

CYSE 695 – Linux for Cybersecurity

Module 2 | Linux Basic Commands

Total: 100 Points

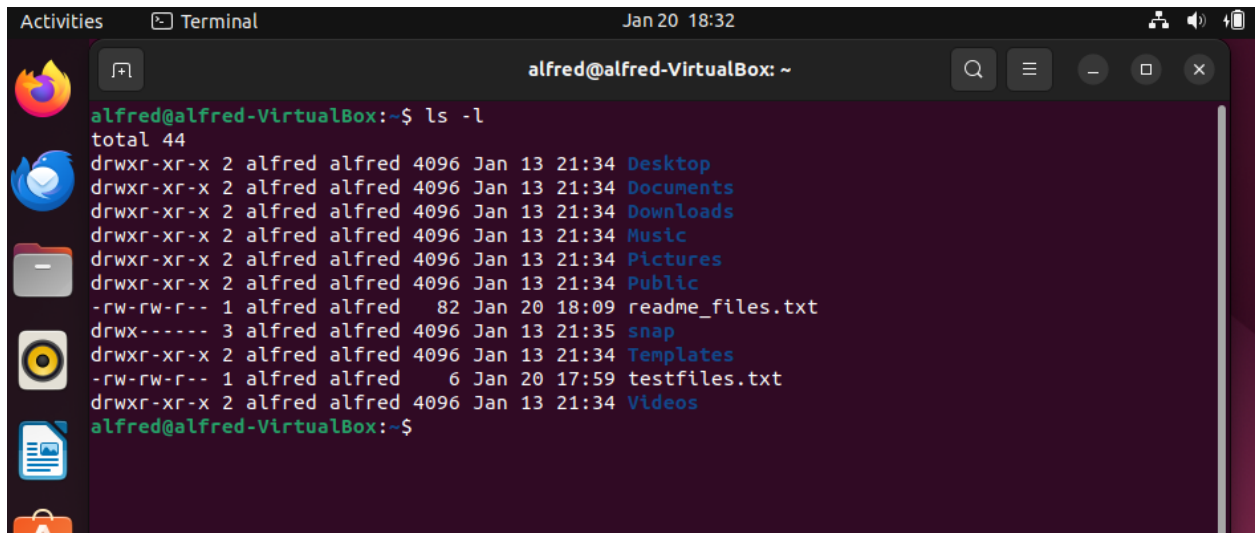
Name: Alfred Acquaye

Directions: Practice the following tasks in Linux VM – Ubuntu using various Linux commands for file management. Insert screenshots where applicable. Upload completed document in Canvas.

Task 1: ls command

- Use `ls -l` to display detailed information about the files in your home directory. Upload the screenshot for this step after executing the command.

[Add screenshot here]

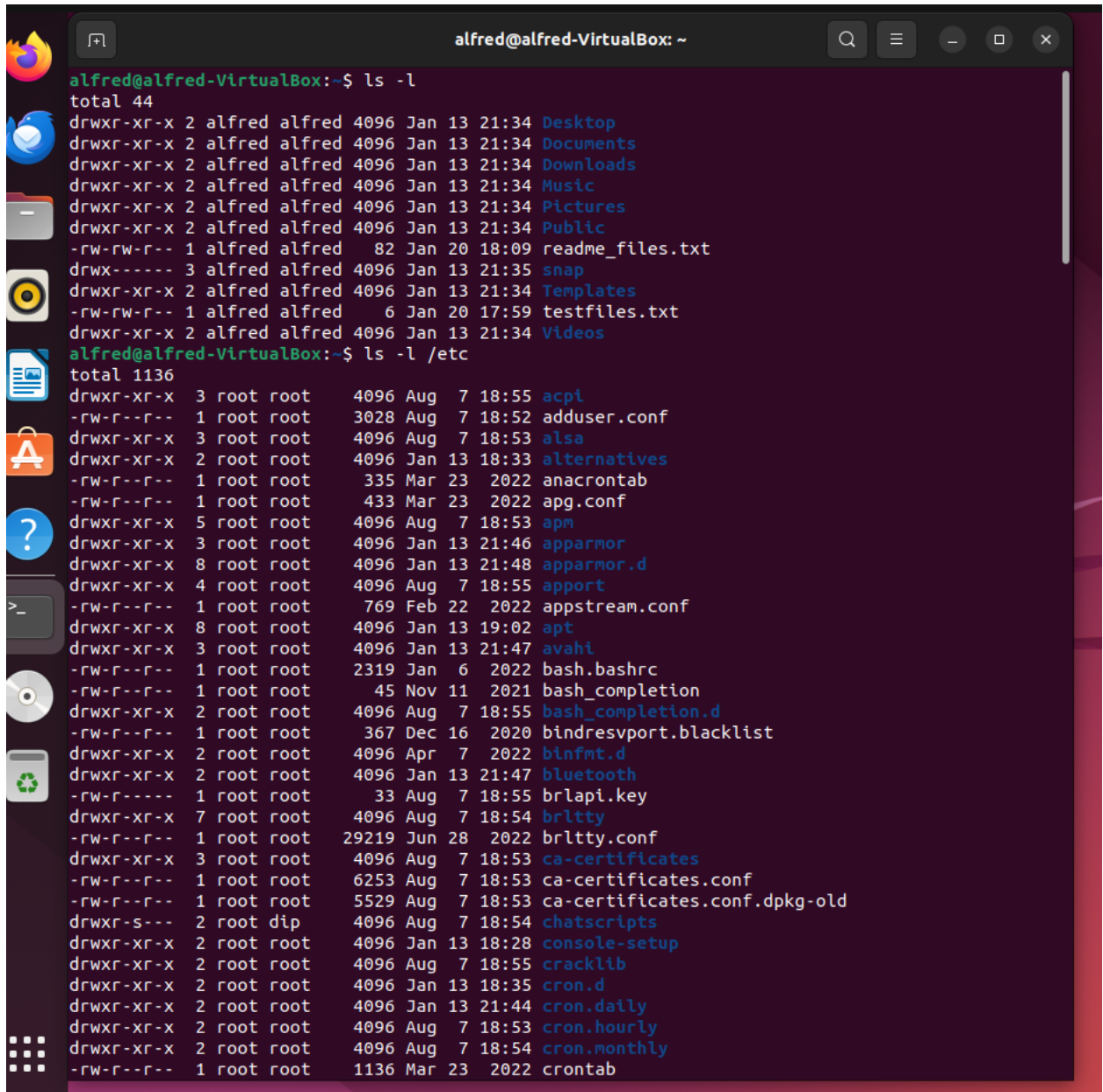


The screenshot shows a terminal window titled 'alfred@alfred-VirtualBox: ~'. The command `ls -l` has been executed, displaying the following output:

```
alfred@alfred-VirtualBox:~$ ls -l
total 44
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Desktop
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Documents
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Downloads
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Music
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Pictures
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Public
-rw-rw-r-- 1 alfred alfred  82 Jan 20 18:09 readme_files.txt
drwx----- 3 alfred alfred 4096 Jan 13 21:35 snap
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Templates
-rw-rw-r-- 1 alfred alfred   6 Jan 20 17:59 testfiles.txt
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Videos
alfred@alfred-VirtualBox:~$
```

- Use `ls -l` to display detailed information about the files in `/etc` directory. Upload the screenshot for this step after executing the command.

[Add screenshot here]



```
alfred@alfred-VirtualBox: ~  
alfred@alfred-VirtualBox:~$ ls -l  
total 44  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Desktop  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Documents  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Downloads  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Music  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Pictures  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Public  
-rw-rw-r-- 1 alfred alfred 82 Jan 20 18:09 readme_files.txt  
drwx----- 3 alfred alfred 4096 Jan 13 21:35 snap  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Templates  
-rw-rw-r-- 1 alfred alfred 6 Jan 20 17:59 testfiles.txt  
drwxr-xr-x 2 alfred alfred 4096 Jan 13 21:34 Videos  
alfred@alfred-VirtualBox:~$ ls -l /etc  
total 1136  
drwxr-xr-x 3 root root 4096 Aug 7 18:55 acpi  
-rw-r--r-- 1 root root 3028 Aug 7 18:52 adduser.conf  
drwxr-xr-x 3 root root 4096 Aug 7 18:53 alsa  
drwxr-xr-x 2 root root 4096 Jan 13 18:33 alternatives  
-rw-r--r-- 1 root root 335 Mar 23 2022 anacrontab  
-rw-r--r-- 1 root root 433 Mar 23 2022 apg.conf  
drwxr-xr-x 5 root root 4096 Aug 7 18:53 apm  
drwxr-xr-x 3 root root 4096 Jan 13 21:46 apparmor  
drwxr-xr-x 8 root root 4096 Jan 13 21:48 apparmor.d  
drwxr-xr-x 4 root root 4096 Aug 7 18:55 appport  
-rw-r--r-- 1 root root 769 Feb 22 2022 appstream.conf  
drwxr-xr-x 8 root root 4096 Jan 13 19:02 apt  
drwxr-xr-x 3 root root 4096 Jan 13 21:47 avahi  
-rw-r--r-- 1 root root 2319 Jan 6 2022 bash.bashrc  
-rw-r--r-- 1 root root 45 Nov 11 2021 bash_completion  
drwxr-xr-x 2 root root 4096 Aug 7 18:55 bash_completion.d  
-rw-r--r-- 1 root root 367 Dec 16 2020 bindresvport.blacklist  
drwxr-xr-x 2 root root 4096 Apr 7 2022 binfmt.d  
drwxr-xr-x 2 root root 4096 Jan 13 21:47 bluetooth  
-rw-r----- 1 root root 33 Aug 7 18:55 brlapi.key  
drwxr-xr-x 7 root root 4096 Aug 7 18:54 brltty  
-rw-r--r-- 1 root root 29219 Jun 28 2022 brltty.conf  
drwxr-xr-x 3 root root 4096 Aug 7 18:53 ca-certificates  
-rw-r--r-- 1 root root 6253 Aug 7 18:53 ca-certificates.conf  
-rw-r--r-- 1 root root 5529 Aug 7 18:53 ca-certificates.conf.dpkg-old  
drwxr-xr-x 2 root dip 4096 Aug 7 18:54 chatscripts  
drwxr-xr-x 2 root root 4096 Jan 13 18:28 console-setup  
drwxr-xr-x 2 root root 4096 Aug 7 18:55 cracklib  
drwxr-xr-x 2 root root 4096 Jan 13 18:35 cron.d  
drwxr-xr-x 2 root root 4096 Jan 13 21:44 cron.daily  
drwxr-xr-x 2 root root 4096 Aug 7 18:53 cron.hourly  
drwxr-xr-x 2 root root 4096 Aug 7 18:54 cron.monthly  
-rw-r--r-- 1 root root 1136 Mar 23 2022 crontab
```

- What are the security implications of using the ls command? How can it be configured to display only specific file attributes? Type your answer in **3 to 5** sentences here.

Response:

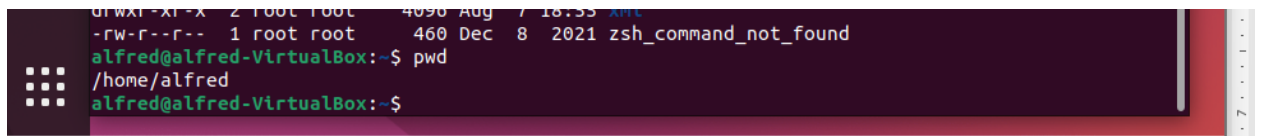
The exposure of sensitive files or directories might be a security issue if they are visible to unauthorized users or stored in unsafe locations. For example, a malicious individual may utilize the information from the ls command to learn about the organization of directories, patterns used for file names, or possible configuration files.

To selectively show particular file properties, you may integrate the "ls" tool with other commands and arguments. As an example: Using the command "ls -l" to exhibit comprehensive data, after that redirect the output to either "awk" or "cut" to extract particular columns.

Task 2: pwd command

- Use pwd command to confirm your new working directory. Upload the screenshot for this step after executing the command.

[Add screenshot here]

A terminal window with a dark background and light green text. The prompt is 'alfred@alfred-VirtualBox:~\$'. The user enters 'pwd' and the output is '/home/alfred'. The prompt changes to 'alfred@alfred-VirtualBox:~\$'.

- What are the potential security vulnerabilities associated with the pwd command and how can they be mitigated? Type your answer in **3 to 5** sentences here.
 - Logging or displaying the output of the pwd command in an unsecured context, such as a shared terminal session or a web application, may expose directory hierarchies, system architecture, or the presence of sensitive directories to unauthorized users.
 - Exercise caution with the location where the output of the pwd command is displayed or recorded. Refrain from utilizing it unduly in scripts or command outputs that unauthorized persons might potentially access.

Task 3: echo command

- Use the echo command to display a greeting message with your username. Take the screenshot for this step after executing the command.

[Add screenshot here]

A terminal window with a dark background and light green text. The prompt is 'alfred@alfred-VirtualBox:~\$'. The user enters 'echo Alfred' and the output is 'Alfred'. The prompt changes to 'alfred@alfred-VirtualBox:~\$'.

- Redirect the output of the echo command to a new file named "greeting.txt" in your home directory. Take the screenshot for this step after executing the command.

[Add screenshot here]

```
Alfred
alfred@alfred-VirtualBox:~$ echo Alfred > greeting.txt
alfred@alfred-VirtualBox:~$
```

Task 4: cd command

- Use cd command to change the directory to /etc. Take the screenshot for this step after executing the command.

[Add screenshot here]

```
alfred@alfred-VirtualBox:~$ cd /etc
alfred@alfred-VirtualBox:/etc$
```

Task 5: Pattern searching using grep command

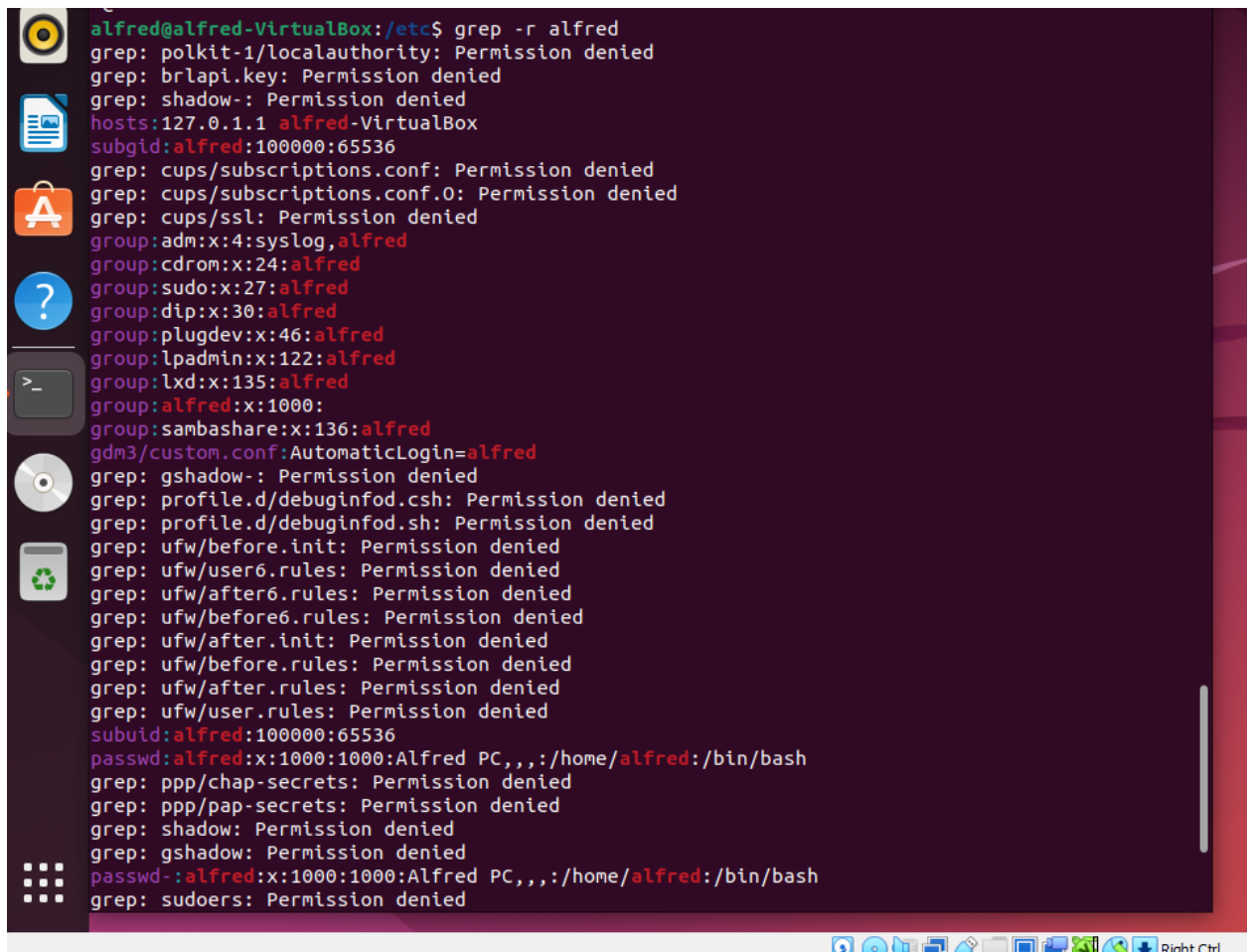
- Use the grep command to search for your username within the contents of the “/etc/passwd” file.

[Add screenshot here]

```
alfred@alfred-VirtualBox:~$ cd /etc
alfred@alfred-VirtualBox:/etc$ grep alfred /etc/passwd
alfred:x:1000:1000:Alfred PC,,,:/home/alfred:/bin/bash
alfred@alfred-VirtualBox:/etc$
```

- Display the lines containing "your username." Take the screenshot for this step after executing the command.

[Add screenshot here]



```
alfred@alfred-VirtualBox:/etc$ grep -r alfred
grep: polkit-1/localauthority: Permission denied
grep: brlapi.key: Permission denied
grep: shadow-: Permission denied
hosts:127.0.1.1 alfred-VirtualBox
subgid:alfred:100000:65536
grep: cups/subscriptions.conf: Permission denied
grep: cups/subscriptions.conf.0: Permission denied
grep: cups/ssl: Permission denied
group:adm:x:4:syslog,alfred
group:cdrom:x:24:alfred
group:sudo:x:27:alfred
group:dip:x:30:alfred
group:plugdev:x:46:alfred
group:lpadmin:x:122:alfred
group:lxde:x:135:alfred
group:alfred:x:1000:
group:sambashare:x:136:alfred
gdm3/custom.conf:AutomaticLogin=alfred
grep: gshadow-: Permission denied
grep: profile.d/debuginfod.csh: Permission denied
grep: profile.d/debuginfod.sh: Permission denied
grep: ufw/before.init: Permission denied
grep: ufw/user6.rules: Permission denied
grep: ufw/after6.rules: Permission denied
grep: ufw/before6.rules: Permission denied
grep: ufw/after.init: Permission denied
grep: ufw/before.rules: Permission denied
grep: ufw/after.rules: Permission denied
grep: ufw/user.rules: Permission denied
subuid:alfred:100000:65536
passwd:alfred:x:1000:1000:Alfred PC,,,:/home/alfred:/bin/bash
grep: ppp/chap-secrets: Permission denied
grep: ppp/pap-secrets: Permission denied
grep: shadow: Permission denied
grep: gshadow: Permission denied
passwd:alfred:x:1000:1000:Alfred PC,,,:/home/alfred:/bin/bash
grep: sudoers: Permission denied
```

Grading Criteria

Task 1: ls command [3 subtasks x 10 = 30 Points]

Task 2: pwd command [2 subtasks x 10 = 20 Points]

Task 3: echo command [2 subtasks x 10 = 20 Points]

Task 4: cd command [1 subtask = 10 Points]

Task 5: Pattern searching using grep command [2 subtasks x 10 = 20 Points]