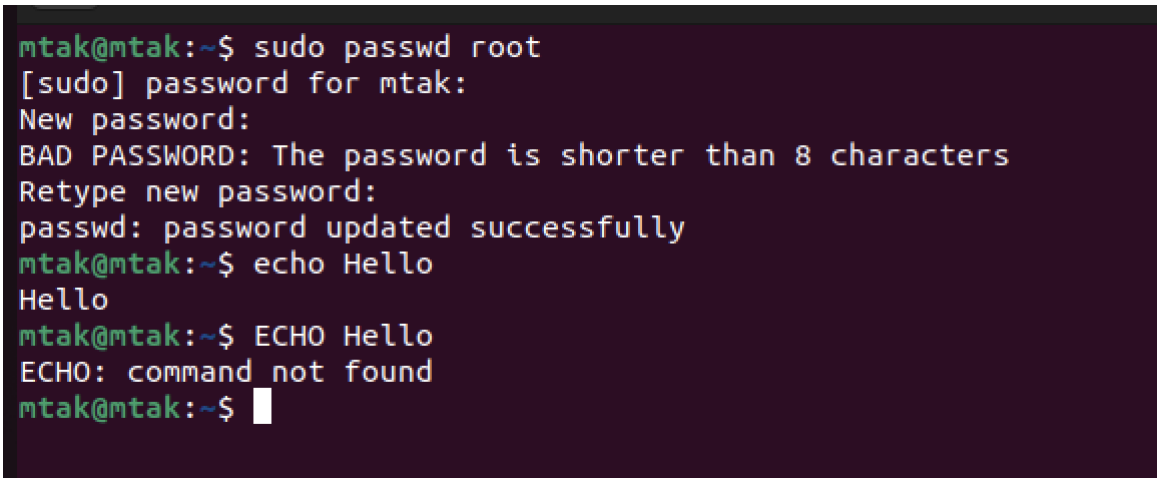
Homework #1

1. Start a Terminal (Applications>Accessories>Terminal)

2. Change the root password to “1234” by using “sudo passwd”.

3. Compare the command “echo Hello” and “Echo Hello”

(1) Take a screenshot



(2) Explain the reason of the result

sudo passwd root 로 비밀번호를 변경하였는데, mtak 은 sudoer 이므로 password for mtak 에 mtak 의 password 를 입력하고 일치하면, New password:가 나온다. 1234 를 치고, 재입력을 하면 변경이 완료된다.

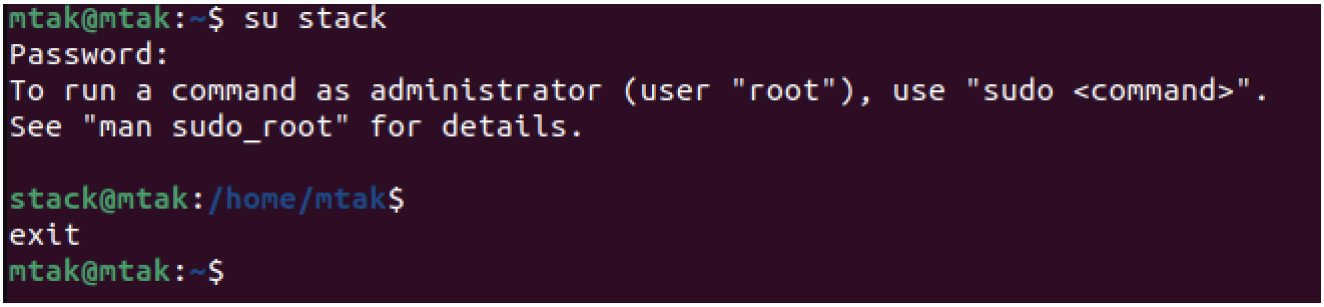
command 는 대소문자를 구별하므로, Echo 명령어는 리눅스 명령어가 아니므로 실행 되지 않는다.

4. Press “CTRL+d” or “ALT+F4”

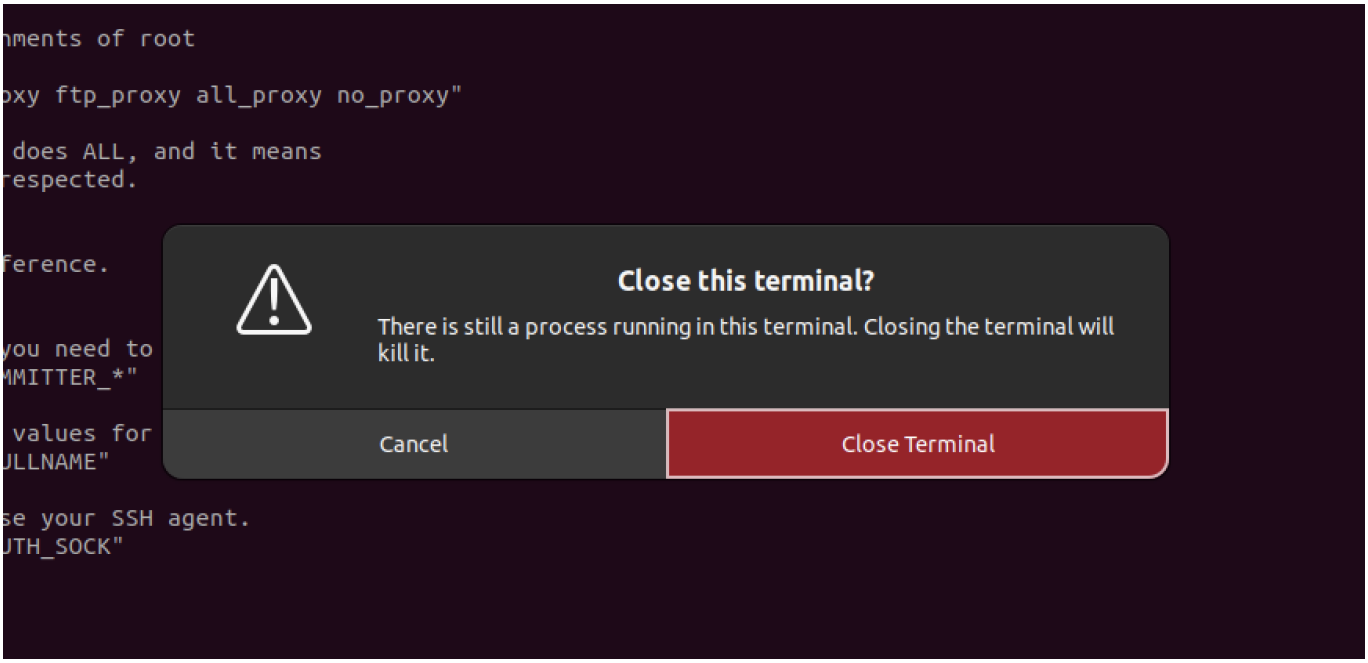
(1) Describe what happens

“Ctrl + D”는 명령어 exit처럼 해당 계정을 shell 에서 log out 하는데 반해, Alt + F4 도 비슷하나, 이는 터미널 자체를 꺼버린다.

예를 들어, mtak 에서 su stack 이라는 명령으로 유저를 바꾸고, Ctrl+D 를 누르면 다시 mtak 으로 돌아오지만,



Alt +F4 를 누르고, Close Terminal 을 누르면 , 아예 터미널 자체를 종료시킨다.



5. 다음을 따라와보자.

1. Start a Terminal, then do “su” (enter the password, “1234”),
2. then do “groupadd defender”,
3. then do “groupadd attacker”,
4. then do “groupadd neverland”,
5. then do ”useradd peterpan -m -s /bin/bash -G defender,neverland”,
6. then do “useradd hook -m -s /bin/bash -G neverland”,
7. then do “passwd peterpan” (set new password (1234)),
8. then do “passwd hook” (set new password(1234)),
9. then do “usermod -a -G attacker hook”,
10. then do “tail /etc/passwd”,
11. then do “tail /etc/group”,
12. then do “id peterpan”,
13. then do “id hook”,
14. do “exit”

(1) Take a screen shot

```
mtak@mtak:~$ su
Password:
root@mtak:/home/mtak# groupadd defender
root@mtak:/home/mtak# groupadd attacker
root@mtak:/home/mtak# groupadd neverland
root@mtak:/home/mtak# useradd peterpan -m -s -G defender, neverland
useradd: invalid shell '-G'
root@mtak:/home/mtak# useradd peterpan -m -s -G defender,neverland
useradd: invalid shell '-G'
root@mtak:/home/mtak# useradd peterpan -m -s /bin/bash -G defender,neverland
root@mtak:/home/mtak# useradd hook -m -s /bin/bash -G neverland
root@mtak:/home/mtak# passwd peterpan
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
root@mtak:/home/mtak# passwd hook
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
root@mtak:/home/mtak# usermod -a -G attacker hook
root@mtak:/home/mtak# tail /etc/passwd
geoclue:x:124:131::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:125:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:126:65534::/run/gnome-initial-setup/:/bin/false
hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
mtak:x:1000:1000:mtak,,,:/home/mtak:/bin/bash
stack:x:1001:1002::/home/stack:/bin/bash
gslee:x:1002:1004::/home/gslee:/bin/bash
peterpan:x:1003:1008::/home/peterpan:/bin/bash
hook:x:1004:1009::/home/hook:/bin/bash
root@mtak:/home/mtak# tail /etc/group
sambashare:x:136:mtak
admin:x:1001:stack
stack:x:1002:
faculty:x:1003:gslee
gslee:x:1004:
defender:x:1005:peterpan
attacker:x:1006:hook
neverland:x:1007:peterpan,hook
peterpan:x:1008:
hook:x:1009:
root@mtak:/home/mtak# id peterpan
uid=1003(peterpan) gid=1008(peterpan) groups=1008(peterpan),1005(defender),1007(neverland)
root@mtak:/home/mtak# id hook
uid=1004(hook) gid=1009(hook) groups=1009(hook),1006(attacker),1007(neverland)
root@mtak:/home/mtak# exit
exit
mtak@mtak:~$
```

(2) Describe the meaning of the commands

(a) “useradd peterpan -m -s /bin/bash -G defender,neverland”

peterpan 이라는 유저를 추가하는데 -m 은 peterpan 의 홈 디렉토리를 /home 에 만든다. -s 는 default 로그인 쉘을 설정하는데 peterpan 의 default shell 을 /bin/bash 로 설정한다. -G defender,neverland 는 peterpan 을 defender, neverland 그룹에 추가한다.

(b) usermod -a -G attacker hook

system account file 을 수정하는 명령어 인데, hook을 attacker 그룹에 추가한다. -a(append) 를 붙여주지 않는다면, hook 는 neverland 그룹에 속하지 않고 attacker 그룹에만 속합니다. 고로 -a를 붙였으니 hook는 neverland 와 attacker 그룹에 속하게 된다.

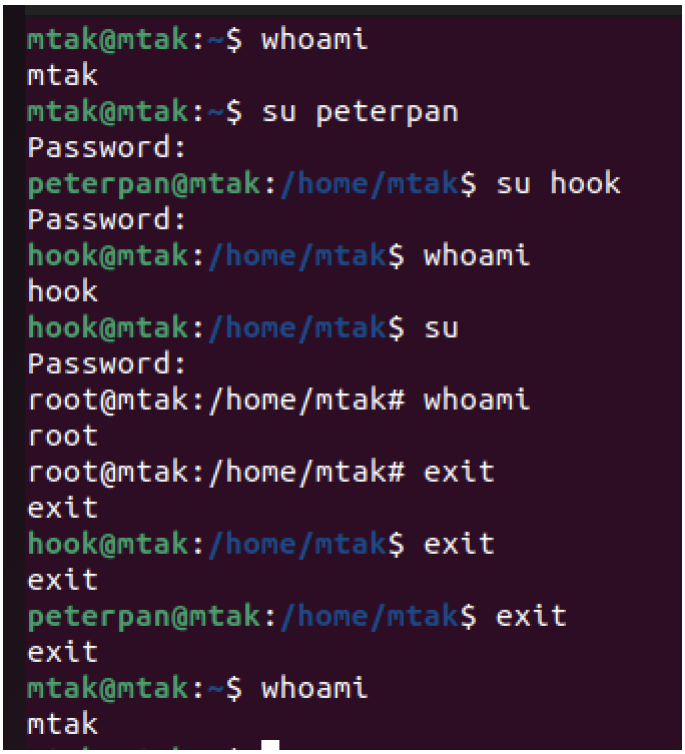
(3) Describe GID and members of new groups (defender, attacker and neverland), UID of new users (peterpan, hook)

tail /etc/group 를 통해 그룹정보를 볼 수 있는데, defender 의 GID 는 1004 입니다. 여기에는 peterpan 이 속해있습니다. attacker 의 GID 는 1006이고, hook 가 속해있다. neverland 의 GID 는 1007이고, 여기에는 hook,peterpan 이 속해있다. tail /etc/passwd 를 통해 유저정보를 알 수 있는데, peterpan 의 UID 는 1003, default GID는 1008, hook 의 UID 는 1004, default GID는 1009 임을 알 수 있습니다.

6. 다음을 따라와보자.

1. Do “clear”, and do “whoami” command,
2. then do “su peterpan” (enter the password),
3. then do “whoami”,
4. then do “su hook” (enter the password),
5. then do “whoami”,
6. then “su” and enter root password (1234),
7. then do “whoami”,
8. then do “exit”,
9. then do “exit”,
10. then do “exit” ,
11. then do “whoami”

(1) Take a screen shot



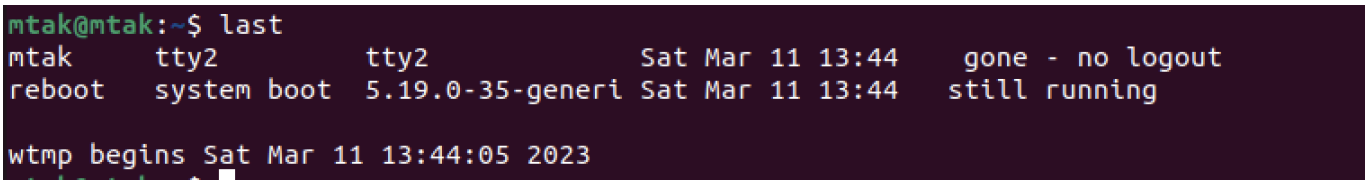
(2) Explain the functionality of “su” and “whoami”

su 명령어는 switch user의 줄임말로 다른 사용자로 변경하는 명령어이다. whoami 는 현재 쉘을 사용하고 있는 유저가 누군지 나타내는 명령어이다.

(3) Explain why three times of doing “exit” is required.

처음에 mtak이였는데 peterpan, hook, root 순으로 유저를 바꾸었다. su로 호출한 후 또 su명령을 실행해서 다른 유저로 바꾸면 바꾸기 전의 쉘은 종료되지 않은 상태로 남으므로 su로 이동한 만큼 exit을 해야 원래 있던 root 쉘으로 돌아오게 된다.

7. Do “last” command, then take a screen shot



Problems

1. Create a new user “wendy”.

(Conditions : “Wendy” is included in two groups, “neverland” and “defender”. The home directory of “Wendy” will be “/home/wendy”, and the shell will be “/bin/bash”.)

(1) List the required commands sequentially, and describe their roles.

1. su 명령어로 root 쉘 실행
2. useradd Wendy -m -d /home/wendy -s /bin/bash -G neverland,defender

- -m 은 user home directory 생성을 하는 명령어.(/home/username) -d가 없으면 username으로 정해진다.
- -d 는 home directory 의 위치를 /home/wendy 로 설정
- -s 는 default login shell 을 /bin/bash 로 설정합니다.
- -G neverland, defender 로 그룹 추가하는 명령어를 실행합니다.

3. passwd wendy 로 비밀번호를 설정합니다.

(2) For validating the operations of the commands, print the contents of “/etc/passwd” file and “/etc/group” file by tail and take the screenshot.

```
root@mtak:/home/mtak# tail /etc/passwd
pulse:x:125:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:126:65534::/run/gnome-initial-setup/:/bin/false
hplip:x:127:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
mtak:x:1000:1000:mtak,,,:/home/mtak:/bin/bash
stack:x:1001:1002::/home/stack:/bin/bash
gslee:x:1002:1004::/home/gslee:/bin/bash
peterpan:x:1003:1008::/home/peterpan:/bin/bash
hook:x:1004:1009::/home/hook:/bin/bash
Wendy:x:1005:1010::/home/wendy:/bin/bash
```

```
root@mtak:/home/mtak# tail /etc/group
admin:x:1001:stack
stack:x:1002:
faculty:x:1003:gslee
gslee:x:1004:
defender:x:1005:peterpan,Wendy
attacker:x:1006:hook
neverland:x:1007:peterpan,hook,Wendy
peterpan:x:1008:
hook:x:1009:
Wendy:x:1010:
```

2. Describe what is /etc/login.defs file, and list the important configuration parameters with simple explanation.

사용자 계정의 설정과 관련된 기본 값을 정의한 파일이다.

명칭	설명
PASS_MAX_DAYS	패스워드 최대 사용일
PASS_MIN_DAYS	패스워드 최소 사용일수
PASS_MIN_LEN	패스워드의 최소 길이
PASS_WARN_AGE	패스워드 만료경고 날짜
UID_MAX	UID 최댓값
UID_MIN	UID 최솟값
GID_MAX	GID 최댓값
GID_MIN	GID 최솟값
ENCRYPT_METHOD	암호화 방식

3.

(1) Create the following 3 users

- tester1 : UID = 2001, default-group = class1
- tester2 : UID = 2003, default-group = class1, other-groups = class2

- tester3 : UID = 2005, default-group = class2, other-groups = class1, class3 To verify the results, print the contents of “/etc/passwd” file and “/etc/group” file by tail and take the screenshot.

```
root@mtak:/home/mtak# tail -3 /etc/group
class1:x:1011:tester3
class2:x:1012:tester2
class3:x:1013:tester3
```

```
root@mtak:/home/mtak# tail -3 /etc/passwd
tester1:x:2001:1011::/home/tester1:/bin/sh
tester2:x:2003:1011::/home/tester2:/bin/sh
tester3:x:2005:1012::/home/tester3:/bin/sh
```

- 내용이 너무 길어 스샷에 안들어가서, 관련된 부분만 잘랐습니다.

(2) Then, set a group password for class2 as “13579”.

After then, switching user to “tester1” (su) and initiating a new session with class2 GID (newgrp). To check the session run “id” command. To verify the results, take the screenshot of this procedure.

```
root@mtak:/home/mtak# gpasswd class2
Changing the password for group class2
New Password:
Re-enter new password:
root@mtak:/home/mtak# su tester1
$ newgrp class2
Password:
$ id
uid=2001(tester1) gid=1012(class2) groups=1012(class2),1011(class1)
$
```

(3) Describe the meaning of the result (1) and (2)

1. /etc/group 에는 보조 그룹으로 속하는 member만 확인할 수 있고, /etc/passwd에는 주 그룹 정보만 확인할 수 있다. 이 때, /etc/passwd에 있는 주그룹 GID의 그룹 이름이 궁금하다면 /etc/group의 세번째 칼럼 값과 같은 row를 찾아 첫 칼럼의 그룹 이름을 확인하거나, `id`명령어로 확인할 수 있다.
2. gpasswd로 그룹의 패스워드를 변경한 후, tester1은 class2 그룹에 속해있지 않음에도 불구하고 class2 그룹으로 로그인하여 (newgrp) 해당 그룹의 권한을 사용할 수 있게 되었다.

4. Describe why “newgrp" command is required. When you can use this command? Provide a scenario for using “newgrp" command.

default group 을 잠깐 바꾸려는데, 기존 default group 으로 쓰던 그룹을 삭제하지 않고 다른 새로운 group 을 default 로 사용하고 싶을 때 사용하게 된다.