

Cognoms:

Nom:

DNI:

## ADMINISTRACIÓ DE SISTEMES OPERATIUS

3er Parcial, 14 de Gener de 2020

L'examen és individual

Responen en l'espai assignat

Poseu COGNOMS, NOM (per aquest ordre)

L'examen és sense llibres ni apunts

Es pot utilitzar calculadora

**És obligatori justificar totes les respostes**

Temps: 2 hores (No es pot sortir abans de mitja hora)

### **Pregunta 1 – Xarxes i Seguretat (3 Punts)**

1. Què fa que FTP sigui un protocol insegur en general? Indica'n 2 motius com a mínim. **Justifica la resposta. (0.5 Punt)**

FTP es un protocol insegur degut a que el control d'accés es controla a nivell usuari, descartant aquells usuaris que no volem que entrin:

-Per defecte no va xifrat

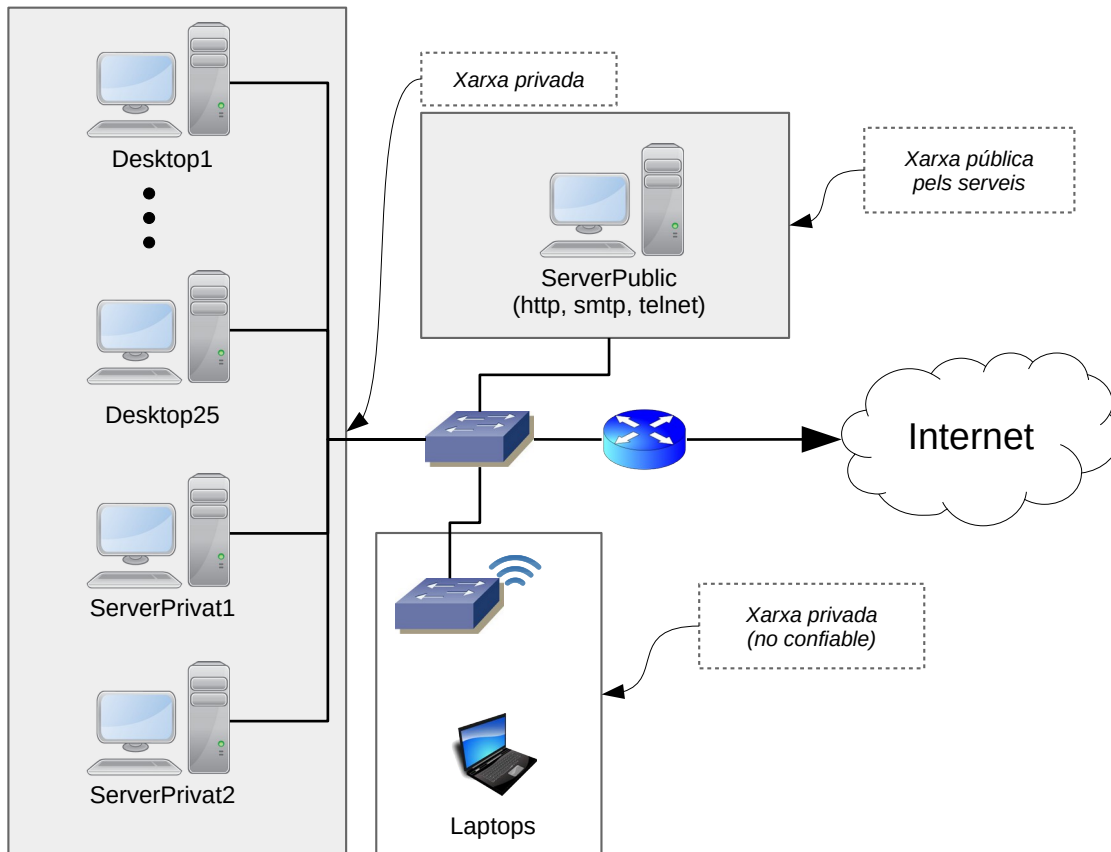
-S'executaba com a root per defecte

2. Quina és la funcionalitat d'un firewall. Indica què fan i a quin nivell treballen en general. **(0.5 Punts)**

Un firewall, es una eina, la cual ens permet filtrar els diferents tipus de trafics cap a determinats punts d'una red. Un firewall no pot controlar el que hi ha dins del paquet de informació, per tant no es una eina perfecta. Aquest firewall treballa a nivell 3, controlant els paquets IP.

3. Donada la xarxa de la següent figura, indica on posaries el (o els) firewall. Justifica el motiu del posicionament i la configuració que tindrien – només cal que indiquis quins filtres posaries.

**(0.5 Punts)**



Fisicament el posaria en el router d'accés a internet, pero logicament, es trobaria situat en cada una de les interfícies del switch, cap a cada una de les subreds, per tal de protegir la xarxa privada i la DMZ i la red wifi.

4. Dels serveis oferts a la pregunta anterior (http, smtp, telnet) indica quines alternatives segures en faries servir per tenir un sistema més segur.

**(0.5 Punts)**

HTTP --> HTTPS

SMTP --> No té alternativa

Telnet --> SSH

5. Quin problema pot tenir el posar el directori . Al PATH del sistema en UNIX:

**(0.5 Punts)**

Un atacant maliciós podria descarregar un binari maliciós al "." anomenat cp o mv o ls... al executar aquesta comanda, estaries executant el codi maliciós, degut a que es troba al ".", per tant hi ha que evitar-lo.

6. Descriu quins problemes de seguretat, i com mitigar-los té el protocol DHCP. **Justifica la resposta.**

**(0.5 Punts)**

El problema és que es dona IP a tothom en connexió, com a molt pots fer control per MAC, però qualsevol es pot canviar la mac, per tant el administrador ha de controlar això.

## Pregunta 2 – Usuaris i permisos (2 punts)

Donada la següent situació inicial d'un directori dins del nostre sistema de fitxers:

```
rserral@asoserver:/shared$ ls -Rla
.:
total 18
dr-xrwxr-x  4 rserral profe  4096 Oct 11 10:59 .
drwxr-xr-x 12 root    root   4096 Oct 11 10:59 ..
drwxrwsrwt  2 rserral profe  4096 Oct 11 11:18 d1
```

```
./d1:
total 8
drwxrwsr-t 2 rserral profe  4096 Oct 11 11:18 .
dr-xrwxr-x 4 rserral profe  4096 Oct 11 10:59 ..
-rwx--x--- 1 root    rserral   6 Oct 11 11:19 f2
-rw-r--r-- 1 profe   rserral 3451 Oct 11 11:00 f1
```

**Nota:** Per defecte un usuari només pertany al grup que té el mateix nom que ell.

**Nota2:** Assumeix que cada pregunta és independent, o sigui que l'efecte de les comandes **NO** es propaga a les altres preguntes.

Respon JUSTIFICANT cada resposta a les següents preguntes.

1. Indica l'efecte d'executar la següent comanda:

```
student@asoserver:/shared$ rm -rf d1
```

(0.25 Punts)

No té cap efecte per l'sticky bit.

2. Quin és l'efecte d'executar:

(0.25 Punts)

```
profe@asoserver:/shared$ echo Testing >> d1/f3
```

Com té permisos de escriptura, es crearia un nou archiu.

3. Indica què fan les següents comandes i fitxers de configuració:

(0.5 Punts)

**passwd:** **Cambiar la contraseña**      **/etc/aliases:** **Cambiar el correu electronic**

**chmod:** **Cambiar els permisos d'un fitxer o carpeta**      **/etc/shadow:** **Veure els usuaris, el hash de contrasenyes i el temps d'expiració**

4. Descriu què és i què fa la crida a sistema `setuid`:

**(0.5 Punts)**

Es la crida a sistema encarregada d'assignar el UID de l'usuari durant el procés de login en el sistema.

5. Volem donar a l'usuari `aso` permís per poder utilitzar la comanda `mkfs` al disc `/dev/sda`, però que no tingui privilegis sobre el `/dev/sdb`. Indica què faries per aconseguir-ho: **(0.5 Punts)**

**Nota:** No pots utilitzar ni `su` ni `sudo` per fer-ho.

Amb `chmod` o `chown`

### Pregunta 3 – Monitorització (1.5 punts)

1. Quin efecte té en un sistema quan el %sy és molt alt?

(0.5 Punt)

Provoca que l'usuari té menys recursos per consumir del ordinador, per tant trigarà més temps en poder realitzar les tasques.

2. Tenim un sistema amb un total de 4 cores i veiem la següent sortida de la comanda uptime en dos moments de temps diferents:

16:03:02 up 43 days, 3 users, load average: 5.40, 7.31, 10.51

17:05:21 up 43 days, 5 users, load average: 6.40, 2.41, 2.64

(0.5 Punts)

Indica si consideres que el sistema està correctament dimensionat. **Justifica la resposta.**

En ambos casos no es troba ben dimensionat, degut a que es troba gastant més CPUs que les que té el ordinador en el últim minut, si que es veritat que en el primer cas, la tendencia es a la baixa, però en el segon cas, la tendencia es a la alça, lo que provocaria que el sistema arribi a un punt que no pugui donar abast a tants de processos.

3. Indica una eina i les seves principals característiques per la monitorització dels següents aspectes del sistema.

(0.5 Punts)

Usuaris: W

Xarxa: Tcpdump

Disc: Vmstat

Memòria: Vmstat

#### Pregunta 4 – Backups (1.5 Punts)

1. Quines restriccions en general té fer un backup d'una base de dades com per exemple MySQL? (0.5 Punt)

Que no es pot fer un backup incremental d'una base de dades, degut a que pot portar a inconsistències en les dades que almacena, per tant realitzar una còpia de seguretat de una BBDD sempre ocupara més memòria, degut a que no es poden fer incrementals.

2. Volem fer una política de backup per una empresa amb les següents condicions: (1 Punt)

L'empresa vol realitzar backups de 10 servidors d'usuaris connectats a la xarxa. **Cada** servidor té unes característiques similars, cada un té:

- 50GB plens amb homes d'usuari, que canvien un 2% al dia. La taxa de compressió mitja de 0.1%.
- 10GB amb bases de dades de suport als usuaris. Canvien un 1% al dia i la taxa de compressió és del 30%.
- 8GB amb aplicacions d'usuari (/usr/local) compilades. No canvien mai i la taxa de compressió és del 25%.

Defineix la política de backups (tipus de backup, freqüència, si es comprimeix o no, política d'expiració), independentment dels discos (o cintes) de backup sabent que només disposes d'un disc de 1TB i una cinta de 3TB.

10 servidors	50 GB + 2% diari	/home	No comprimir	1inc diari i 1tot mensual (70GB mensual)
	10 GB + 1% diari	BBDD	Si comprimir	1 total cada 2 dies (7GB cada 2 dies)
	8 GB	App	Si comprimir	1 total (6GB)

Treballant 5 dies a la setmana i 4 setmanes al mes;

Cada servidor cada mes gasta 146 GB → 1460 GB mes en total, per tant podria almacenar: 2 mesos

## Pregunta 5 (2 Punts)

Respon les següents preguntes marcant la casella correcta. Hi ha una i només una resposta vàlida per pregunta.

**Cada resposta correcta val 0.5 punts. LES RESPOSTES INCORRECTES RESTEN 0.25 punts. I les no contestades no puntuen.**

1. El sistema `cron`
  - ☐ a) Serveix per executar tasques puntuals a un moment donat
  - ☐ b) Executa tasques periòdiques com a `root`
  - ☒ c) Executa tasques periòdiques com l'usuari que l'ha invocat
2. El cicle de vida d'un equip indica:
  - ☐ a) Què fer per tenir l'equip correctament configurat
  - ☒ b) Els estats pels que passa un equip des que es compra fins que es retira
  - ☐ c) El procediment per poder reciclar un equip
3. Volem reduir la prioritat del procés `gcc` amb PID 1345, sabem que actualment té 0:
  - ☒ a) `$ renice -n 5 1345`
  - ☐ b) `$ renice -n 5 gcc`
  - ☐ c) `$ renice -n -5 1345`
4. Compilem software basat amb autotools executant (indica la més correcta):
  - ☐ a) `user $ sudo ./configure --prefix=/usr/local; sudo make; sudo make install`
  - ☒ b) `user $ ./configure --prefix=/usr/local && make; sudo make install`
  - ☐ c) `user $ ./configure --prefix=/usr/local/[app_name]* && make && make install`

\* On `app_name` és el nom de l'aplicació que estem instal·lant