PRÁCTICA 2 – PERMISOS

Vamos a crear una estructura de directorios similar a la que dispone el centro (socrates), imponer restricciones de contraseñas y acceso y administrar las cuentas de usuarios del centro educativo.

1. Obtén información acerca de los ficheros */etc/passwd, /etc/group, /etc/shadow y /etc/pam.d/common-password*. ¿Cómo se estructura la información que aparece en él?

2. Crea tantos directorios como ciclos/estudios tenga el centro. Crea cuentas de usuario suficientes (al menos una por curso) para poder realizar las pruebas, simulando a los alumnos y profesores del centro. Adicionalmente, tenemos un directorio general común accesible por todos los alumnos y profesores y otro sólo accesible por los profesores.

3. Configura unos requisitos de contraseña que vas a requerir por parte de los usuarios y comprueba su funcionamiento con distintas restricciones. ¿Tienes algún problema al realizar cambios de contraseña, insistiendo por una contraseña que no cumple esos mínimos? ¿Cuáles son los requisitos mínimos de seguridad que tiene por defecto sin ninguna configuración?

4. Configura todo lo necesario para que sólo los usuarios (estudiantes) de un determinado ciclo/estudio tengan acceso exclusivo a sus materiales (y al general) y no al resto. Del mismo modo para los profesores ¿Nos encontramos con algún problema?

5. Configura, prueba y alterna otorgando distintos permisos y listas de control de acceso. Permite que determinados alumnos tengan acceso a determinados archivos de otros ciclos ¿Qué similitudes y diferencias encuentras en la hora de implementarlo? ¿Qué limitaciones podemos solventar con el uso de ambos métodos y a su vez que limitaciones nos presenta? ¿Nos encontramos con algún problema?

6. Conéctate con cuentas de usuarios de forma remota (*ssh*) y comprueba su funcionamiento.

7. Qué amenazas y técnicas de ataque nos vamos a tener que enfrentar en nuestro sistema para tener que realizar esta protección.

8. Obtén información de la herramienta *John The Ripper*. Instala el paquete John y crea un listado (*listado.lst*) de palabras posibles de contraseñas, incluyendo alguna de los usuarios e intenta obtener la contraseña con el correspondiente usuario.

Deberán incluirse justificación y evidencia de las máquinas empleadas, cualquier cambio de la configuración del entorno de virtualización, así como poder defender el trabajo realizado en caso de que sea solicitado.

Toda imagen utilizada para demostrar una evidencia deberá ir con su correspondiente numeración, descripción y referenciado correctamente en el texto.

La fecha de entrega definitiva se fijará entre todos, así como el procedimiento de entrega.