Álvaro Almellones Fernández

PRACTICA Nº 17-C, ARRANQUE DEL SISTEMA OPERATIVO.

Ejercicio de enunciado y resolución abierto teniendo en cuenta el criterio de evaluación 6.b.

Yo he supuesto que el objetivo es securizar una máquina donde se ha instalado un SO por primera vez

```
almellonesfernandez@Ubuntu-server-arranquesistema ~$ sudo apt update && sudo apt upgrade
[sudo] password for almellonesfernandez:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
127 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  python3-boto3 python3-botocore python3-dateutil python3-jmespath python3-packaging python3-s3transfer
The following upgrades have been deferred due to phasing:
```

Lo primero que he hecho es actualizar todos los paquetes a los más nuevos

```
almellonesfernandez@Ubuntu-server-arranquesistema ~$ sudo apt autoremove && sudo apt clean
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
almellonesfernandez@Ubuntu-server-arranquesistema:~$
```

Lo siguiente que he realizado es eliminar paquetes antiguos y que no se usen

Álvaro Almellones Fernández

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo awk -F: '$3 >= 1000 { print $1 }' /etc/passwd
nobody
almellonesfernandez
usuarioprescindible
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo deluser usuarioprescindible
info: Removing crontab ...
info: Removing user `usuarioprescindible' ...
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo awk -F: '$3 >= 1000 { print $1 }' /etc/passwd
nobody
almellonesfernandez
almellonesfernandez@Ubuntu-server-arranquesistema:~$
```

En el caso de que tengamos usuarios que no sean necesarios en el SO se eliminan dejando solo los usuarios necesarios

```
  GNU nano 7.2                                  /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3 minlen=12 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
```

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo adduser pruebapasswordrobusta
info: Adding user `pruebapasswordrobusta' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `pruebapasswordrobusta' (1001) ...
info: Adding new user `pruebapasswordrobusta' (1001) with group `pruebapasswordrobusta (1001)' ...
info: Creating home directory `/home/pruebapasswordrobusta' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password contains less than 1 digits
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password is shorter than 12 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password contains less than 1 uppercase letters
Retype new password:
Sorry, passwords do not match.
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
Try again? [y/N]
```

Álvaro Almellones Fernández

Lo siguiente que he hecho es realizar modificaciones en common-password para que se pidan contraseñas más robustas a la hora de crear usuarios

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-05-23 17:37:08 UTC; 47s ago
       Docs: man:fail2ban(1)
   Main PID: 1933 (fail2ban-server)
      Tasks: 5 (limit: 3433)
     Memory: 22.3M (peak: 22.8M)
        CPU: 266ms
     CGroup: /system.slice/fail2ban.service
             └─1933 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

May 23 17:37:08 Ubuntu-server-arranquesistema systemd[1]: Started fail2ban.service - Fail2Ban Service.
May 23 17:37:08 Ubuntu-server-arranquesistema fail2ban-server[1933]: 2025-05-23 17:37:08,611 fail2ban.configreader   [1933]: WARNIN>
May 23 17:37:08 Ubuntu-server-arranquesistema fail2ban-server[1933]: Server ready
lines 1-14/14 (END)
```

Otra cosa que he activado es el servicio fail2ban para banear las IP que intentan constantemente conexión con mi ubuntu server

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ufw status verbose
Status: inactive
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)

almellonesfernandez@Ubuntu-server-arranquesistema:~$
```

Lo siguiente que he hecho es configurar cortafuegos para bloquear el tráfico entrante y he dejado el puerto 22 activado para poder acceder por ssh

Álvaro Almellones Fernández

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo systemctl status auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-05-23 18:01:46 UTC; 37s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
   Main PID: 2747 (auditd)
      Tasks: 2 (limit: 3433)
     Memory: 480.0K (peak: 2.1M)
        CPU: 42ms
     CGroup: /system.slice/auditd.service
             └─2747 /sbin/auditd

May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: enabled 1
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: failure 1
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: pid 2747
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: rate_limit 0
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: backlog_limit 8192
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: lost 0
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: backlog 4
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: backlog_wait_time 60000
May 23 18:01:46 Ubuntu-server-arranquesistema augenrules[2761]: backlog_wait_time_actual 0
May 23 18:01:46 Ubuntu-server-arranquesistema systemd[1]: Started auditd.service - Security Auditing Service.
almellonesfernandez@Ubuntu-server-arranquesistema:~$
```

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo cat /etc/audit/rules.d/audit.rules
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

# Registrar cambios en /etc/passwd
-w /etc/passwd -p wa -k passwd_changes

# Registrar cambios en /etc/shadow
-w /etc/shadow -p wa -k shadow_changes

# Registrar cambios en /etc/group
-w /etc/group -p wa -k group_changes

# Registrar intentos de cambios en los módulos del kernel
-w /sbin/insmod -p x -k modules

# Registrar eventos de inicio de sesión
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
almellonesfernandez@Ubuntu-server-arranquesistema:~$
```

Álvaro Almellones Fernández

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ausearch -k passwd_changes
----
time->Fri May 23 18:04:23 2025
type=PROCTITLE msg=audit(1748023463.762:253): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C
6573
type=SYSCALL msg=audit(1748023463.762:253): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7fff7ef3fb20 a2=43c a3=0 items=0
ppid=3024 pid=3038 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl"
 exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1748023463.762:253): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="passwd_changes" li
st=4 res=1
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo ausearch -k shadow_changes
----
time->Fri May 23 18:04:23 2025
type=PROCTITLE msg=audit(1748023463.762:254): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C
6573
type=PATH msg=audit(1748023463.762:254): item=0 name="/etc/" inode=1441793 dev=08:02 mode=040755 ouid=0 ogid=0 rdev=00:00 nametype=P
ARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1748023463.762:254): cwd="/"
type=SOCKADDR msg=audit(1748023463.762:254): saddr=100000000000000000000000
type=SYSCALL msg=audit(1748023463.762:254): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7fff7ef3fb20 a2=43c a3=0 items=1
ppid=3024 pid=3038 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl"
 exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1748023463.762:254): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="shadow_changes" li
st=4 res=1
almellonesfernandez@Ubuntu-server-arranquesistema:~$
```

```
almellonesfernandez@Ubuntu-server-arranquesistema:~$ sudo head /var/log/audit/audit.log
type=DAEMON_START msg=audit(1748023306.690:9444): op=start ver=3.1.2 format=enriched kernel=6.8.0-60-generic auid=4294967295 pid=274
7 uid=0 ses=4294967295 subj=unconfined  res=successAUID="unset" UID="root"
type=CONFIG_CHANGE msg=audit(1748023306.722:125): op=set audit_backlog_limit=8192 old=64 auid=4294967295 ses=4294967295 subj=unconfi
ned res=1AUID="unset"
type=SYSCALL msg=audit(1748023306.722:125): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffd575ba600 a2=3c a3=0 items=0 ppi
d=2751 pid=2761 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" ex
e="/usr/sbin/auditctl" subj=unconfined key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="roo
t" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1748023306.722:125): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C
6573
type=CONFIG_CHANGE msg=audit(1748023306.722:126): op=set audit_failure=1 old=1 auid=4294967295 ses=4294967295 subj=unconfined res=1A
UID="unset"
type=SYSCALL msg=audit(1748023306.722:126): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffd575ba600 a2=3c a3=0 items=0 ppi
d=2751 pid=2761 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" ex
e="/usr/sbin/auditctl" subj=unconfined key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="roo
t" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1748023306.722:126): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C
6573
type=CONFIG_CHANGE msg=audit(1748023306.722:127): op=set audit_backlog_wait_time=60000 old=60000 auid=4294967295 ses=4294967295 subj
=unconfined res=1AUID="unset"
type=SYSCALL msg=audit(1748023306.722:127): arch=c000003e syscall=44 success=yes exit=60 a0=3 a1=7ffd575ba600 a2=3c a3=0 items=0 ppi
d=2751 pid=2761 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" ex
e="/usr/sbin/auditctl" subj=unconfined key=(null)ARCH=x86_64 SYSCALL=sendto AUID="unset" UID="root" GID="root" EUID="root" SUID="roo
t" FSUID="root" EGID="root" SGID="root" FSGID="root"
type=PROCTITLE msg=audit(1748023306.722:127): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756469742E72756C
6573
almellonesfernandez@Ubuntu-server-arranquesistema:~$
```

Lo siguiente que he realizado es activar el servicio de auditoría que nos ayuda a registrar eventos de seguridad, le he añadido un par de reglas de seguridad básicas y he comprobado que se generen log de auditorías

```
almellonesfernandez@Ubuntu-server-arranquesistema ~$ sudo aa-status
apparmor module is loaded.
```

He comprobado que apparmor está activo para securizar un poco el kernel ya que el kernel consulta a AppArmor antes de permitir cualquier acción bloqueando las que no estén autorizadas.

Álvaro Almellones Fernández

Otra cosa que se puede realizar es cifrar el disco que en la práctica siguiente se mostrará cómo cifrarlo

CRITERIOS DE EVALUACIÓN	
6.b	Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad