

Nom:

DNI:

ADMINISTRACIÓ DE SISTEMES OPERATIUS – Grau en Informàtica
Control 3, 16 de Desembre de 2021

L'examen és individual, es mirarà si hi ha hagut còpies, si se'n detecta alguna es prendran les mesures adients

L'examen és sense llibres ni apunts. Com això no ho podem controlar, si es detecta copy paste també es prendran mesures al respecte

Indiqueu els vostres COGNOMS, NOM i DNI (per aquest ordre), a dalt d'aquest full

És obligatori justificar totes les respostes

Temps: 1 hora i 55 minuts (No hi haurà extensions de temps)

Pregunta 1 – Aplicacions, Monitorització (2.5 punts)

1. Volem instal·lar l'aplicació «John the Ripper» al directori /usr/local/john utilitzant el codi font. Sabem que utilitza autotools per compilar-se, indica quin usuari i quina comanda hauríem d'executar per poder compilar i instal·lar l'aplicació. **(0.5 Punts)**

2. Resulta que volem executar l'aplicació de la pregunta anterior per tal de verificar quins passwords dèbils té el sistema. Com sabem que fer aquest anàlisis requereix molts recursos decidim programar una tasca al sistema per a que s'executi cada divendres a les 10 de la nit exceptuant els divendres d'Agost. Indica quina eina utilitzaries i com la configuraries per executar aquesta comanda:

`john -c /etc/john.conf`

(0.5 Punts)

3. Un dia, ens demanen validar la robustesa dels passwords del sistema de forma urgent per què creiem que hi ha algun usuari que no té un password segur. Com a administradors sabem que fer aquesta acció requereix molts recursos de CPU, com ho podríem fer per iniciar la execució quan abans millor amb baixa prioritat? **(0.25 Punts)**

4. Hem vist que el servidor va molt lent, fem un top i veiem la següent sortida:

```
top - 15:14:24 up 1 day,  1:03,  1 user,  load average: 13.72, 9.82, 5.21
Tasks: 297 total, 14 running, 282 sleeping, 0 stopped, 1 zombie
%Cpu(s):  4.5 us, 5.5 sy, 0.0 ni, 0.0 id, 90.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem:  8099488 total, 7874304 used,  225184 free, 3038912 buff/cache
KiB Swap: 7821308 total,    504 used, 7820804 free, 2364628 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
9682	aso2	20	0	191m	157m	4992	R	2.0	2.0	0:02.36	firefox
9688	aso2	20	0	189m	155m	6568	R	1.6	0.4	0:02.44	find / - name
9661	aso2	20	0	193m	160m	6476	R	1.0	2.0	0:02.44	firefox
9678	aso2	20	0	198m	164m	6624	R	0.5	2.1	0:02.68	firefox

Quina causa creus que pot causar el problema?

(0.5 Punts)

5. Hem notat que un usuari ha configurat una tasca periòdica cada minut que afecta al rendiment del sistema com hem vist a la pregunta anterior, com l'usuari no vol treure la tasca hem pensat en deshabilitar-li el servei de temporització, com ho podríem fer? **(0.25 Punts)**

6. Un usuari ens pregunta com ho pot fer per executar per defecte la versió 2 de python, quan el vostre sistema per defecte utilitza la versió 3. Sabem que el 2 està instal·lat a `/usr/local/python2` i la 3 a `/usr/local/python3`. **(0.25 Punts)**

Pregunta 2 – Permisos i Backups (2.5 Punts)

1. Què fa el bit de SetUID en fitxers?

(0.25 Punts)

2. Indica el propòsit i com funciona l'umask

(0.25 Punts)

3. Quines particularitats cal tenir en compte per fer backups d'una base de dades?

(0.25 Punts)

4. Descriu detalladament el funcionament de muntar un sistema de fitxers en un sistema UNIX.

(0.5 Punts)

5. Quin impacte té l'sticky bit en fitxers?

(0.25 Punts)

6. Indica diferències i similituds entre els backup incrementals i els incrementals inversos. **(0.5 Punts)**

(0.5 Punts)

7. Què fa el permís d'execució en directoris?

(0.5 Punts)

Pregunta 3 – Test (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.

1. El protocol DHCP:
 - ☐ a) S'utilitza principalment per la transferència de fitxers
 - ☐ b) És un protocol amb estat
 - ☐ c) És un protocol orientat a connexió
2. En la configuració d'un firewall cal tenir en compte?:
 - ☐ a) Que un firewall és sempre un equip centralitzat amb una vista única
 - ☐ b) Que com és la peça més important en quant a seguretat podem relaxar altres aspectes
 - ☐ c) Que tot i poder estar centralitzat ens convé tenir en compte les particularitats de cada segment de xarxa
3. Què volem dir quan parlem de SaaS?
 - ☐ a) És un servei de software que redueix costos per a grans empreses
 - ☐ b) Aplicacions al núvol que absteuen els detalls de gestió de les aplicacions a través d'una API i de cops una interfície d'usuari basada amb Web
 - ☐ c) Significa Software as a System, són aplicacions al núvol que donen l'accés al sistema

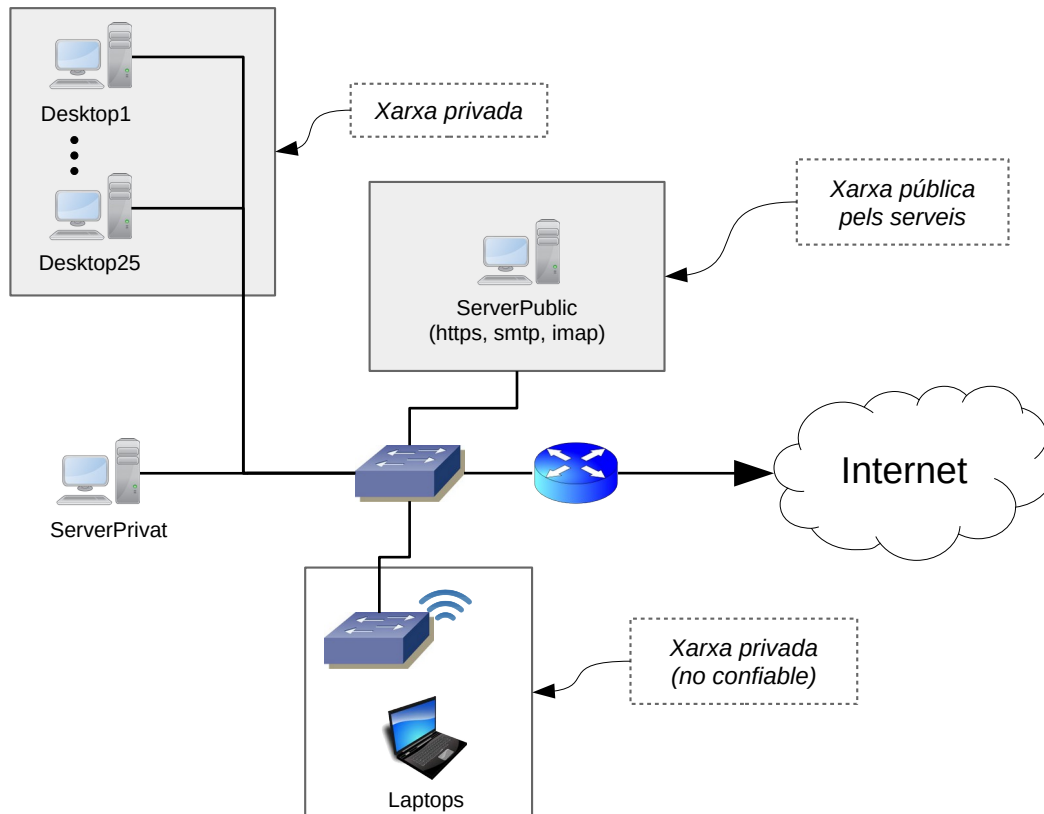
4. Donada la següent situació inicial d'un directori dins del nostre sistema de fitxers indica la resposta vàlida més avall:

```
rserral@asoserver:/shared$ ls -Rla
.:
total 18
drwxrwxr-x  4 rserral profe  4096 Oct 11 10:59 .
drwxr-xr-x 12 root      root   4096 Oct 11 10:59 ..
drwxrwsr-x  2 profe    aso     4096 Oct 11 11:18 d2
./d2:
total 7
drwxrwsr-x 2 profe    aso     4096 Oct 11 11:18 .
drwxrwxr-x 4 rserral profe  4096 Oct 11 10:59 ..
-r--rwxr-- 1 rserral profe      6 Oct 11 11:19 file
rserral@asoserver:/shared$ umask
027
```

- ☐ a) Executar `aso:/shared$ mv d2/file /shared/new_file` funciona perfectament
- ☐ b) Un fitxer creat així: `root:/shared$ touch d2/nou_fitxer` tindria de grup propietari aso
- ☐ c) **No** es podria executar satisfactòriament la comanda: `aso:/shared$ cat d2/file`

Pregunta 4 – Xarxes i Seguretat (3 punts)

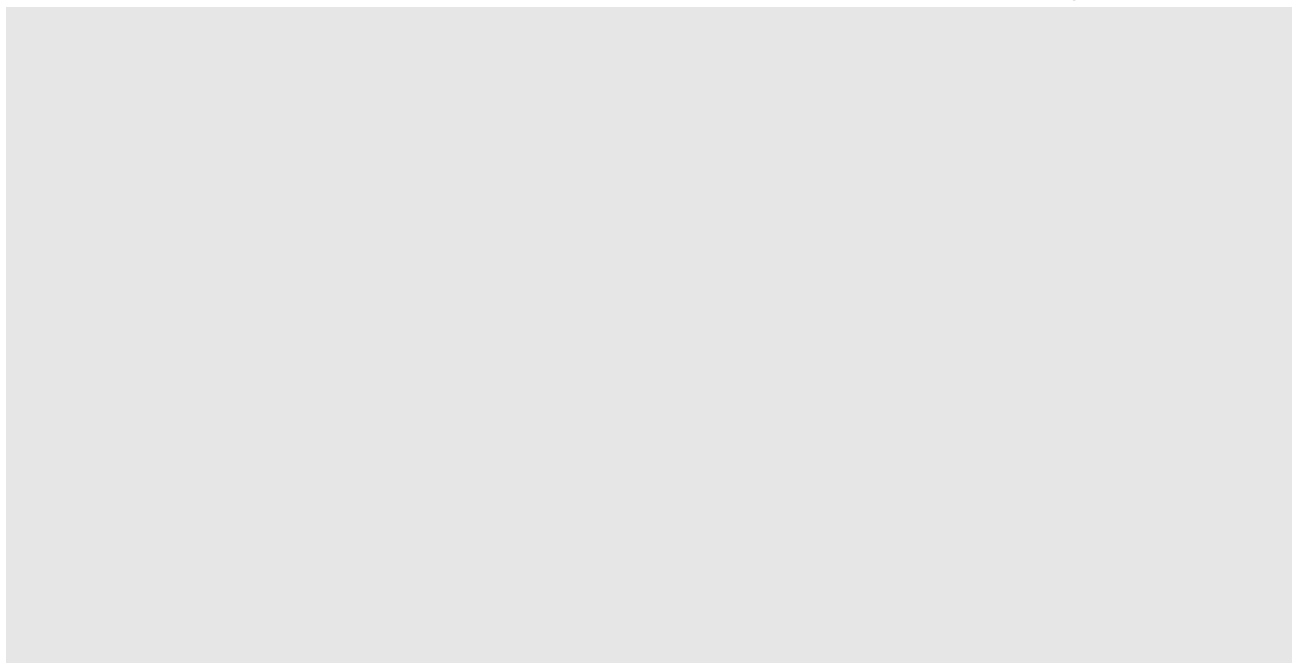
Una empresa té la xarxa que es mostra en la següent figura:



Se'ns diu que l'empresa té 25 empleats amb equips de sobretaula, mentre que disposa d'una xarxa WiFi (no fiable!!) per als treballadors que venen esporàdicament.

D'altra banda, l'empresa té dos servidors privats (a la figura només n'hi ha un) per oferir serveis interns, que per seguretat volem separar de la xarxa dels empleats, i un de públic per serveis com per exemple el Mail i la pàgina web.

1. Assigna adreces IP i divideix la xarxa com et sembli que hauria de distribuir-se, indica si s'escau la divisió amb VLAN. Si vols pots resoldre l'exercici directament a la figura. **(0.5 Punts)**



2. Volem instal·lar els següents serveis: Impressió, SSH, LDAP, Web, NFS, DNS. Indica a quin dels tres servidors (2 privats i un públic) instal·laries els serveis i quines consideracions de seguretat hauries de tenir per garantir que els serveis funcionen correctament. **Justifica la resposta:**

(0.5 Punts)

3. Indica on configuraries el firewall i quins criteris de protecció hauria de permetre donat l'esquema de xarxa de la figura. **(0.5 Punts)**

4. Quins problemes de seguretat té el protocol telnet?. Indica també per quin altre servei el substituiries en cas de necessitar-lo. **(0.5 Punts)**

5. Indica com ho fa el sistema per poder utilitzar el servidor web com a usuari normal, sabent que per utilitzar el port 80 o el 443 com a servidor són necessaris privilegis de root. **Justifica la resposta.**

(0.5 Punts)

6. Volem compartir fitxers des d'un servidor Linux Debian a un client Windows 10. Indica quin protocol utilitzaries i descriu-ne les principals característiques.

(0.5 Punts)