



Försättsblad tentamen / Examination cover



2707183

Anonymitetskod / Anonymous code

S - 0 0 0 1 - B X N

Kurskod / Course code

D T 1 4 9 G

Provkod / Test code

T 1 0 5

Tentamensdatum / Examination date

2 0 2 3 - 0 4 - 1 3

Kursnamn / Course name

Datateknik GR (B), Administration av UNIX-lik system

Provnamn / Test name

Skriftlig tentamen

Skriv din anonymitetskod på varje inlämnat papper

Write your anonymous code on each sheet submitted

Sätt ett kryss (x) för varje inlämnad uppgift

Use an x to indicate which questions has been submitted

Markera nedan med X / Mark below with an X	Poäng / Credit	Lärarens anteckningar / Teacher's notes	Markera nedan med X / Mark below with an X	Poäng / Credit	Lärarens anteckningar / Teacher's notes
1	X		16		
2	X		17		
3	X		18		
4	X		19		
5	X		20		
6	X		21		
7	X		22		
8	X		23		
9	X		24		
10	X		25		
11			26		
12			27		
13			28		
14			29		
15			30		
Poängssumma / Points		Betyg / Grade	Lärarsign./ Teachers sign		

Fylls i av tentamensvakt / To be filled in by the invigilator

Antal lösa blad/ No. of sheets submitted	Inlämnad tentamen / Submitted exam	Leg kontroll / Control identification	Sign. tentamensvakt / Sign. invigilator
4	0	✓	

2707183



Försättsbladet skall alltid lämnas in även om ingen uppgift behandlats
Examination cover should always be submitted even if no questions are answered

Utskriven 2023-04-12 kl. 10:28:24

<p>1. One reason is that building your own kernel allows you to choose components you want. You can build a lightweight kernel that's more customized to your needs.</p> <p>Another reason, and arguably the best one, is that building your own kernel allows you to learn how things work on a deeper level. You gain knowledge regarding how everything is set up, and that's the most valuable gain.</p>	<p>Lärarens anteckning / Teachers note:</p> <p>3</p>
<p>2. passwd contain information regarding passwords on the system.</p> <p>groups contain information regarding the groups on the system, the names, the members, ID and such.</p> <p>!!</p>	<p>0,5</p>
<p>3. The user is trying to kill process with ID 1 /sbin/init.</p> <p>Killing that process isn't something you should/can do because it plays a crucial role in booting the system and booting other processes. That's why it has ID 1 because it's the very first process the kernel executes.</p> <p>I don't know why you would ever want to kill /sbin/init? To restart the execution of everything? Perhaps you could try suspending it instead, since I don't think you should kill it. But even that feels like it shouldn't work...</p> <p>I didn't know this was an open book exam !!</p>	<p>2</p>

4. Using an Access Agent without encryption would prove to be a big security risk.

Blen

Lärarens anteckning /
Teachers note:

—

5. Example of reverse zone:

BTTL 30d
BORIGIN 1.168.192.in-addr.arpa.

@ IN SOA nclab.miun.se, mail.nclab.miun.se,
2023041301
3600
1800
604800
3600)

@ IN NS nclab.miun.se.
nclab.miun.se IN A 192.168.1.125

125 IN PTR nclab.miun.se.

Important part

Where a forward zone maps a domain name to its IP address, a reverse zone does the opposite. It allows you to find the name of a domain using the IP address.

The name of the reverse file is also important, since it contains the first three parts of the IP address. Using the PTR resource record, you point at domains that have the given last number, here that's 125.

Attid så?

6. The reason to enable anything in the firewall is to give it access and to stop the firewall from hindering it.

Lärarens anteckning /
Teachers note:

7. The syslog works by receiving messages from anywhere in the system. There are different log files, found in /var/log, and what message ends up where depends on configuration.

The standard syslog contains messages from the whole system. It's a collection of what has happened on the system, with timestamps, ID, MAC address, source IP address, destination, maybe some text explaining what has been done.

Exactly what the message contains depends on the application. Some have very comprehensive messages while others do not.

The good thing is that you have logs containing all kinds of information, which makes it easier to troubleshoot and figure out where something is going wrong.

Downsides can be to find the exact message, where is it, which file? Maybe the application doesn't provide any logging at all. I can imagine there might be a security risk as well perhaps.

3

8. The purpose of `skel`, as the name suggests, is to provide a "skeleton" for when a new user is created. Whatever `skel` contains, the user will get in their files. So if you want every user to have something specific, you add it to `skel`, and it will then be added upon the creation of a new user.

Lärarens anteckning /
Teachers note:

3

9. The purpose of the `ramdisk` is to provide a temporary storage for the boot process until the kernel can mount the actual root file system properly. The `ramdisk` is a part of the Linux booting process and is an important step where the kernel mounts a temporary file system on it before the proper root file system is mounted on the drive.

3

10. To see a process' resource amount, you can use `top` or `pidstat`. Both display the amount of resources it's currently holding. With `top`, you can use the option `-p` to display only one process.

3

In order to suspend a process instead of killing it, you can use:

`kill -STOP PID`

To continue the process, you can use:

`kill -CONT PID`