SEGURIDAD EN SISTEMAS OPERATIVOS
4º Grado en Informática – Complementos de Ing. del Software
Curso 2017-18

Práctica [1]

Sesión [4]

Autor[1]: Iván Rodríguez Millán

Ejercicio 1.

[root@ivancito ivancito]# useradd -m admin

[root@ivancito ivancito]# semanage user --roles 'sysadm_r' --prefix user --add admin_u

[root@ivancito ivancito]# semanage login --add --seuser admin_u admin

[root@ivancito ivancito]# passwd admin

Cambiando la contraseña del usuario admin.

Nueva contraseña:

CONTRASEÑA INCORRECTA: La contraseña no supera la verificación de diccionario - Está basada en una palabra del diccionario.

Vuelva a escribir la nueva contraseña:

passwd: todos los tokens de autenticación se actualizaron exitosamente.

En primer lugar creamos el usuario correspondiente en Linux.

En segundo lugar añadimos con la orden semanage añadimos un usuario SELinux al sistema asignandole el role sysadm_r y después con semanage login conecta el usuario SELinux con nombre admin_u.

Por último se modifica la contraseña para el usuario.

---

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la "Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada" esto "conllevará la calificación numérica de cero … independientemente del resto de calificaciones que el estudiante hubiera obtenido ..."

Ejercicio 2.

En primer lugar comprobamos que SELinux está corriendo y en estado enforcing:

[root@ivancito ivancito]# sestatus

```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      30
```

En segundo lugar vamos a provocar un fallo del tipo introducir mal la contraseña para root para generar un error en el archivo /var/log/audit/audit.log .

Una vez generado el error podemos auditarlo con el comando :

ausearch -ts recent

```
type=USER_AUTH msg=audit(1510136534.434:434): pid=4762 uid=1003 auid=1000 ses=4 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=? acct="root" exe="/usr/bin/su" hostname=ivancito addr=? terminal=pts/0 res=failed'
```

En el error podemos ver que el fallo ha sido del tipo ‘USER_AUTH’ (autenticación de espacio de usuario según https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-audit_record_types).También podemos ver que el resultado no ha sido aceptado res=failed.

Ejercicio 3.

Según se puede leer en la documentación podemos modificar el estado de enforcing a permissive y viceversa con la orden setenforce:

```
setenforce(8)                                   SELinux Command Line documentation
setenforce(8)

NAME
      setenforce - modify the mode SELinux is running in

SYNOPSIS
      setenforce [Enforcing|Permissive|1|0]

DESCRIPTION
      Use Enforcing or 1 to put SELinux in enforcing mode.
      Use Permissive or 0 to put SELinux in permissive mode.

      If  SELinux  is  disabled  and you want to enable it, or SELinux is enabled and you
want to disable it, please see
      selinux(8).

AUTHOR
      Dan Walsh, <dwalsh@redhat.com>

SEE ALSO
      selinux(8), getenforce(8), selinuxenabled(8)

dwalsh@redhat.com                                                    7  April  2004
setenforce(8)
```

Para ello hacemos lo siguiente:

setenforce permissive

Y comprobamos que las modificaciones han salido correctamente:

sestatus

```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      30
```

Y efectivamente ya tenemos SELinux en modo actual permissive.

También podemos saber el estado actual de SELinux con el siguiente comando:

```
[root@ivancito ivancito]# getenforce
Permissive
```

Ejercicio 4.

Para completar la tabla en primer lugar mostramos la versión de distribución que tenemos:

```
[root@ivancito ivancito]# cat /etc/fedora-release
Fedora release 26 (Twenty Six)
```

En nuestro caso tenemos un fedora en la versión 26.

Para obtener la información de la tabla como hemos estado usando hasta ahora:

sestatus

```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      30
```

Si queremos obtener más información como hemos visto en la documentación podemos usar el comando seinfo:

```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:            30 (MLS enabled)
Target Policy:             selinux
Handle unknown classes:    allow
  Classes:            94    Permissions:       441
  Sensitivities:       1    Categories:       1024
  Types:            4816    Attributes:        272
  Users:               9    Roles:              14
  Booleans:          312    Cond. Expr.:       358
  Allow:          102814    Neverallow:          0
  Auditallow:        155    Dontaudit:        8916
  Type_trans:      69725    Type_change:        74
  Type_member:        35    Range_trans:      5753
  Role allow:         39    Role_trans:        420
  Constraints:        38    Validatetrans:       0
  MLS Constrain:      71    MLS Val. Tran:       0
  Permissives:        19    Polcap:              2
```

```
Defaults:            7    Typebounds:          0
Allowxperm:          0    Neverallowxperm:     0
Auditallowxperm:     0    Dontauditxperm:      0
Initial SIDs:       27    Fs_use:             30
Genfscon:          107    Portcon:           607
Netifcon:            0    Nodecon:             0
```

También con la opción siguiente podemos expandir los detalles adicionales del componente, y podemos ver que dominios son unconfined con el siguiente comando como nos indican en la documentación de GENTOO :

```
seinfo -aunconfined_domain_type -x
```

```
Type Attributes: 1
  attribute unconfined_domain_type;
       abrt_handle_event_t
       anaconda_t
       authconfig_t
       bacula_unconfined_script_t
       boinc_project_t
       bootloader_t
       certmonger_unconfined_t
       cinder_api_t
       cinder_backup_t
       cinder_scheduler_t
       cinder_volume_t
       cloud_init_t
       cluster_t
       clvmd_t
       condor_startd_t
       conman_unconfined_script_t
       crond_t
       depmod_t
       devicekit_disk_t
       devicekit_power_t
       devicekit_t
       dirsrvadmin_unconfined_script_t
       firstboot_t
       fsadm_t
       fwupd_t
       httpd_unconfined_script_t
       inetd_child_t
       inetd_t
       initrc_t
       insmod_t
       install_t
       kdumpctl_t
       keepalived_unconfined_script_t
       kernel_t
       livecd_t
       lvm_t
       mount_t
       nagios_eventhandler_plugin_t
       nagios_unconfined_plugin_t
       openshift_initrc_t
       openvpn_unconfined_script_t
```

```
        openwsman_t
        pegasus_openlmi_logicalfile_t
        pegasus_openlmi_unconfined_t
        pki_tomcat_script_t
        prelink_t
        preupgrade_t
        puppetagent_t
        realmd_consolehelper_t
        realmd_t
        rolekit_t
        rpm_script_t
        rpm_t
        rtas_errd_t
        samba_unconfined_net_t
        samba_unconfined_script_t
        semanage_t
        setfiles_mac_t
        sge_job_t
        sge_shepherd_t
        sosreport_t
        system_cronjob_t
        systemd_coredump_t
        tomcat_t
        tuned_t
        udev_t
        unconfined_cronjob_t
        unconfined_dbusd_t
        unconfined_mount_t
        unconfined_munin_plugin_t
        unconfined_sendmail_t
        unconfined_service_t
        unconfined_t
        virt_qemu_ga_unconfined_t
        virtd_lxc_t
        virtd_t
        vmtools_helper_t
        vmtools_t
        vmware_host_t
        watchdog_unconfined_t
        wine_t
        xdm_unconfined_t
        xserver_t
        zabbix_script_t
```

```
seinfo -aubac_contrained_type -x

Type Attributes: 0
```

Distribució	Fedora 26
Policy Store Name	Targeted
MLS?	Enabled
Deny_unknown	Allowed
Unconfined domains?	Sí
UBAC?	No

Bibliografía

https://linux.die.net/man/8/semanage

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/chap-security-enhanced_linux-selinux_contexts

https://docs-old.fedoraproject.org/en-US/Fedora/11/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Working_with_SELinux-Enabling_and_Disabling_SELinux.html

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-working_with_selinux-changing_selinux_modes

https://wiki.gentoo.org/wiki/SELinux/Unconfined_domains

https://wiki.gentoo.org/wiki/SELinux/User-based_access_control