| EJERCICIO PRÁCTICO  Desarrollo de Aplicaciones Web  (1WET)  Sistemas Informáticos |
| --- |

| **DOCENTE**  Enrique Diego Alfonso | **ALUMNO**  Hugo Ruiz Sánchez  . |
| --- | --- |

| **ENUNCIADO**  Propuesto en cada cuestión del ejercicio. |
| --- |

**Gestión de usuarios en Linux**

| 1. Crea los grupos SI1 SI2.      1. Crea los usuarios usuario1 y usuario2. Ambos deben pertenecer únicamente al grupo SI1.      1. Crea los usuarios usuario3 y usuario4. Ambos deben pertenecer únicamente al grupo SI2.      1. Intenta eliminar el grupo SI1.     No es posible eliminar el grupo, sin borrar antes a los usuarios quelo integran.   1. Comprueba que los usuarios y grupos han sido creados correctamente. |
| --- |

**Seguridad de cuentas de usuarios en Linux**

| 1. Asigna la contraseña sistEmas\_%20 a todos los usuarios utilizando el comando usermod      1. Deshabilita la cuenta de usuario3 y bloquea la contraseña de usuario4.      1. Habilita la cuenta de usuario 3 y desbloquea la contraseña de usuario4.      1. Establece 20 días como máximo y 10 días como mínimo para cambiar la contraseña de usuario2 2. Establece una fecha de usuario4 a partir de la cual la cuenta caducará y será inaccesible. |
| --- |

**Gestión db e recursos y permisos en Linu**

| 1. En tu caperta personal crea la carpeta dirPerm y dentro de ella un archivo llamado permisos.      1. Emplea la notación octal para modificar los permisos de dirPerm a rwx r-- —      1. Emplea la notación simbólica para deshabilitar el permiso de lectura para el grupo sobre el archivo permisos.      1. Emplea la notación octal para modificar los permisos de dirPerm rwx rwx rwx-      1. Emplea la notación simbólica para rehabilitar todos los permisos para el propietario del grupo y deshabilitar todos los permisos al resto de usuarios sobre el archivo permisos      1. Cambia el propietario y grupo de permiso a usuario1 y SI1 respectivamente afectando a todo su contenido. |
| --- |

**Permisos especiales en Linux**

| 1. Crea un directorio llamado dirCompartido en el que todos los usuarios del grupo SI2 pueden escribir para guardar sus archivos en sus carpetas.        1. Modifica los permisos del directorio para que solo el propietario de cada objeto pueda borrar sus propios archivos.      1. Modifica los permisos de dirCompartido para que los archivos y subdirectorios creados en su interior sean forzados a pertenecer al grupo del directorio y no al grupo del usuario que lo haya creado. |
| --- |

**Máscara de permisos en Linux**

| 1. Para usuario 1 modifica la máscara de permisos por defecto para que los ficheros creados tengan todos los permisos activos. Comprueba si es posible.        1. Configura la máscara de permisos por defecto para que los nuevos ficheros del propietario tenga permiso de lectura solo y los demás no tengan ningún permiso      1. Sal de la sesión de usuario1 y comprueba si se ha guardado la máscara de permisos. |
| --- |

**Súper usuario en Linux**

| 1. ¿Por qué se encuentra la cuenta root deshabilitada por defecto?   La cuenta root está deshabilitada por defecto en muchos sistemas operativos debido a motivos de seguridad. La cuenta root es una cuenta con privilegios de superusuario que tiene acceso a todos los recursos y configuraciones del sistema operativo. Si se habilita esta cuenta, es más probable que se produzcan errores y problemas de seguridad, ya que cualquier persona con acceso a ella podría tener acceso completo al sistema.   1. ¿Cómo se podría habilitar? |
| --- |

**Gestión de usuarios en Windows desde la consola de Administracion de equipos**

| 1. Crea los grupos SI1 SI2.          1. Crea los usuarios usuario1 y usuario2. Ambos deben pertenecer únicamente al grupo SI1.          1. Crea los usuarios usuario3 y usuario4. Ambos deben pertenecer únicamente al grupo SI2.        1. Comprueba que los usuarios y grupos han sido creados correctamente. |
| --- |