Networked Services - Week one quiz

> 05/12/2019

Question 1

Given the following:

```
$ chmod 345 test
$ chmod og-w,u=rx test
```

What are the resulting permissions? Show the answer in numeric notation.

Answer 1

> 345 to start

> og-w tries to take away 2 (010) from 4 (100) for group and from 5 (101) for other. But the middle bit is not set anyway so this makes no change. Remains 345.

> u=rx sets the user permission to 5 (101) regardless of what it was previously.

> Answer is 545

Revision 1

There are three permissions:

> -r = Read -w = Write -x = Execute

Three permission levels:

> -u = User -g = Group -o = Other

Permission table

Octal	Binary	Perms	Octal	Binary	Perms
7	111	rwx	3	011	-wx
6	110	rw-	2	010	-w-
5	101	r-x	1	001	--x
4	100	r--	0	000	---

Question 2

Logical Volume management, LVM, offers additional features in comparison to fixed partitioning strategies. Reflect on the challenges of dynamic partitioning strategies when compared to traditional partitions.

Answer 2

> Dynamic partitioning allows partitions and disks to be added to existing partitions at runtime, allowing filesystems to be grown or shrunk. But this is complex and error-prone, and careful partitioning at the start is probably safer and more effective. (LVM does this)

Revision 2

Logical Volume Management (LVM)

If you want to change your partitions after installing, then you are doing something very risky…

- It is possible to destroy every partition by damaging the partition table.
- Often the current partitions use 100% of the disk, so repartitioning to make something bigger means shrinking other partitions.
- Formatted partitions don’t like being shrunk, and need to be compressed and migrated before being shrunk.
- LVM and other tools tries to make this simpler, by adding dynamic run-time controls to partition management.

Question 3

Keeping systems patched and up to date is good practice, but fraught with difficulties. When maintaining a critical server, discuss how such a system can be kept up to date safely.

Answer 3

> Rebooting machine which have been running a while may result in electrical failures. New updates may render currently functioning systems unusable, introduce incompatibilities, or change current behaviours. Keeping backups is valuable, but testing changes on a mirror may be helpful.

Revision 3

Question 4

XINETD follows a different philosophy in comparison to traditional schemes like init.d in the way they handle service daemons. Discuss any negative issues about the approach used by XINETD, i.e. reasons for not wanting to use this approach.

Answer 4

> XINETD may be slower, and more complex, and harder to debug, and has a harder to predict effect on system resources.

Revision 4

Extended Internet Service Deamon (XINETD)

In computer networking, xinetd (Extended Internet Service Daemon) is an open-source super-server daemon, runs on many Unix-like systems and manages Internet-based connectivity. It offers a more secure alternative to the older inetd ("the Internet daemon"), which most modern Linux distributions have deprecated.

Deamons

A daemon (also known as background processes) is a Linux or UNIX program that runs in the background. Almost all daemons have names that end with the letter "d". For example, httpd the daemon that handles the Apache server, or, sshd which handles SSH remote access connections. Linux often start daemons at boot time.

Question 5

Write a 1 line statement, using a pipe, which reports how many directories in /home have a group ownership of “people”. Make sure it checks subdirectories too.

Answer 5

> `find /home -group people -type d | wc -l`

Revision 5

`find`

> Options used highlighted with `...`.

```
Usage: find [-H] [-L] [-P] [-Olevel] [-D debugopts] [path...] [expression]

default path is the current directory; default expression is -print
expression may consist of: operators, options, tests, and actions:
operators (decreasing precedence; -and is implicit where no others are
given):
      ( EXPR ) ! EXPR -not EXPR EXPR1 -a EXPR2 EXPR1 -and EXPR2
      EXPR1 -o EXPR2 EXPR1 -or EXPR2 EXPR1 , EXPR2
positional options (always true): -daystart -follow -regextype

normal options (always true, specified before other expressions):
      -depth --help -maxdepth LEVELS -mindepth LEVELS -mount -noleaf
      --version -xdev -ignore_readdir_race -noignore_readdir_race
tests (N can be +N or -N or N): -amin N -anewer FILE -atime N -cmin N
      -cnewer FILE -ctime N -empty -false -fstype TYPE -gid N `-group` NAME
      -ilname PATTERN -iname PATTERN -inum N -iwholename PATTERN -iregex
PATTERN
      -links N -lname PATTERN -mmin N -mtime N -name PATTERN -newer FILE
      -nouser -nogroup -path PATTERN -perm [-/]MODE -regex PATTERN
      -readable -writable -executable
      -wholename PATTERN -size N[bcwkMG] -true `-type` [bcdpflsD] -uid N
      -used N -user NAME -xtype [bcdpfls]      -context CONTEXT

actions: -delete -print0 -printf FORMAT -fprintf FILE FORMAT -print
      -fprint0 FILE -fprint FILE -ls -fls FILE -prune -quit
      -exec COMMAND ; -exec COMMAND {} + -ok COMMAND ;
      -execdir COMMAND ; -execdir COMMAND {} + -okdir COMMAND ;

Valid arguments for -D:
exec, help, opt, rates, search, stat, time, tree
Use '-D help' for a description of the options, or see find(1)
```

Question 6

Given that all the passwords in Linux are hashed, speculate on why it was felt important to move the hashed passwords from /etc/passwd into /etc/shadow. As part of your answer, comment on the need to regularly change the hashing algorithm used in password hashing.

Answer 6

> /etc/passwd is readable by everyone, so that UID and GID can be translated into names, and so everyone has access to hashed passwords. This was considered dangerous, and hashes were moved to shadow. Through hacking techniques it may still be possible to get the hashes, so making hashes difficult to break is important. Thus the reason for updating the hashing technique with changes to current security thinking.