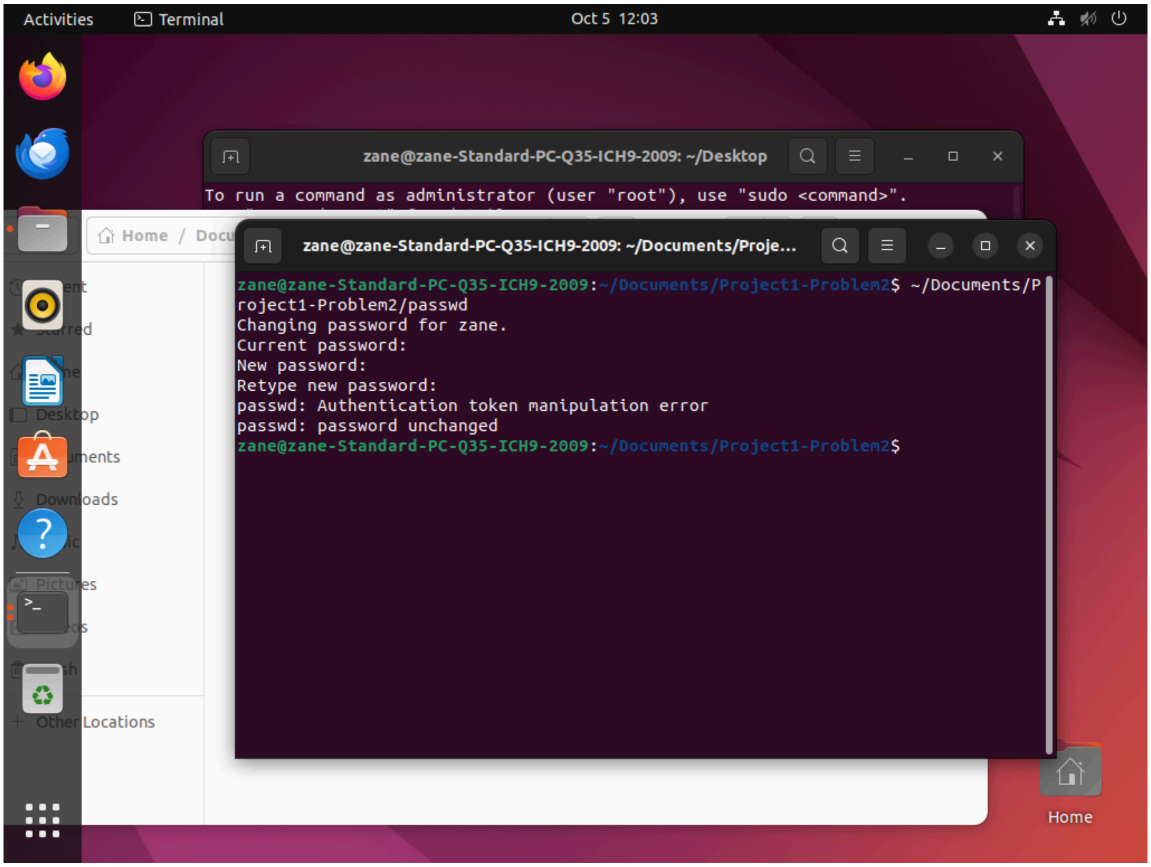
 / COURSE: CS 645 - SECURYITY & PRIVACY IN COMPUTER SYSTEMS
// PROJECT: 1
// TEAM MEMBERS: 2
// MEMBERS: Suraj Kumar Ojha (UCID: so299), Zane Xu (UCID: zx4)

Problem 2

(a)

The screenshot shows the authentication token manipulation error.


Activities
Terminal
Oct 5 12:03
zane@zane-Standard-PC-Q35-ICH9-2009: ~/Desktop
Home / Docu
zane@zane-Standard-PC-Q35-ICH9-2009: ~/Documents/Proje...
Desktop
Downloads
Pictures
Other Locations
Home

```
To run a command as administrator (user "root"), use "sudo <command>".
```

```
zane@zane-Standard-PC-Q35-ICH9-2009:~/Documents/Project1-Problem2$ ~/Documents/P
roject1-Problem2/passwd
Changing password for zane.
Current password:
New password:
Retype new password:
passwd: Authentication token manipulation error
passwd: password unchanged
zane@zane-Standard-PC-Q35-ICH9-2009:~/Documents/Project1-Problem2$
```

When I checked the permission of the copied file, it shows:

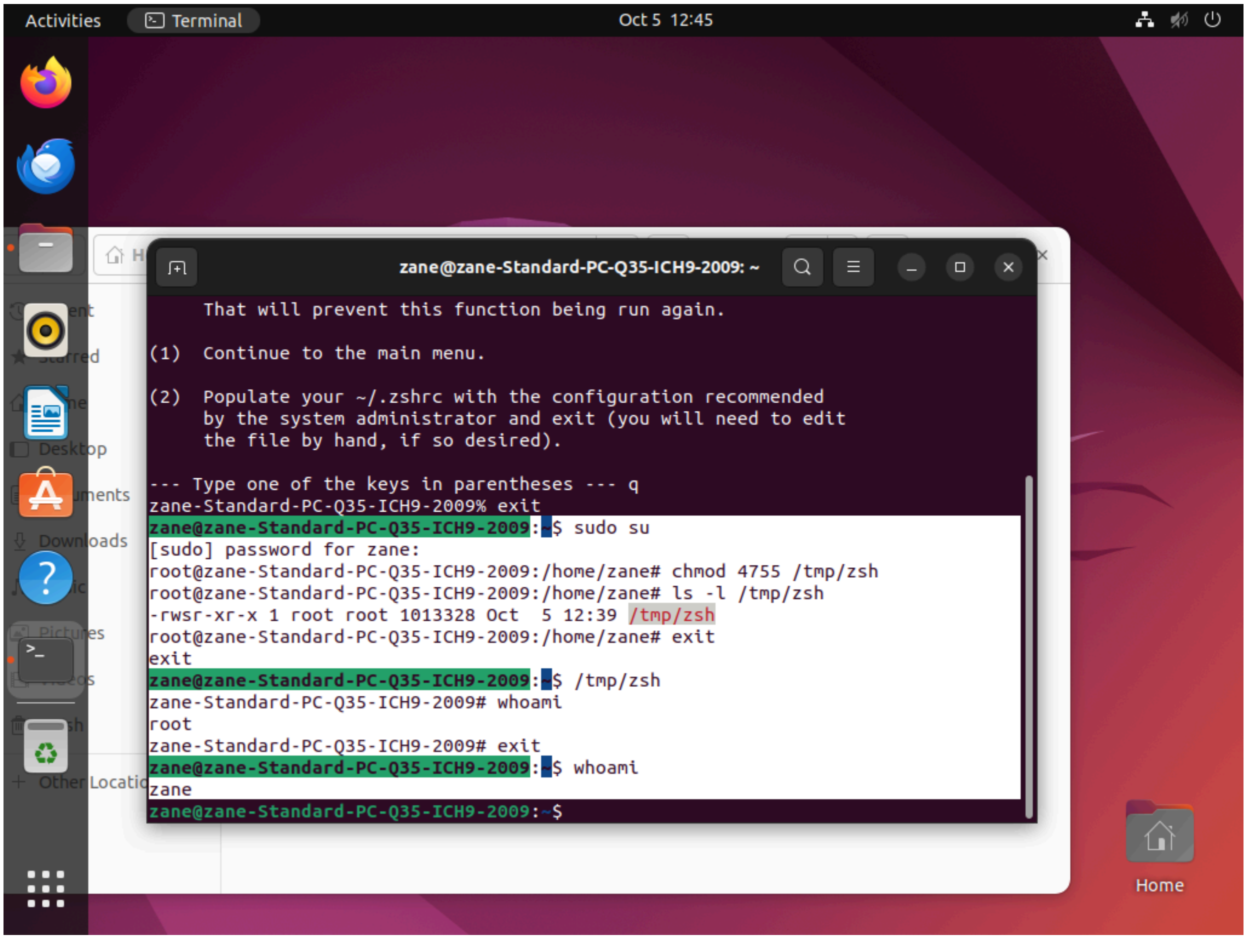
- -rwxr-xr-x 1 zane zane 59976 Oct 5 11:56 /home/zane/Documents/Project1-Problem2/passwd

When I checked the permission of the original file, it shows:

- -rwsr-xr-x 1 root root 59976 Feb 6 2024 /usr/bin/passwd

As a result, the owner becomes me, and it runs as my user “Zane”, so I do not have the privilege to modify /etc/shadow and can not Set-UID.

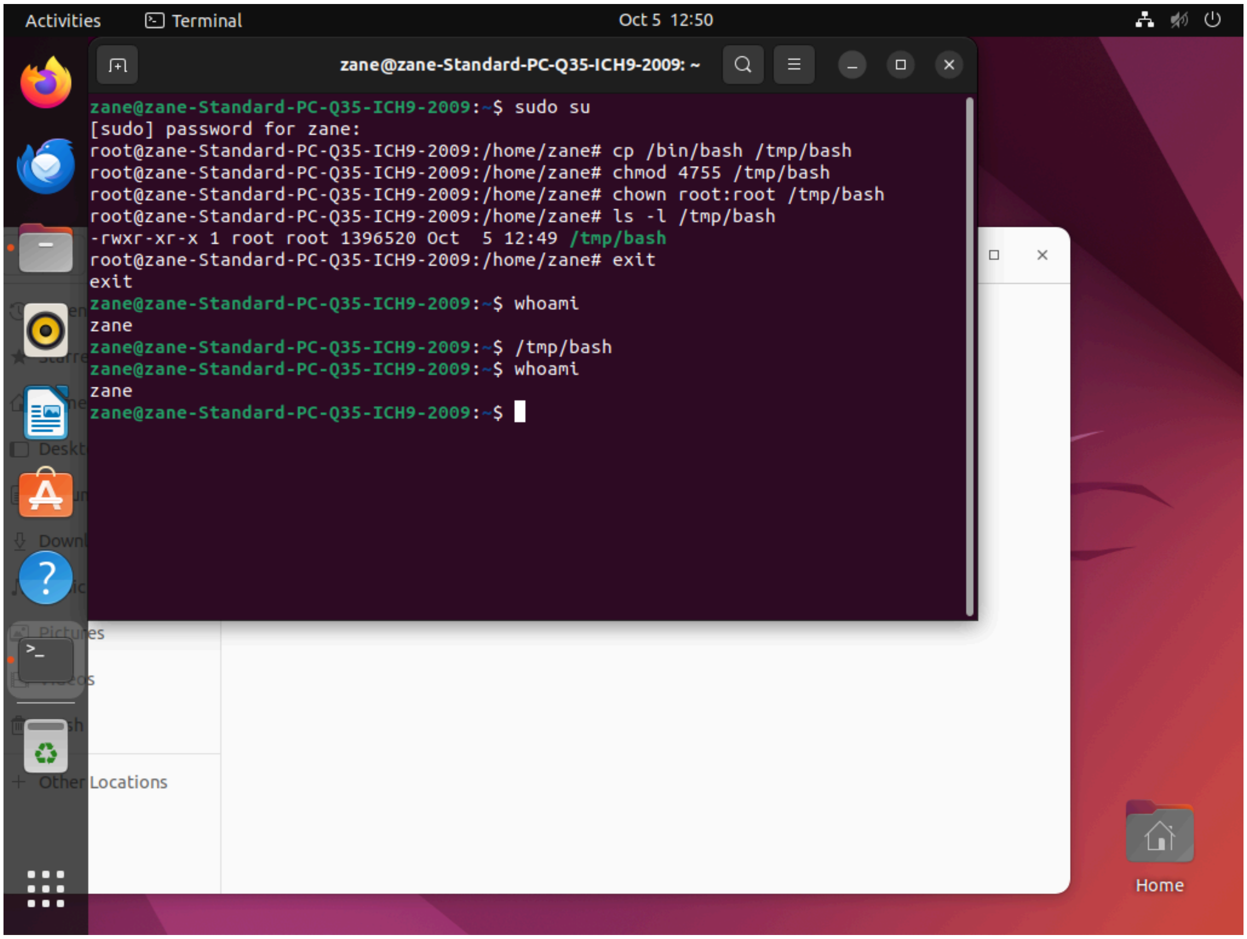
(b1)



```
     That will prevent this function being run again.

(1)  Continue to the main menu.

(2)  Populate your ~/.zshrc with the configuration recommended
     by the system administrator and exit (you will need to edit
     the file by hand, if so desired).

--- Type one of the keys in parentheses --- q
zane-Standard-PC-Q35-ICH9-2009% exit
zane@zane-Standard-PC-Q35-ICH9-2009:~$ sudo su
[sudo] password for zane:
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# chmod 4755 /tmp/zsh
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# ls -l /tmp/zsh
-rwsr-xr-x 1 root root 1013328 Oct  5 12:39 /tmp/zsh
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# exit
exit
zane@zane-Standard-PC-Q35-ICH9-2009:~$ /tmp/zsh
zane-Standard-PC-Q35-ICH9-2009# whoami
root
zane-Standard-PC-Q35-ICH9-2009# exit
zane@zane-Standard-PC-Q35-ICH9-2009:~$ whoami
zane
zane@zane-Standard-PC-Q35-ICH9-2009:~$
```

When I log in /tmp/zsh, I still have root privilege, which is a security vulnerability.

(b2)



```
zane@zane-Standard-PC-Q35-ICH9-2009:~$ sudo su
[sudo] password for zane:
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# cp /bin/bash /tmp/bash
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# chmod 4755 /tmp/bash
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# chown root:root /tmp/bash
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# ls -l /tmp/bash
-rwxr-xr-x 1 root root 1396520 Oct  5 12:49 /tmp/bash
root@zane-Standard-PC-Q35-ICH9-2009:/home/zane# exit
exit
zane@zane-Standard-PC-Q35-ICH9-2009:~$ whoami
zane
zane@zane-Standard-PC-Q35-ICH9-2009:~$ /tmp/bash
zane@zane-Standard-PC-Q35-ICH9-2009:~$ whoami
zane
zane@zane-Standard-PC-Q35-ICH9-2009:~$
```

When I log in /tmp/bash, I do not have the privilege.

When bash starts up, it compares its real UID with its effective UID. If they are different, bash will drop root privilege and run with user privilege, which is safer.

(C1)

No, it is not a good idea. Because the Set-UID program uses the system("ls"), and a user can provide a malicious ls here, a regular user can cause the Set-UID program to execute attacker code with root privileges. The user can implement the command “cp /etc/shadow /tmp/shadow_copy”, after that, we can read “/etc/shadow”.

The result:

cat /tmp/shadow_copy
root:!:20366:0:99999:7:::

```
daemon:*:19977:0:99999:7:::
bin:*:19977:0:99999:7:::
sys:*:19977:0:99999:7:::
sync:*:19977:0:99999:7:::
games:*:19977:0:99999:7:::
man:*:19977:0:99999:7:::
lp:*:19977:0:99999:7:::
mail:*:19977:0:99999:7:::
news:*:19977:0:99999:7:::
uucp:*:19977:0:99999:7:::
proxy:*:19977:0:99999:7:::
www-data:*:19977:0:99999:7:::
backup:*:19977:0:99999:7:::
list:*:19977:0:99999:7:::
irc:*:19977:0:99999:7:::
gnats:*:19977:0:99999:7:::
nobody:*:19977:0:99999:7:::
systemd-network:*:19977:0:99999:7:::
systemd-resolve:*:19977:0:99999:7:::
messagebus:*:19977:0:99999:7:::
systemd-timesync:*:19977:0:99999:7:::
syslog:*:19977:0:99999:7:::
_apt:*:19977:0:99999:7:::
tss:*:19977:0:99999:7:::
uuidd:*:19977:0:99999:7:::
systemd-oom:*:19977:0:99999:7:::
tcpdump:*:19977:0:99999:7:::
avahi-autoipd:*:19977:0:99999:7:::
usbmux:*:19977:0:99999:7:::
dnsmasq:*:19977:0:99999:7:::
kernoops:*:19977:0:99999:7:::
avahi:*:19977:0:99999:7:::
cups-pk-helper:*:19977:0:99999:7:::
rtkit:*:19977:0:99999:7:::
whoopsie:*:19977:0:99999:7:::
sssd:*:19977:0:99999:7:::
speech-dispatcher:!:19977:0:99999:7:::
fwupd-refresh:*:19977:0:99999:7:::
nm-openvpn:*:19977:0:99999:7:::
saned:*:19977:0:99999:7:::
colord:*:19977:0:99999:7:::
geoclue:*:19977:0:99999:7:::
pulse:*:19977:0:99999:7:::
gnome-initial-setup:*:19977:0:99999:7:::
```

```
hplip:*:19977:0:99999:7:::
gdm:*:19977:0:99999:7:::
zane:$y$j9T$8g.FK9SGhfDfbb9B6tWy8/$yEaC77DTNPmhg34B2GM6g04P0zuUx5krwcY9RgA
DOn7:20366:0:99999:7:::
```

(C2)

No, I can not generate the copied file later. When bash starts up, it compares its real UID with its effective UID. If they are different, bash will drop root privilege and sanitize the environment, which makes sure the user’s modification on PATH will not take effect.

(C3)

```
Linux zane-Standard-PC-Q35-ICH9-2009 6.8.0-85-generic #85~22.04.1-Ubuntu SMP
PREEMPT_DYNAMIC Fri Sep 19 16:18:59 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
```