

ComOR Lab 8

นายกานต์ สุดตี 66070014

1. ให้ใช้ CODE คือ รหัส นศ และสร้าง Directory และไฟล์ดังนี้
ใน Home Directory สร้าง Directory ชื่อ CODE-D1 และ ใน CODE-D1
สร้าง Directory CODE-D2 และสร้างไฟล์ 0 byte ชื่อ CODE-F1 ใน
CODE-D1 และ สร้างไฟล์ที่มีข้อความข้างในเป็น รหัส นศ ชื่อ CODE-F2 ใน
CODE-D2

คำสั่งที่ใช้:

- mkdir 66070014-D1 (สร้าง Directory D1)
- cd 66070014-D1 (เข้าไปที่ Directory D1)
- mkdir 66070014-D2 (สร้าง Directory D2)
- touch 66070014-F1 (สร้างไฟล์ 0 byte ที่ D1)
- echo 66070014 > 66070014-F2 (สร้างไฟล์ F2 ใน D2)

```
karn44@kserver:~$ mkdir 66070014-D1
karn44@kserver:~$ ls
66070014-D1  66070014-Dir
karn44@kserver:~$ cd 66070014-D1
karn44@kserver:~/66070014-D1$ mkdir 66070014-D2
karn44@kserver:~/66070014-D1$ touch 66070014-F1
```

```
karn44@kserver:~/66070014-D1$ ls -la
total 12
drwxrwxr-x 3 karn44 karn44 4096 Jan 16 17:55 .
drwxr-x--- 7 karn44 karn44 4096 Jan 16 17:54 ..
drwxrwxr-x 2 karn44 karn44 4096 Jan 16 17:58 66070014-D2
-rw-rw-r-- 1 karn44 karn44    0 Jan 16 17:55 66070014-F1
karn44@kserver:~/66070014-D1$ _
```

(จาก ls -la จะเห็นว่าไฟล์ F2 มีขนาด 0 byte)

```
karn44@kserver:~/66070014-D1$ cd 66070014-D2/
karn44@kserver:~/66070014-D1/66070014-D2$ echo 66070014 > 66070014-F2
karn44@kserver:~/66070014-D1/66070014-D2$ cat 66070014-F2
66070014
karn44@kserver:~/66070014-D1/66070014-D2$ _
```

2.นับจำนวนไฟล์ทั้งหมดใน Directories ดังนี้ (ไม่รวม Subdirectories หรือ Hidden Files)

- Home Directory

ใช้คำสั่ง ls -l | grep ^- | wc -l

```
karn44@kserver:~$ ls -l | grep ^- | wc -l
0
karn44@kserver:~$ ls -l
total 8
drwxrwxr-x 3 karn44 karn44 4096 Jan 16 17:55 66070014-D1
drwxrwxr-x 2 karn44 karn44 4096 Jan 10 07:58 66070014-Dir
karn44@kserver:~$ _
```

ls -l คือ แสดงรายการเป็นบรรทัด

grep ^- คือเอาเฉพาะบรรทัดที่ขึ้นต้นด้วย - เพราะ ถ้าเป็น Directory จะขึ้นต้นด้วย d จึงใช้ grep เพื่อกรองเอาเฉพาะที่เป็นไฟล์

wc -l คือนับจำนวนบรรทัด

- /usr (sec 3)

ใช้คำสั่ง ls -l /usr | grep ^- | wc -l

```
karn44@kserver:~$ ls -l /usr | grep ^- | wc -l
0
karn44@kserver:~$ ls -l /usr
total 88
drwxr-xr-x  2 root root 36864 Jan 10 08:20 bin
drwxr-xr-x  2 root root  4096 Apr 22 2024 games
drwxr-xr-x 33 root root  4096 Nov 19 16:24 include
drwxr-xr-x 79 root root  4096 Jan 10 08:20 lib
drwxr-xr-x  2 root root  4096 Aug 27 14:21 lib64
drwxr-xr-x 11 root root  4096 Jan 10 08:20 libexec
drwxr-xr-x 10 root root  4096 Aug 27 14:18 local
drwxr-xr-x  2 root root 20480 Jan 10 08:20 sbin
drwxr-xr-x 124 root root  4096 Nov 19 16:24 share
drwxr-xr-x  6 root root  4096 Jan 10 08:20 src
karn44@kserver:~$ _
```

- /

ใช้คำสั่ง ls -l / | grep ^- | wc -l

```
drwxr-xr-x  0 root root  4096 Jan 10 08:20 src
karn44@kserver:~$ ls -l / | grep ^- | wc -l
1
karn44@kserver:~$
```

click inside or press Ctrl+G

3.นับจำนวนไฟล์ทั้งหมดใน Directories ดังนี้ (รวม Subdirectories แต่ไม่ต้องนับ Hidden Files)

- Home Directory

ใช้คำสั่ง ls -l -R | grep ^- | wc -l

```
1
karn44@kserver:~$ ls -l -R | grep ^- | wc -l
4
karn44@kserver:~$ ls -l -R
.:
total 8
drwxrwxr-x 3 karn44 karn44 4096 Jan 16 17:55 66070014-D1
drwxrwxr-x 2 karn44 karn44 4096 Jan 10 07:58 66070014-Dir

./66070014-D1:
total 4
drwxrwxr-x 2 karn44 karn44 4096 Jan 16 17:58 66070014-D2
-rw-rw-r-- 1 karn44 karn44     0 Jan 16 17:55 66070014-F1

./66070014-D1/66070014-D2:
total 4
-rw-rw-r-- 1 karn44 karn44  9 Jan 16 17:58 66070014-F2

./66070014-Dir:
total 8
-rw-rw-r-- 1 karn44 karn44 11 Jan 10 07:57 66070014-File
-rw-rw-r-- 1 karn44 karn44 11 Jan 10 07:58 66070014-File-copy
karn44@kserver:~$
```

เพิ่ม -R เข้ามา คือ ให้แสดงผลแบบรวมทั้ง Subdirectories ด้วย

- /usr (sec 3)

ls -l -R /usr | grep ^- | wc -l

```
karn44@kserver:~$ ls -l -R /usr | grep ^- | wc -l
106498
karn44@kserver:~$
```

- /

ใช้คำสั่ง ls -l -R / 2>/dev/null | grep ^- | wc -l

```
217545
karn44@kserver:~$ ls -l -R / 2>/dev/null | grep ^- | wc -l
217549
karn44@kserver:~$
```

4. เขียน Shell script นับเลขจาก x ไป y (รองรับกรณี $y \geq X$ และ $X \leq Y$) และแสดงผลออกหน้าจอ โดยรับค่า X และ Y จากช่องทางต่อไปนี้

- จากการป้อนให้จาก User

```
GNU nano 7.2
#!/bin/bash

read x
read y
step=1
if [ $x -gt $y ]
then step=-1
fi

for ((i=x; i!=y+step; i+=step))
do echo $i
done
```

read x // อ่านค่าจากผู้ใช้

read y // อ่านค่าจากผู้ใช้

step=1 // กำหนด step เริ่มต้นที่ 1

If [\$x -gt \$y]

Then step=-1 // ถ้า x มากกว่า y ให้เปลี่ยน step เป็น -1 เพื่อจะนับลดลง

Fi

For ((i=x; i!=y+step; i+=step))

do echo \$i // ลูปแสดงผล ตั้งแต่ x ถึง y

done

เปลี่ยน permission เพื่อที่จะ execute จากนั้นก็รันโปรแกรม

```
karn44@kserver:~$ chmod a+x app.sh
```

```
karn44@kserver:~$ ./app.sh
1
10
1
2
3
4
5
6
7
8
9
10
karn44@kserver:~$ ./app.sh
10
1
9
8
7
6
5
4
3
2
1
```

- จาก Arguments ตอนเรียก Script

```
#!/bin/bash

x=$1
y=$2
step=1
if [ $x -gt $y ]
then step=-1
fi

for ((i=x; i!=y+step; i+=step))
do echo $i
done
```

เปลี่ยนแค่สองบรรทัดแรก

x=\$1

y=\$2

เรียกใช้โดยใส่ Arguments เพิ่มไปตอนเรียกใช้

```
karn44@kserver:~$ ./app.sh 1 5
1
2
3
4
5
karn44@kserver:~$ ./app.sh 5 1
5
4
3
2
1
karn44@kserver:~$
```

- จาก Enviroment Variable

```
# ! /bin/bash

step=1
if [ $x -gt $y ]
then step=-1
fi

for ((i=$x; i!=$y+step; i+=step))
do echo $i
done
```

ทำการสร้างตัวแปร Enviroment ด้วยคำสั่ง export

```
export x=1
```

```
export y=6
```

```
karn44@kserver:~$ export x=1
karn44@kserver:~$ export y=6
```

```
karn44@kserver:~$ echo $x
1
karn44@kserver:~$ echo $y
6
```

จากนั้นทดลองรัน Shell script

```
karn44@kserver:~$ ./app.sh
1
2
3
4
5
6
karn44@kserver:~$
```

```
karn44@kserver:~$ x=6
karn44@kserver:~$ y=1
karn44@kserver:~$ ./app.sh
6
5
4
3
2
1
karn44@kserver:~$
```

5. เขียน Shell Script หาค่า Hash แบบ md5 จากไฟล์ใน /etc และ Subdirectories แล้วบันทึกลงในไฟล์ชื่อ FileChkSum

```
# ! /bin/bash  
sudo find /etc -type f -exec md5sum {} + > FileChkSum_
```

เขียน Shell Script ตั้งชื่อว่า findHash.sh และก็สังรับ สั่ง ls ดูจะพบไฟล์ FileChkSum จากนั้นใช้ head เพื่อดูข้อมูลในไฟล์ (ถ้าดูหมดข้อมูลเยอะเกิน)

```
karn44@kserver:~$ ls  
66070014-D1 66070014-Dir app.sh findHash.sh temp y  
karn44@kserver:~$ ./findHash.sh  
karn44@kserver:~$ ls  
66070014-D1 66070014-Dir app.sh FileChkSum findHash.sh temp y  
karn44@kserver:~$ head FileChkSum  
d41d8cd98f00b204e9800998ecf8427e /etc/newt/palette.original  
ac72ec93d29d94ad06bb3180f16cefb1 /etc/newt/palette.ubuntu  
e61078721cb3be18f48a8d4530b7201c /etc/locale.alias  
4869da5f5f508dfbc341342a272c36c8 /etc/adduser.conf  
e59ff97941044f85df5297e1c302d260 /etc/motd  
897575e9072555aed9075075e72b5acd /etc/modules  
cd9ed0429e53ea8b5d31e2d544585e5c /etc/apparmor.d/rssguard  
26615466c8cae2bfb8300d7474cb864c /etc/apparmor.d/steam  
53cb9b6edee094984349ab0a1a38efda /etc/apparmor.d/tuxedo-control-center  
588e4c06bb88ca522fd840c83117569f /etc/apparmor.d/unprivileged_userns  
karn44@kserver:~$
```

click inside or press Ctrl+G.

6.เขียน Shell Script สำหรับทำ File Integrity Check โดยการหาค่า Hash แบบ md5 ของไฟล์ใน /etc และเปรียบเทียบกับที่บันทึกในไฟล์ FileChkSum ในข้อ 5 จากนั้นทดสอบโดยสร้าง User ใหม่ชื่อ Hacker และเรียกใช้ Script นี้ แล้วบันทึกผล

เขียนไฟล์ Script ที่จะตรวจสอบความแตกต่างระหว่าง TempFile ที่จะสร้างโดยการหาค่า Hash แบบ md5 ของไฟล์ใน /etc จากนั้น ก็ใช้ diff เพื่อตรวจสอบว่ามันยังเหมือนกันหรือไม่

```
GNU nano 7.2
#!/bin/bash

sudo find /etc -type f -exec md5sum {} + > TempFile
if [ -z "$(diff TempFile FileChkSum)" ]
then echo "No change from FileChkSum"
else
echo "Error! FileChkSum is not the Same, See the different below."
echo "-----File Diff-----"
echo $(diff TempFile FileChkSum)
fi
```

สร้าง User ใหม่มา คือ Hacker

```
karn44@kserver:~$ sudo useradd Hacker
```

เรียกใช้ Script เพื่อตรวจสอบ

```
karn44@kserver:~$ ./integrity_check.sh
Error! FileChkSum is not the Same, See the different below.
-----File Diff-----
274c274 < 78218b1381c6687b144a247c24c71794 /etc/gshadow --- > f6135cd45beefe1
id --- > e75e7a46c1f26290b0f6ab7c563902c3 /etc/subgid 510c510 < de2f569bcf77a
- 598c598 < f6135cd45beefe1380b34da5e2aef2e9 /etc/gshadow- --- > 78218b1381c6
subgid- --- > d50019ba4a7e81ddf6aad5d59b3b3b1c /etc/subgid- 629c629 < 27301e4
```

จะเห็นว่า จะมีความแตกต่างกันอยู่ ดังผลลัพธ์ที่ออกมานะ

ถ้าลองเรียกใช้ findHash.sh อีกครั้ง จากนั้นจึงลอง เรียกใช้ integrity_check

```
karn44@kserver:~$ ./findHash.sh
karn44@kserver:~$ ./integrity_check.sh
No change from FileChkSum
karn44@kserver:~$ _
```

จะสังเกตได้ว่า ทั้งสองไฟล์เหมือนกันแล้ว