Seguridad Informática 2020/2021.

Práctica 3

MUY IMPORTANTE: Leer el documento con la normativa sobre estas prácticas.

Objetivo: Especificar e implementar la seguridad en Sistemas Operativos.

La práctica se realiza en el entorno de virtualización VirtualBox. En esta práctica se utiliza el siguiente sistema, cuya imagen virtual ya está creada:

Máquina CentOS 6.4: **c-diff**

Credenciales: **u** / **toor** Credenciales admin: **root** / **drowssap**

Es una máquina CentOS, con alguna modificación. Está en:

https://unizares-my.sharepoint.com/:f:/g/personal/gvalles_unizar_es/EgMaqbww_bJJhjm_bUFOB2YBPy-5eOtQ0U5gtWaRfniHRw?e=X1F0mI

Para crear las máquinas en VirtualBox, seleccionar el menú "Archivo->Importar servicio virtualizado".

Parte I: Información, estado y dominios en SELinux

1. En primer lugar, entrar en sesión con el usuario u.
2. Anotar con ayuda de "ps aux" los diferentes usuarios efectivos de todos los procesos en ejecución en el sistema.
3. Ejecutar "ps auxZ". ¿Que usuarios Linux están ejecutando procesos en dominios "unconfined_t"? ¿Que usuarios Linux están ejecutando procesos con usuario y rol "system_u" y "system_r"? ¿Por que están unos en dominios "unconfined_t" y otros no?
4. Invocar "passwd" en otra terminal y dejarlo en ejecución sin contestar. ¿Que usuario Linux, usuario SELinux y rol SELinux tiene el proceso "passwd"? ¿Por que?
5. Poner en funcionamiento la aplicación de gestión gráfica de SELinux en CentOS a través de menu "System" -> "Administration" -> "SELinux Management" (contraseña de root). Con esta aplicación se pueden ver los diferentes elementos de SELinux y modificarlos (no modificar nada todavía). SELinux puede estar en estado deshabilitado (disabled) o habilitado (enabled). Cuando está habilitado reside en estado forzado (enforcing) o permisivo (permissive). El estado forzado aplica la política seleccionada (normalmente, targeted). El estado permisivo activa la política pero no la aplica. Si hay violación de la política únicamente se informa de ello, pero no se bloquea nada. El estado permisivo viene muy bien para depuración de políticas. Estos cambios de estado se puede realizar de forma persistente en /etc/selinux/config y aplicarlos con un rearranque de sistema, o temporalmente con setenforce. Para ver el estado en que se encuentra se pueden utilizar "getenforce" o "sestatus | grep mode". También se pueden deshabilitar protecciones para servicios específicos poniendo el dominio asociado al proceso servidor en modo

permisivo con la aplicación de gestión que se ha abierto anteriormente o con "semanage permissive -a httpd_t". La aplicación gráfica deja ver la lista de todos los dominios cargados y su estado en "Process domain". Para obtener solo la lista de los permisivos, con "semanage permissive -l". Hay aplicaciones que cambian de comportamiento si SELinux está activado o desactivado (ls, id, ps, ssh...).

Parte II: Usuarios en SELinux

6. Acceder a cuenta root en una terminal de la sesión del usuario "u" mediante "su -".
7. Crear nueva cuenta de usuario "c" con "adduser –Z user_u c". Asignarle un password mediante "passwd c". Es decir, se asigna el usuario SELinux "user_u" al usuario Linux "c". Entrar desde una terminal a la nueva cuenta creada con "su - c". ¿Que datos de contexto SELinux da el comando "id"?
8. Comprobar asignación de cuenta Linux "c" a cuenta SELinux "user_u" desde el terminal root con "semanage login -l". Se observa que no aparece el usuario "u". La cuentas que no aparecen es porque son asimiladas a Login Name "default", luego son asignadas al usuario SELinux "unconfined_u".
9. Salir de la sesión gráfica del usuario "u" y volver a entrar con el usuario "c".
10. Ejecutar "id". ¿Que salida de contexto da SELinux ahora? ¿Por que es diferente a la salida del comando "id" ejecutado en apartado 7?
11. Abrir una terminal y acceder a cuenta "root" mediante comando "su -". ¿Que ocurre? ¿Por que es diferente al comportamiento de este comando desde la cuenta "u" y desde la cuenta "c"?

Parte III: Listas de Control de Accesos (ACLs) basados en estándar POSIX de Unix del modelo DAC

12. "getfacl" y "setfacl" son comandos para manipular las Listas de Control de Accesos POSIX en Linux. Permiten una asignación mas fina y amplia de permisos a usuarios que solo los 3 ámbitos clásicos de usuario propietario, grupo propietario y los demás. Es el método utilizado en Windows (con permisos mas detallados). Permite asignar permisos de acceso a un fichero a diversos usuarios individuales o grupos mediante los permisos "RWX" de siempre.
13. Crear un fichero en el "home" de usuario "u" y añadir con "setfacl" permisos de lectura y ejecución al usuario "c" y solo de lectura al grupo "c". Comprobar la modificación con "getacl".

Parte IV: Reglas de control de accesos y acceso a dominios

14. Para tener autorización de acceso a un fichero, primero debe existir una regla que permita dicho acceso a partir de un dominio donde se ejecuta el proceso que nos permite dicho acceso, de la forma: allow <fuente> <destino> : <clase> <permisos>
    Donde <fuente> es siempre un dominio y <destino> es cualquier tipo. El campo <clase> permite diferenciar permisos basados en recursos, según sean ficheros regulares, directorios, sockets TCP, etc. Listado de todas las clases con "seinfo -c". Cada clase tiene un conjunto de permisos propio. Para conocer los permisos de una clase, por ejemplo de

un fichero, "seinfo -cfile -x". Se puede solicitar información de la reglas "allow" cargadas con "sesearch –A [-s <dominio fuente>] [-t <tipo destino>] [-c <clase>] [-p <permisos>]

15. ¿A que dominios se les permite acceder a ficheros tipo "shadow_t" y clase "file" con permisos de escritura "write"? ¿Que significa esto?
16. ¿A que dominios puede acceder el rol "user_t" (es decir el usuario "c")? Usar "seinfo -ruser_r -x".