Veridic Solutions, NC, USA

Mentors: Nihar and Sandeep

Name: Vamsi Krishna Edala

Linux 2 QUIZ Answers

1. What command would list all files (except . and ..) in the current working directory?

Answer:

Linux Command: $ ls (List is used to display all the files and directories in the working directory).

```
vamsi@vamsi-VirtualBox:~$ ls
Desktop           file2   krishna     Public     vk
Documents         head    Music       team
Downloads         hello   Pictures    Templates
examples.desktop  hello1  promotions  Videos
vamsi@vamsi-VirtualBox:~$
```

2. What is the simplest command for adding execute permission to file ~/foo, for all users

(without changing any other permission)

Answer: **$** chmod a+x foo.txt

```
vamsi@vamsi-VirtualBox:~$ cat foo.txt
Hello Foo File
vamsi@vamsi-VirtualBox:~$ chmod a+x foo.txt
vamsi@vamsi-VirtualBox:~$ ls -al
total 152
drwxr-xr-x 20 vamsi vamsi  4096 Jun 21 09:33 .
drwxr-xr-x  6 root  root   4096 Jun 11 11:49 ..
-rw-------  1 vamsi vamsi  5637 Jun 11 11:27 .bash_history
-rw-r--r--  1 vamsi vamsi   220 May 29 17:03 .bash_logout
-rw-r--r--  1 vamsi vamsi  3771 May 29 17:03 .bashrc
drwx------ 15 vamsi vamsi  4096 Jun 11 10:20 .cache
drwx------ 13 vamsi vamsi  4096 Jun 13 11:16 .config
drwxr-xr-x  2 vamsi vamsi  4096 Jun 13 11:16 Desktop
drwxr-xr-x  2 vamsi vamsi  4096 May 29 19:16 Documents
drwxr-xr-x  2 vamsi vamsi  4096 May 29 19:16 Downloads
-rw-r--r--  1 vamsi vamsi  8980 May 29 17:03 examples.desktop
-rw-r--r--  1 vamsi vamsi    11 May 30 15:14 file2
-rw-------  1 vamsi vamsi 12288 May 30 12:25 .file.swp
-rwxr-xr-x  1 vamsi vamsi    15 Jun 21 09:33 foo.txt
```

3. **Explain what execute permission means/allows when it is associated with a directory.**

Answer:

Execute permission means by default the users have all permissions, groups have read and execute permissions, and others have only execute permissions. This means **users** can read, write and execute the files in that directory, for **groups** they have only read and execute permissions only, and **others** have only execute permissions.

4. **Suppose that you wanted all users on the machine to be able to see the contents of the file ~/public/software/instructions. text. Explain the minimum set of permissions for files and directories needed to allow this, and any security issues that arise.**

Answer:

Linux Command 1: $ cat > newfile.txt (Creates new file and adding the content inside the new file and saving the new file.

Linux Command 2: $ ls -al (Lists all the files and directory with the initial permissions and who can access the files and directory.

For **newfile.txt** the initial permissions are the **user** have read and write permissions, **groups** have just read permissions and **others** have only read permissions like groups.

```
vamsi@vamsi-VirtualBox:~/krishna$ cat > newfile.txt
Hello New File
^C
vamsi@vamsi-VirtualBox:~/krishna$ ls -al
total 36
drwxr-xr-x  3 vamsi vamsi 4096 Jun 21 14:26 .
drwxr-xr-x 20 vamsi vamsi 4096 Jun 21 09:33 ..
-rw-r--r--  1 vamsi vamsi   10 Jun 13 12:56 ..bye
-rw-r--r--  1 vamsi vamsi   10 Jun 13 12:54 .hai
drwxr-xr-x  2 vamsi vamsi 4096 Jun 13 12:40 hello
-rw-r--r--  1 vamsi vamsi   15 Jun 13 12:53 .hello
-rw-r--r--  1 vamsi vamsi   15 Jun 21 14:27 newfile.txt
-rw-r--r--  1 vamsi vamsi   22 Jun 13 12:29 stringfile
-rwxr-xr-x  1 vamsi vamsi    8 May 30 15:58 vamsi
vamsi@vamsi-VirtualBox:~/krishna$
```

5. **Suppose that you want to allow (only) other users bob and chuck to be able to access the above file. Explain what you would have to do differently from what you described above. (You are not allowed to consider the use of ACLs.)**

Answer:

```
root@vamsi-VirtualBox:/# adduser chuck
Adding user `chuck' ...
root@vamsi-VirtualBox:/# adduser bob
Adding user `bob' ...
vamsi@vamsi-VirtualBox:~$ groups bob
bob : trainers
vamsi@vamsi-VirtualBox:~$ groups chuck
chuck : trainers
vamsi@vamsi-VirtualBox:~$ su - bob
Password:
bob@vamsi-VirtualBox:~$ ls
examples.desktop  file1.txt
bob@vamsi-VirtualBox:~$ cat file1.txt
kjbkdjb
bob@vamsi-VirtualBox:~$ chmod 740 file1.txt
bob@vamsi-VirtualBox:~$ su - chuck
Password:
chuck@vamsi-VirtualBox:~$ pwd
/home/chuck
chuck@vamsi-VirtualBox:~$ cd ../bob
chuck@vamsi-VirtualBox:/home/bob$ ls
examples.desktop  file1.txt
chuck@vamsi-VirtualBox:/home/bob$ cat file.txt
cat: file.txt: No such file or directory
chuck@vamsi-VirtualBox:/home/bob$ cat file1.txt
kjbkdjb
chuck@vamsi-VirtualBox:/home/bob$
```

6. **How would your answer to the previous problem change if you were to use ACLs (access control lists)?**

Answer:

7. **What are set UID (SUID) files, and when are they typically used?**

Answer:

SUID – Set owner User ID is a special type of file permissions given to a file. Normally in Linux/Unix when a program runs, it inherits access permissions from the logged in user. SUID is defined as giving temporary permissions to a user to run a program/file with the file owner's permissions as well as owner UID and GID when executing a file/program/command.

8. **Find one SUID file on a Linux system, and show its "long listing" (permissions, owner, etc.).**

Answer: Here after listing the files **Command: $** ls -l /usr/bin/passwd

This shows the -rw**s**r-xr-x 1 - This **s** represents SUID on a Linux System, and ls -l shows the long listing of the files.

Usually the USER has the read, write and SUID permissions, the GROUPS have read and execute permissions and OTHERS have only execute permissions.

```
vamsi@vamsi-VirtualBox:~$ which passwd
/usr/bin/passwd
vamsi@vamsi-VirtualBox:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59640 Jan 25 10:09 /usr/bin/passwd
vamsi@vamsi-VirtualBox:~$
```

9. **Why are SUID root files considered a security issue?**

Answer:

SUID root files considered a security issue because these programs grant special privileges to the user who is executing them, it is necessary to ensure that insecure programs are not installed.

10. **What command would be used to set a file foo to be SUID, and how exactly would it be done?**

Answer:

```
vamsi@vamsi-VirtualBox:~/krishna$ chmod u+s newfile.txt
vamsi@vamsi-VirtualBox:~/krishna$ ls -al
total 44
drwxr-xr-x  3 vamsi vamsi 4096 Jun 21 16:41 .
drwxr-xr-x 20 vamsi vamsi 4096 Jun 21 09:33 ..
-rw-r--r--  1 vamsi vamsi   43 Jun 21 16:33 abc.txt
-rw-r--r--  1 vamsi vamsi   69 Jun 21 16:41 ab.txt
-rw-r--r--  1 vamsi vamsi   10 Jun 13 12:56 ..bye
-rw-r--r--  1 vamsi vamsi   10 Jun 13 12:54 .hai
drwxr-xr-x  2 vamsi vamsi 4096 Jun 13 12:40 hello
-rw-r--r--  1 vamsi vamsi   15 Jun 13 12:53 .hello
-rwSr--r--  1 vamsi vamsi   15 Jun 21 14:27 newfile.txt
-rw-r--r--  1 vamsi vamsi   22 Jun 13 12:29 stringfile
-rwxr-xr-x  1 vamsi vamsi    8 May 30 15:58 vamsi
```

11. **What command could determine the process ID (PID) of a running SSH server (sshd)?**

Answer: **Linux Command: $** ps axjf | grep ssh

This command defines the list of all Process ID of running SSH server. Here **axjf** displays the columns PPID, PID, SID, UID, TIME, COMMAND, STAT, TTY, TPGID, and **grep ssh** filters the all sshd process in the linux.

```
vamsi@vamsi-VirtualBox:~$ ps axjf | grep ssh
 1038  1131  1131  1131 ?           -1 Ss    1000   0:00
    \_ /usr/bin/ssh-agent /usr/bin/im-launch env GNOME_SHELL_SESSI
ON_MODE=ubuntu gnome-session --session=ubuntu
    1   713   713   713 ?           -1 Ss       0   0:00 /usr/sbin
/sshd -D
 1619  1680  1680  1619 pts/0    26623 T     1000   0:00
\_ ssh root@172.31.27.206
 1619 26624 26623  1619 pts/0    26623 S+    1000   0:00
\_ grep --color=auto ssh
vamsi@vamsi-VirtualBox:~$
```

12. **What command would best identify which process is using excessive CPU resources?**

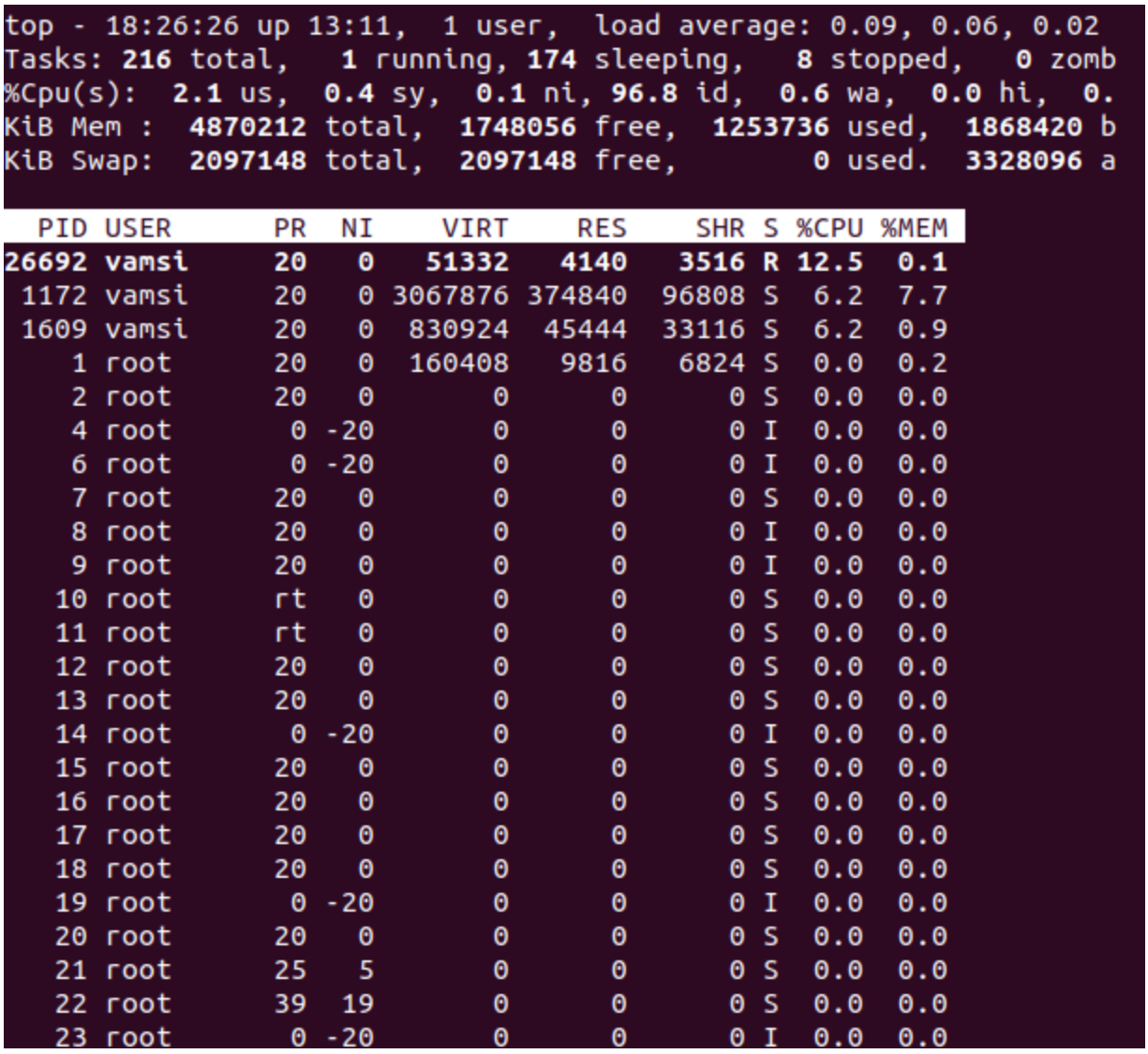
Answer:

Linux Command: $ top **(or)** $ top -n 10

Command **top** displays the system running information as well as a list of processes or threads currently being managed in Kernel.

Press **s** to change refresh time.

Press **i** to see only running process.



13. What command that should definitely terminate the process identified above?

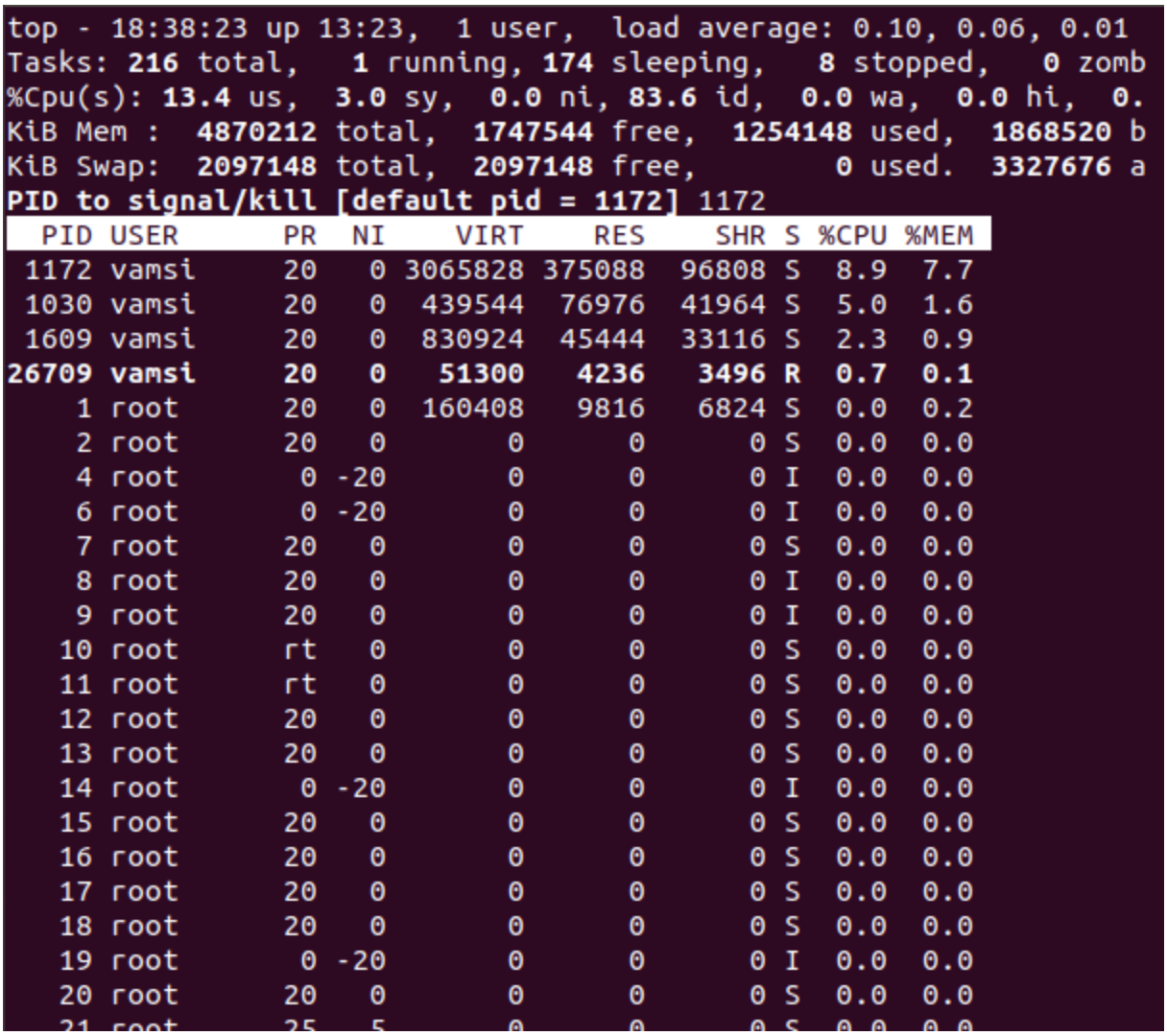
Answer:

Linux Command: $ top **(or)** $ top -n 10

Command **top** displays the system running information as well as a list of processes or threads currently being managed in Kernel.

Note down thee PID then,

Press **k** and type **PID** to close the process. Or ***Linux Command:* $ kill -9 PID**



14. **What file contains the list of valid user ID's (UID's) and their associated usernames?**

Answer:

Linux Command: $ cat /etc/passwd

This is used to list all the UID's which is created in the linux and location of the user.

```
vamsi@vamsi-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/u
sr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/syste
md/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve
:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-auto
ipd:/usr/sbin/nologin
```

15. **What file contains passwords on a Linux system (if that system is using local authentication rather than NIS, etc.)?**

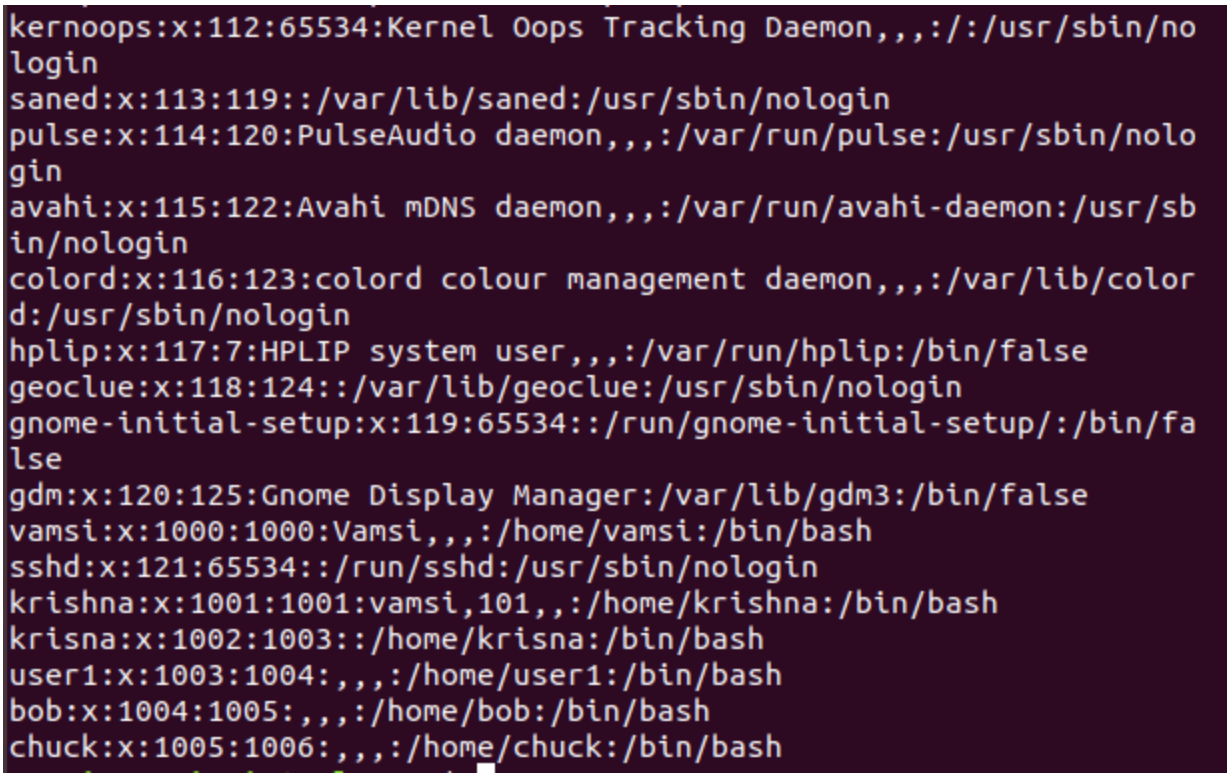
Answer:

Linux Command: $ cat /etc/passwd

This command shows the passwords on a Linux system.

Here **X** shows the password of the user (X is next to the user).

X is an encrypted password is stored in **etc/shadow** file.



16. **What is difference between telnet and ssh. When will you use each command? give examples.**

Answer:

Telnet:

- Telnet was designed to work within a private network and99l not across a public network where threats can appear.
- If a user was sniffing a network it's very possible they could grab your Username and password, as they were being transmitted.
- It is insecure because it transfers all data in clear text.

Examples:

- Accessing old school servers for remote connections.
- Watch movies in full text, play games, check weather forecast.

Linux Command: $ telnet -l myusername myhost.com:5555

SSH (Secure Shell):

- It is secure protocol for remote logins.
- Using SSH client, a user can connect to a server to transfer information in a more secure manner than Telnet.
- It is cryptographic network protocol.
- It is encrypted and secured.

Examples:

Log into remote machines and execute commands.
Connect two Linux operating system with secure
Linux Command to connect two operating system: ssh username@ip_address