Curso de Introducción a la Informática

Práctica:	**LINUX: AUDITORÍA**
Profesor:	Héctor Menéndez
Departamento:	Ingeniería Informática
Centro:	Escuela Politécnica Superior
Curso:	2012/13
Tiempo estimado:	1 hora 30 min

Objectivos y Descripción

El objetivo de esta práctica es adquirir una serie de conocimientos más avanzados sobre el manejo de un Sistema Operativo Linux como auditores.

Estos ejemplos muestran una serie de características que complementan en gran medida los conocimientos adquiridos en la parte sobre usuario avanzado y administración en Linux.

En este caso no se desarrolla un guión sino una serie de ejercicios por bloques que complementen las tranparencias.

Bloque 7: Auditoría, Logs y Backups

Sistemas de Auditoría

Ejercicio 1. *Ver y estudiar el fichero de configuración de audit.*

Ejercicio 2. *Pasar parámetros a través de auditctl para controlar passwd y shadow.*

Ejercicio 3. *Pasar parámetros para controlar llamadas al sistema.*

Ejercicio 4. *Limpiar las reglas del sistema.*

Ejercicio 5. *Mostral la lista de reglas.*

Ejercicio 6. *Ver los logs de /var/log/audit/audit.log. Explicarlos.*

Ejercicio 7. *Ver y estudiar el fichero de configuración de audit.*

Ejercicio 8. *Generar distintos informes con aureport.*

Ejercicio 9. *Realizar distintas búsquedas con ausearch.*

Ejercicio 10. *Realizar un trace a less con autrace.*

Ejercicio 11. *Generar un informe sumario.*

Ejercicio 12. *Utilizar herramientas de visualización sobre el informe sumario.*

Herramientas para monitorizar a un usuario

Ejercicio 13. *Traquear usuarios con los comandos con ac, sa y lastcomm.*

Logs del sistema

Ejercicio 14. *Comprobar los distintos ficheros de logs que genera el sistema.*

Generación de Backups

Ejercicio 15. *Probar los ejemplos de sincronización de rsync.*