

COGNOMS: _____

NOM: _____

Full: 1/3

ADMINISTRACIÓ DE SISTEMES OPERATIUS

Examen Final

21 de Juny de 2007

L'examen és individual

Responen en l'espai assignat

Poseu COGNOMS, NOM (per aquest ordre) a tots els fulls

L'examen és sense llibres ni apunts

Les notes sortiran el dia 29 de Juny

La revisió serà el dia 2 de Juliol

Temps estimat: 2 hores

1. (2 punts) Indica si les següents afirmacions són **certes o falses**. En cas de que sigui falsa explica perquè ho és. (Cada resposta incorrecta resta mitja correcta).
 - a) Un bon lloc per guardar els backups del nostre sistema és a una partició separada al mateix disc.
 - b) Al contrari que LPR, LPRng no necessita executar-se com a root ja que no fa cap operació sobre ports privilegiats.
 - c) Podem fer servir signatures digitals per reduir les possibilitats d'instal.lar software maliciós.
 - d) Un problema específic d'instal.lar una aplicació desde codi font és que necessitem instal.lar també totes les seves dependències.
 - e) RPC no és pot utilitzar per implementar serveis que necessitin guardar estat al servidor.

f) El bit SetUID en un directori no té cap efecte.

g) En una xarxa en la que tenim una DMZ mai pot haver-hi un servei a la xarxa privada.

h) A un sistema poden haver-hi un nombre indeterminat de particions primàries.

2. (2 punts) A un sistema que estem monitoritzant obtenim la següent informació amb la comanda top:

```
top - 00:39:54 up 41 days, 14:53, 3 users, load average: 2.49, 0.98, 0.36
Tasks: 66 total, 1 running, 65 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.7%us, 10.3%sy, 0.0%ni, 50.3%id, 37.7%wa, 1.0%hi, 0.0%si, 0.0%st
Mem: 208308k total, 204752k used, 3556k free, 760k buffers
Swap: 979924k total, 616620k used, 363304k free, 1876k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
8818	aduran	17	0	141m	86m	68	S	5.0	42.6	0:02.00	compact
96	root	15	0	0	0	0	S	3.3	0.0	0:29.44	kswapd0
777	xavim	16	0	590m	81m	68	S	2.0	40.2	0:07.74	netscape
877	root	16	0	2328	584	416	R	0.7	0.3	0:01.31	top
1	root	16	0	2032	76	56	S	0.0	0.0	0:05.77	init
2	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/0

a) Quin problema creus que té aquest sistema?

b) Quina creus que és la causa del problema?

c) Qui creus que és el responsable?

d) Quines accions emprendries?

COGNOMS: _____

NOM: _____

Full: 2/3

3. (1 punt) Explica què és un rootkit i com podem detectar la seva presència als nostres sistemes.

4. (2 punts) Serveis de Xarxa

a) Expliqueu la necessitat d'usar el protocol *secure http* (HTTPS), enlloc de l'HTTP, quan transferim per la xarxa informació sensible, com ara números de tarjetes de crèdit.

b) Quin protocol orientat a connexió està implementat sobre la mateixa tecnologia de transferència de dades segura, com l'HTTPS?

c) Explica com es fa que el protocol DHCP sigui tolerant a la caiguda del servidor.

d) Explica el funcionament del servei d'ftp i compara'l amb la transferència de fitxers a través del *secure ftp*.

5. (2 punts) **Com a administrador júnior**, instal·leu una nova màquina en el nostre departament per fer de servidor del Web extern cap a Internet i, a mig instal·lar, just després de connectar-la a la xarxa, fer-la accessible des d'Internet, i sense haver instal·lat encara el servidor de secure shell (ssh), rebem la trucada d'un dels **becaris de la nostra empresa** demanant-nos: “Hola, sóc el Toni, si-us-plau, que ens podries donar accés **al Martí i a mi**, que hem de fer **unes proves** en aquest tipus de màquina? Ens podem connectar **a través de telnet** o rlogin. **Envia'm els passwords per correu electrònic** a mi, que jo ja li donaré el seu al Martí”.

a) Indica quina és la resposta que li dones al Toni.

b) Comenta tots els aspectes (en negreta en el text) de la petició del Toni, indicant si són correctes o incorrectes.

... **al Martí i a mi**...:

... **unes proves**...:

... **a través de telnet**...:

Envia'm els passwords per correu electrònic...:

c) Si al cap de dues hores hem donat un compte provisional al Martí i al Toni per a que es puguin connectar per telnet a la màquina, per fer les proves que ens demanaven, què o qui hi ha intervingut?

d) Si aquest és el cas, quines limitacions s'hauran posat en quan a l'accés a la màquina a través de la xarxa?

COGNOMS: _____

NOM: _____

Full: 3/3

6. (1 punt) Explica el mecanisme d'entrada al sistema, pel qual un usuari s'autentifica en el sistema i obté un intèrpret de comandes, indicant clarament quins processos i fitxers (binaris, de configuració, shell scripts) estan involucrats en cada pas.