SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2017-18

Práctica [1]. Administración de la seguridad en Linux

Sesión [1]. Seguridad básica en Linux: privilegios de usuario y permisos

Autor[1]: Rubén Calvo Villazán

Ejercicio 1.

Formato de los archivos:

/etc/passwd:

login : contraseña (x) : UID : GID : usuario : directorio de trabajo : terminal asociada

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

...

/etc/group:

nombre del grupo : contraseña (x) : GID : miembros

root:x:0:

daemon:x:1:

bin:x:2:

sys:x:3:

adm:x:4:

---

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 ..."

/etc/shadow:

nombre del usuario : contraseña cifrada : 1* : 2* : 3* : 4* : 5* : 6*

1: Dias transcurridos desde 1970 donde la contraseña fue cambiada por ultima vez

2: Número mínimo de dias entre cambios de contraseña

3: Días máximos de validez de la cuenta

4: Días que avisa antes de caducar la contraseña

5: Días después de que la contraseña caduque para deshabilitar la cuenta

6: Fecha de caducidad

daemon:*:17272:0:99999:7:::

bin:*:17272:0:99999:7:::

sys:*:17272:0:99999:7:::

/etc/gshadow:

nombre del grupo : contraseña (*), (! bloquea el comando `newgrp`) : administradores : miembros

root:*::

daemon:*::

bin:*::

sys:*::

adm:*::

tty:*::

Ejercicio 2.

Cambiar LOGIN_TIMEOUT:

```
#
# Max time in seconds for login
#
LOGIN_TIMEOUT                60
```

```
$ useradd -m usuario
```

Ejercicio 3.

Si tenemos ACL activado en el sistema de archivos

setacl -m u:usuario:rw archivo

Ejercicio 4.

Archivos de configuración pam:

`/etc/pam.d/su` - Permite al usuario si es root hacer sudo sin necesidad de contraseña

auth sufficient pam_rootok.so

`/etc/pam.d/login` – Configuracion para el servicio shadow de login

Establece los limites de la sesion de acuerdo con /etc/security/limits.conf:

session required pam_limits.so

Crea una nueva sesión:

session optional pam_keyinit.so force revoke

`/etc/pam.d/cron` - Configuracion del servicio para el demonio cron

Ejercicio 5.

En `/etc/pam.d/common-password`

```
password required pam_cracklib.so retry=3 minlen=8 difok=3
password required pam_unix.so md5 use_authtok
```

Longitud minima de 8, número mínimo de caracteres que debe ser diferente 3

Ejercicio 6.

```
Oct 15 12:41:52 UBUNTU passwd[25160]: (pam_unix) password changed for root
Oct 15 12:41:52 UBUNTU passwd[25160]: (pam_unix) Password for root was changed
```

Ejercicio 7.

usuario ALL=(ALL:ALL) ALL

Ejercicio 8.

Oct 15 18:33:39 UBUNTU systemd[1]: Started Network Manager Script Dispatcher Service.

Oct 15 18:33:39 UBUNTU nm-dispatcher: req:1 'dhcp4-change' [eth0]: new request (2 scripts)

Oct 15 18:33:39 UBUNTU nm-dispatcher: req:1 'dhcp4-change' [eth0]: start running ordered scripts...

Oct 15 18:33:39 UBUNTU dhclient[12921]: bound to 192.168.1.35 -- renewal in 20426 seconds.

Oct 15 18:35:01 UBUNTU CRON[13103]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)

Ejercicio 9.

$ last

reboot system boot 4.9.0-ubuntu-amd6 Mon Jul 10 10:32 - 00:27 (1+13:55)

root tty7 :0 Sun Jul 9 20:16 - down (04:46)

reboot system boot 4.9.0-ubuntu-amd6 Sun Jul 9 22:09 - 01:02 (02:53)

root tty7 :0 Sat Jul 8 12:28 - down (02:44)

reboot system boot 4.9.0-ubuntu-amd6 Sat Jul 8 14:26 - 15:13 (00:46)

$ lastlog

Username Port From Latest

root tty5 Fri Jun 30 12:45:07 +0200 2017

daemon **Never logged in**

bin **Never logged in**