construir usando un elemento de cada una de las columnas. No se podrá usar dos veces el mismo elemento en sentencias diferentes:

NFS	…se almacena en …	log de operaciones
El *portmapper*	…permite la conectividad con…	RPCs
El modo autónomo	…escucha…	XDM
El profesor de SSOO	…se programa con …	Sistemas Windows
Una clave cifrada	…evita el abuso de …	DNS
SMB	…configura la red para…	*shadow*
PABS	…sincroniza datos de…	Jethro Tull
JFS	…es un modo de funcionamiento de…	*peer-to-peer*
Inetd	…dispone de un …	X11

SEP-04

Su amiga Rigoberta le llama alarmada para que usted acuda a ayudarla. Ella sospecha que, dentro de la red de ordenadores de su pequeña empresa ha podido entrar un *hacker*. La red está compuesta por equipos Windows (puestos de trabajo) y Linux (servidores de cuentas de usuario vía *samba* y de correo electrónico). La red no tiene un *firewall* y todos los equipos están directamente conectados a Internet a través de un *router*.

Se pide:

a) Tras una sonora bronca, ¿qué acciones tomaría, y en qué orden, de cara a localizar el o los equipos posiblemente comprometidos?
b) Dado un equipo UNIX bajo sospecha, ¿qué posibles acciones maliciosas podrían haberse llevado a cabo? y ¿qué efecto pueden éstas tener?
c) ¿Qué aspectos del sistema estudiaría para determinar si el sistema ha sido manipulado o han habido intentos de manipulación?
d) ¿Qué acciones correctivas permitirían restituir la red a una situación segura con mayor grado de garantía? (Considérese que Rigoberta es muy paranoica).

e) ¿Qué recomendaciones básicas de seguridad le realizaría a Rigoberta para que no vuelva a verse en esta situación en el futuro?

FEB-05

Debido a lo desmesuradamente complicado que ha sido el último examen de Diseño de Sistemas Operativos, cuyos resultados espera que sean poco satisfactorios, se ha visto obligado a tomar medidas desesperadas (y evidentemente delictivas). Para ello, y bajo el seudónimo de AMORPHEO, usted se va a convertir en un avispado *hacker* en cruzada personal contra los profesores de la asignatura. El grupo de sistemas operativos dispone de una máquina UNIX, denomina `ilws.datsi.fi.upm.es` (ILWS son las siglas de "*I love William Stallings*") donde mantiene las aplicaciones y datos relativos a las calificaciones.

a) El primer paso debe consistir en entrar en el sistema (como cualquier usuario del mismo). Indique **dos** formas de ganar dicho acceso al sistema violando la seguridad de la máquina.

b) Supóngase que ha accedido al mismo suplantando la personalidad del usuario `chema`. ¿Qué estrategia (evidentemente ilegítima) se podría utilizar para convertirse en el usuario `root`? (Evidentemente no conoce la contraseña de `root` y además, como éste es un tipo inteligente su contraseña es una combinación de caracteres difícil de adivinar)

c) Una vez suplantado al administrador del sistema, se propone realizar las siguientes acciones perniciosas. Para cada una de ellas describa brevemente cómo las realizaría e indique si dicha acción tiene un nombre determinado dentro de los términos de seguridad:

   c.i) [AVERIGUAR CONTRASEÑAS DE OTRAS MÁQUINAS] Debido a que hay profesores que utilizan sus propias máquinas para corregir las prácticas, a usted le parecería apropiado intentar conseguir nombres de usuario y contraseñas válidas de otras máquinas de la misma red.

   c.ii) [MODIFICAR LAS NOTAS] El programa para registrar las calificaciones usa una base de datos cifrada de la que se desconoce las claves y que no parece razonable poder descifrar antes de la convocatoria de Septiembre. De dicho programa sí se dispone del código fuente.

d) Antes de abandonar el sistema, ¿cuáles serías las acciones que habría que realizar para impedir que fuésemos detectados….. y posteriormente sancionados?

JUN-05

Tu amigo Evaristo ha tenido un serio problema con su ordenador (un sistema Linux). Debido a un problema de tensión eléctrica varias particiones han quedado inutilizables (superbloques y/o contenidos corruptos). Los discos del sistema se encuentran particionados como:

- Primer disco (/dev/hda):
  - Partición raíz (/bin, /boot, /etc, /var): /dev/hda1 [OPERARTIVA]
  - Partición de *swap*: /dev/hda2 [CORRUPTA]
  - Partición de usuarios (/home): /dev/hda3 [CORRUPTA]
- Segundo disco (/dev/hdb):
  - Partición de aplicaciones del SO (/usr): /dev/hdb1 [CORRUPTA]
  - Partición para archivos temporales (/tmp): /dev/hdb2 [OPERATIVA]
  - Partición de aplicaciones extra (/opt): /dev/hdb3 [CORRUPTA]
  - Espacio libre sin asignar.

a) **[2 puntos]** ¿Cuáles son los directorios y particiones mínimas para poder arrancar un sistema UNIX e iniciar su recuperación?. En la situación actual, ¿podría Evaristo arrancar su equipo?

b) **[1 punto]** Los contenidos de la partición /dev/hdb1 es recuperable por medio de la utilidad estándar de verificación de la integridad de un sistema de ficheros de forma manual. ¿Cuál es dicha utilidad?

c) **[4 puntos]** Evaristo tiene una copia de backup completa de los contenidos de /opt y un backup incremental del directorio /home. Indíquele a su amigo, paso a paso, cómo recuperar su sistema. Evaristo es relativamente habilidoso en estos temas y sabe hacer perfectamente cosas como "arrancar o cambiar de run-level", "montar o crear sistemas de ficheros", "hacer y deshacer backups". Utilice estos términos en su explicación.

d) **[3 puntos]** Semanas después de haber recuperado su equipo, su amigo le pide ayuda para hacer una actualización del sistema operativo. La nueva versión del mismo ocupa ligeramente más y no entra en las particiones de sistema y aplicaciones.
   - ¿Cuáles con las particiones cuyo contenido se conserva y cuáles no?
   - ¿Cuál sería la estrategia para reparticionar el disco con el mínimo movimiento de particiones?. El

espacio libre del final es relativamente pequeño (no entra el nuevo sistema operativo entero).

SEP-05

Después de instalar un nuevo servicio llamado su_seguro_servidor, que usa el puerto TCP 666, el administrador pretende configurar el sistema de manera que este servicio se active automáticamente al arrancar el equipo. Este servicio sólo debe activarse cuando el sistema arranque en modo multiusuario y con red, ya sea en modo gráfico o no. Asimismo, el momento de activación de este servicio debe de ser tal que se asegure que antes ya se ha activado otro determinado servicio, cuyo arranque automático ya está configurado en la versión actual del sistema. Se pide:

- **a)** Explicar qué acciones debería llevar a cabo el administrador, especificando el nombre de los ficheros que debe modificar y/o crear.
- **b)** Supóngase que el administrador cambia de estrategia y decide que el servidor no debe arrancarse inicialmente sino que se arrancará cuando se produzca la primera solicitud dirigida al mismo. ¿Cómo se realizaría en este caso la configuración? ¿Qué ventajas y desventajas tiene esta estrategia frente a la planteada en el apartado previo?