Administración de Sistemas Unix/Linux
Practica: IPTables

Rafael García Damián 313103591
Carmona Mendoza Martín 313075977
Barajas Figueroa José de Jusús 314341015
Vazquez Aguilar Lisandro 314272117

11 de Mayo de 2019

1. Al instalar CentOS, por default crea los siguientes usuarios: sysadm_u, system_u, xguest_u, root, guest_u, staff'_u, user_u y unconfined_u. Investiga cuales son las diferencias entre ellos y con que comandos puedo ver que tiene permitido cada uno de ellos.

   - sysadm_u
     Tiene los mismos privilegios que el usuario $staff\_u$ con la diferencia de que puede hacer uso del comando su. Solo debe tener el rol $sysadm\_r$.
   - $system\_u$
     Este es un usuario para los servicios del sistema, por lo que ningún usuario debe mapearse a él.
   - $xguest\_u$
     Este usuario tiene acceso a la GUI y a la red únicamente desde el navegador web firefox, no tiene permisos de ejecución de scripts y únicamente tiene acceso al rol $xguest\_r$
   - *root* Es el usuario al que se mapea por defecto el usuario root de SELinux, por lo que debe tener privilegio para poder hacer lo mismo que hace el usuario root.
   - $guest\_u$
     Este es un usuario sin privilegios, no tiene acceso a la red ni a la ejecución de scripts. Solo tiene acceso al rol $guest\_r$.
   - $staff\_u$
     Este usuario puede obtener mayores privilegios ya qu puede usar el comando sudo, ademas tiene acceso a la GUI y a la red.
   - $user\_u$

Este usuario tiene permitido el acceso a GUI a y a la red, ademas de que puede ejecutar los archivos contenidos en su directorio home, ademas tiene acceso a los archivos con el type *user_t*.

- *unconfined_u*
  Este usuario no tiene restricciones de privilegios. Además puede tomar los roles *unconfied_r* y *system_r*.

Para ver a que tiene acceso un usuario determinado podemos hacer uso de los siguientes comandos:

```
[root@localhost ~]# semanage user -l

                Etiquetado MLS/       MLS/
Usuario SELinux  Prefijo    Nivel MCS  Rango MCS                  Roles SELinux

guest_u         user       s0         s0                         guest_r
root            user       s0         s0-s0:c0.c1023             staff_r sysadm_r system_r uncon
fined_r
staff_u         user       s0         s0-s0:c0.c1023             staff_r sysadm_r system_r uncon
fined_r
sysadm_u        user       s0         s0-s0:c0.c1023             sysadm_r
system_u        user       s0         s0-s0:c0.c1023             system_r unconfined_r
unconfined_u    user       s0         s0-s0:c0.c1023             system_r unconfined_r
user_u          user       s0         s0                         user_r
xguest_u        user       s0         s0                         xguest_r
[root@localhost ~]#
```

Figure 1: Listado de usuario y roles permitidos para ellos.

Una vez obtenidos los roles a los que tiene acceso el usuario podemos consultar a que dominios y que tipos de objeto tienen acceso dichos roles con el comando *sesearch*:

```
[root@localhost ~]# seinfo -rguest_r -x | head -15
   guest_r
      Dominated Roles:
         guest_r
      Types:
         alsa_home_t
         antivirus_home_t
         httpd_user_script_t
         auth_home_t
         chkpwd_t
         updpwd_t
         chrome_sandbox_home_t
         chronyc_t
         container_home_t
         cvs_home_t
         fetchmail_home_t
[root@localhost ~]# _
```

Figure 2: Algunos roles y tipos para el rol *guest_r*

De igual manera para ver las reglas relacionadas con un dominio o tipo de objeto también podemos hacer uso del comando *sesearch*:

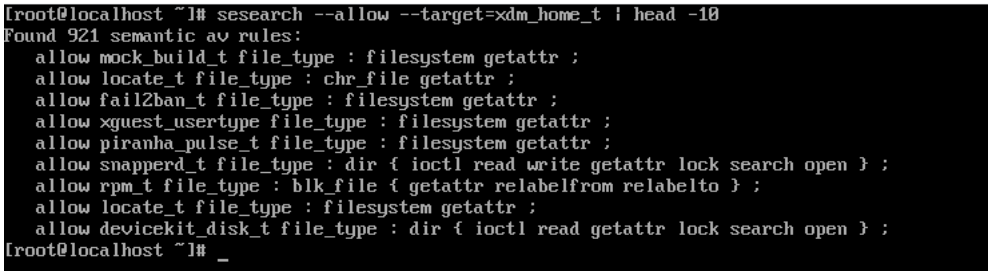

Figure 3: Algunas reglas con el objeto *xdm_home_t* como objetivo de la regla.

2. Al crear un usuario de linux en un sistema con SELinux por default se le asigna un usuario de SELinux. ¿En qué tipo de sistemas convendría los usuarios que tiene por default CentOS? Cambia el usuario por default de SELinux que se asigna en CentOS.

   Convendría en un sistema que sea para uso personal, ya que aunque CentOS ya tiene usuarios definidos, siempre que se agrega un nuevo usuario este se mapea por default al usuario *unconfined_u* el cual no tiene restriscciones ya que puede acceder al rol *system_r*.

   Para cambiar el usuario default al que se mapean los nuevos usuarios hacemos uso del comando *semanage*.

Figure 4: Cambio del mapeo por default de los usuarios.

Revisando nuevamente el mapeo de usuarios podemos ver que ahora a los nuevos usuarios se le asignará por default el usuario *guest_u*

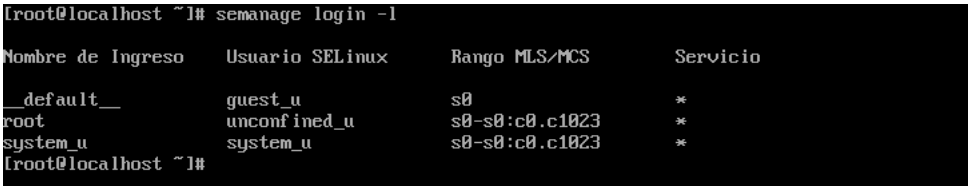

Figure 5: Mapeo por default cambiado.

3. Investiga el comando *auditallow*, ¿para qué sirve? ¿Cómo se usa? Da un ejemplo de uso.

   No encontramos el comando *auditallow* por lo que el más parecido fue:

audit2allosw este comando genera una política permisiva de a partir de los registros (*logs*) de operaciones negadas, por lo que esta nueva política permitirá las operaciones a las que previamente se les denegaba el acceso.

Ejemplo de uso: para ver las reglas que permitirían un acceso de las operaciones negadas usamos el comando *audit2allow* $-a$:

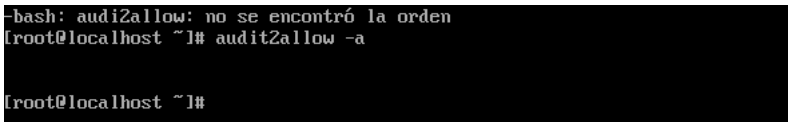

Figure 6: Cuando no hay logs de operaciones negadas la salida de este comando es vacía.

4. Crea un usuario tal que solamente pueda tener acceso a su carpeta home. Si el nombre de usuario es *user* entonces se debe agregar un tipo de archivo *user_t* y todos los archivos de dicho usuario deben tener ese tipo.

   Ya que el usuario user_u de selinux cumple con lo requerido ya que solo tiene acceso a su home, a la red y las etiquetas en SELinux se heredan del directorio padre y en linux el directorio home de cada usuario tiene la etiqueta (nombre del usuario)_home_dir_t nos basta con cambiar el usuario de SELinux al que se mapea el usuario *user*:

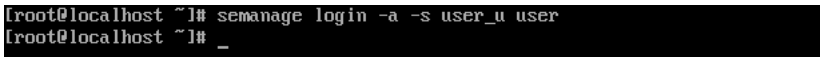

Figure 7: Le asignamos el usuario de SELinux a user

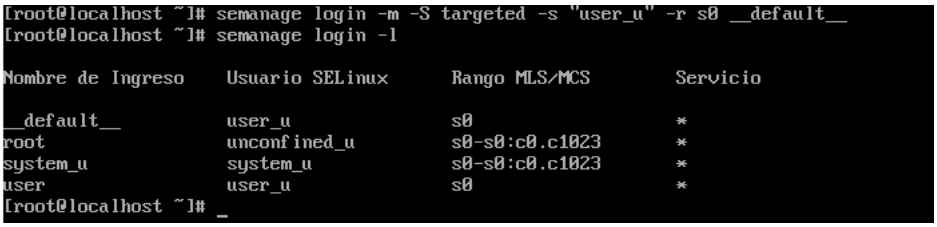

Figure 8: Para que todos los usuarios tengan estas restricciones hacemos que por default se mapeen al usuario user_u en SELinux

5. Dependiendo de los requerimientos del sistema, a ciertos usuarios, procesos o carpetas pueden tener acceso o no a recursos del sistema. Crea dos reglas de SELinux:

   -
   -