Homework 2
One Liner Script & System Info

hslin, cwang, xizhen

國立陽明交通大學資工系資訊中心

Computer Center of Department of Computer Science, NYCU

HW 2-1: One liner script (40%)

國立陽明交通大學資工系資訊中心

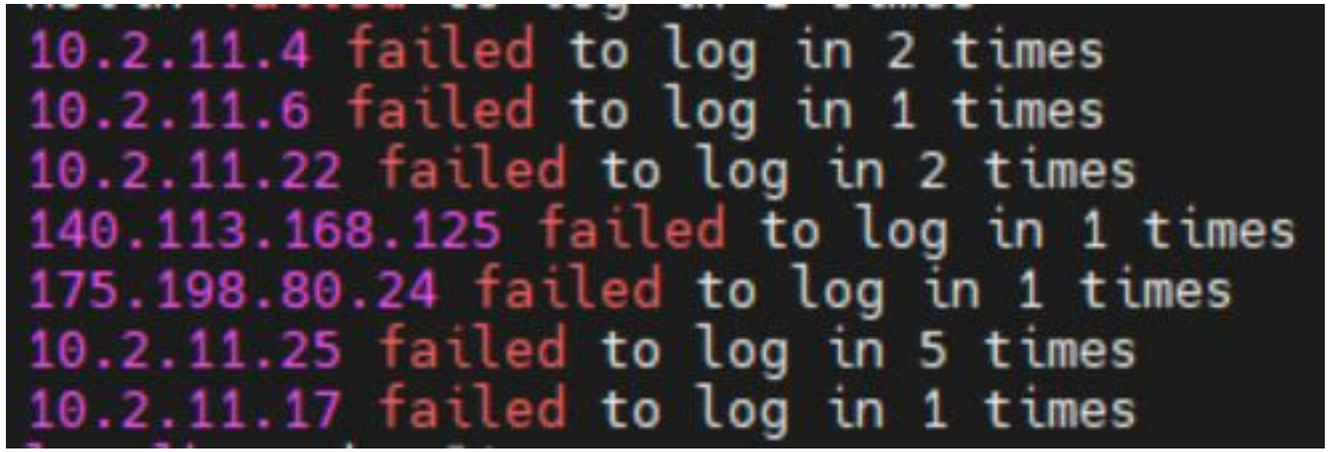
Computer Center of Department of Computer Science, NYCU

HW 2-1: One liner script (40%)

- Use shell script to analyze the content of **auth.log (secure)** and output three files:
  - **audit_ip.txt**: List the source IPs that ssh login failed and count the number of login failed times.
  - **audit_sudo.txt**: List the commands and users who used `sudo`.
  - **audit_user.txt**: List the users who ssh login failed and count the number of login failed times. (Users who in the system)

HW 2-1: One liner script (40%)

- **audit_ip.txt**: List the source IPs that ssh login failed and count the number of login failed times. (10%)



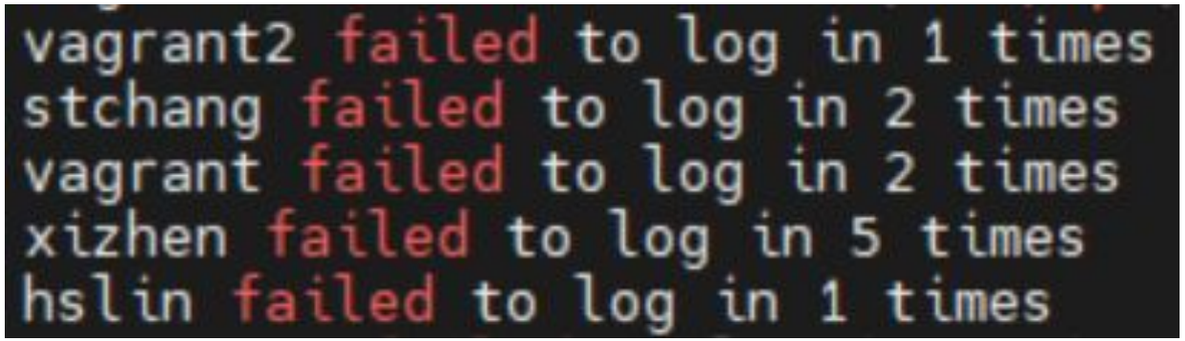
HW 2-1: One liner script (40%)

- **audit_sudo.txt:** List the commands and users who used `sudo`. (20%)

```
xizhen used sudo to do `/bin/nmcli connection modify ens192 IPv4.address 10.2.4.7/32` on Sep 23 16:16:32
xizhen used sudo to do `/bin/systemctl restart network.service` on Sep 23 16:22:26
xizhen used sudo to do `/bin/systemctl restart NetworkManage` on Sep 23 16:22:47
xizhen used sudo to do `/bin/nmtui edit ens192` on Sep 23 16:29:59
xizhen used sudo to do `/bin/vim /etc/sysconfig/network-scripts/ifcfg-ens192` on Sep 23 16:59:19
xizhen used sudo to do `/bin/nmcli connection down ens192` on Sep 23 17:00:21
xizhen used sudo to do `/bin/nmtui` on Sep 23 17:10:32
vagrant used sudo to do `/bin/cat /var/log/secure` on Sep 23 17:12:46
vagrant used sudo to do `/bin/cp /var/log/secure /vagrant/hw2` on Sep 23 17:14:15
```

HW 2-1: One liner script (40%)

- **audit_user.txt**: List the users who ssh login failed and count the number of login failed times. (Users who in the system) (10%)



HW 2-1: One liner script (40%)

- Your script is limited to one line and outputs 3 files.
- **Must not** use the following commands:
  - Subshell for grouping: ***(…)***
  - Command substitution: ***$(…)*** also spelled ***`…`***
  - Process substitution: ***<(…)*** or ***>(…)***
  - ***tee***, ***sh***, ***bash***, ***csh***, ***base64***, ***eval***
  - ***;***, ***&&***, ||
- Temporary files are not allowed.
- Only use > to redirect output to file once.

HW 2-1: One liner script (40%)

- Must not use shell variables.
- Must not call network tools (such as curl, wget...)
- Must not call interpreters or compiler (such as Python, Ruby…).
- Only one shell, sh, are allowed.
- If you are not sure whether a tool is allowed, please ask TA on Google group.
- Your script must start with

FreeBSD: ***cat /var/log/auth.log |***

CentOS: ***cat /var/log/secure |***

HW 2-1: One liner script (40%)

- Bonus (10%):
  - Convert the date format of audit_sudo.txt. (5%)
    - Example: **Sep 23 16:16:32 → 2021-09-23 16:16:32**

```
xizhen used sudo to do `/bin/nmcli connection modify ens192 IPv4.address 10.2.4.7/32` on 2021-09-23 16:16:32
xizhen used sudo to do `/bin/systemctl restart network.service` on 2021-09-23 16:22:26
xizhen used sudo to do `/bin/systemctl restart NetworkManage` on 2021-09-23 16:22:47
xizhen used sudo to do `/bin/nmtui edit ens192` on 2021-09-23 16:29:59
xizhen used sudo to do `/bin/vim /etc/sysconfig/network-scripts/ifcfg-ens192` on 2021-09-23 16:59:19
xizhen used sudo to do `/bin/nmcli connection down ens192` on 2021-09-23 17:00:21
xizhen used sudo to do `/bin/nmtui` on 2021-09-23 17:10:32
vagrant used sudo to do `/bin/cat /var/log/secure` on 2021-09-23 17:12:46
vagrant used sudo to do `/bin/cp /var/log/secure /vagrant/hw2` on 2021-09-23 17:14:15
```

  - If you can finish homework 2-1 without awk, please email ta@nasa.cs.nctu.edu.tw (5%)

HW 2-1: Sample log

- FreeBSD : https://reurl.cc/vgmnak
- CentOS : https://reurl.cc/0x6zvK

HW 2-2: System Info Panel (60%)

Freebsd: Dialog (1)

DIALOG(1) General Commands Manual DIALOG(1)

NAME

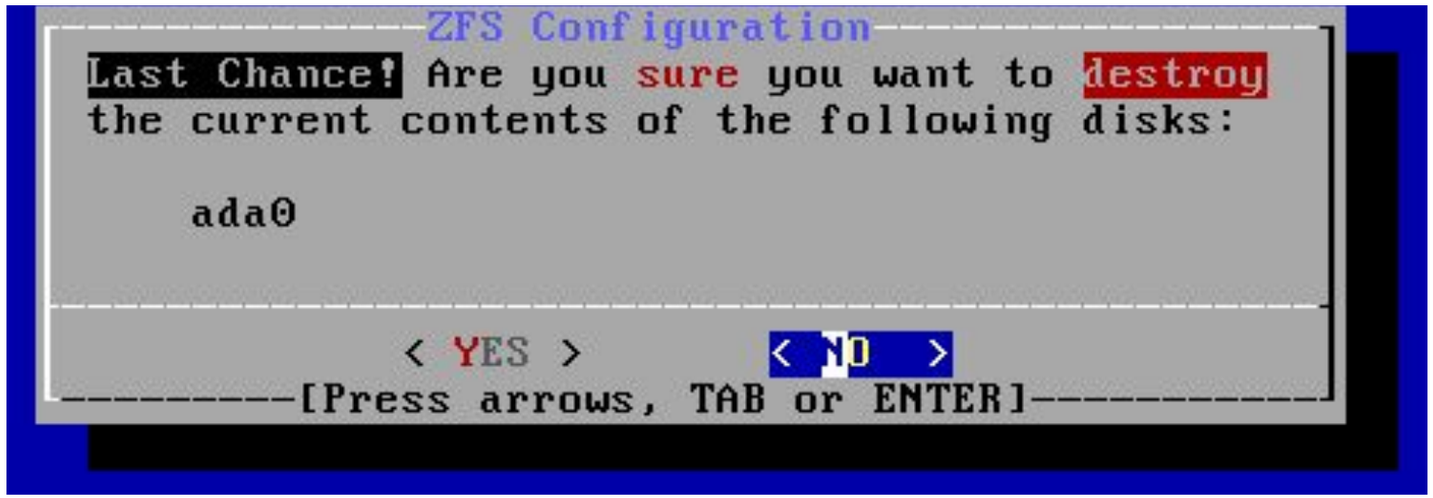
dialog - display dialog boxes from shell scripts

DESCRIPTION

Dialog is a program that will let you to present a variety of questions or display messages using dialog boxes from a shell script.

Freebsd: Dialog (1) - Example 1

Freebsd: Dialog (1) - Example 2



System Info Panel

- You are a System Admin
- You decided to develop a text-based user interface (TUI) program to help you manage the system
- It comes with several functions
  - After selecting one, use dialog(1) to show system information
  - It has to be beautiful. It has to be formatted output but raw output

Ref.

- Use flow: https://bit.ly/39HB6zu
- Video: https://bit.ly/3zUwJf9

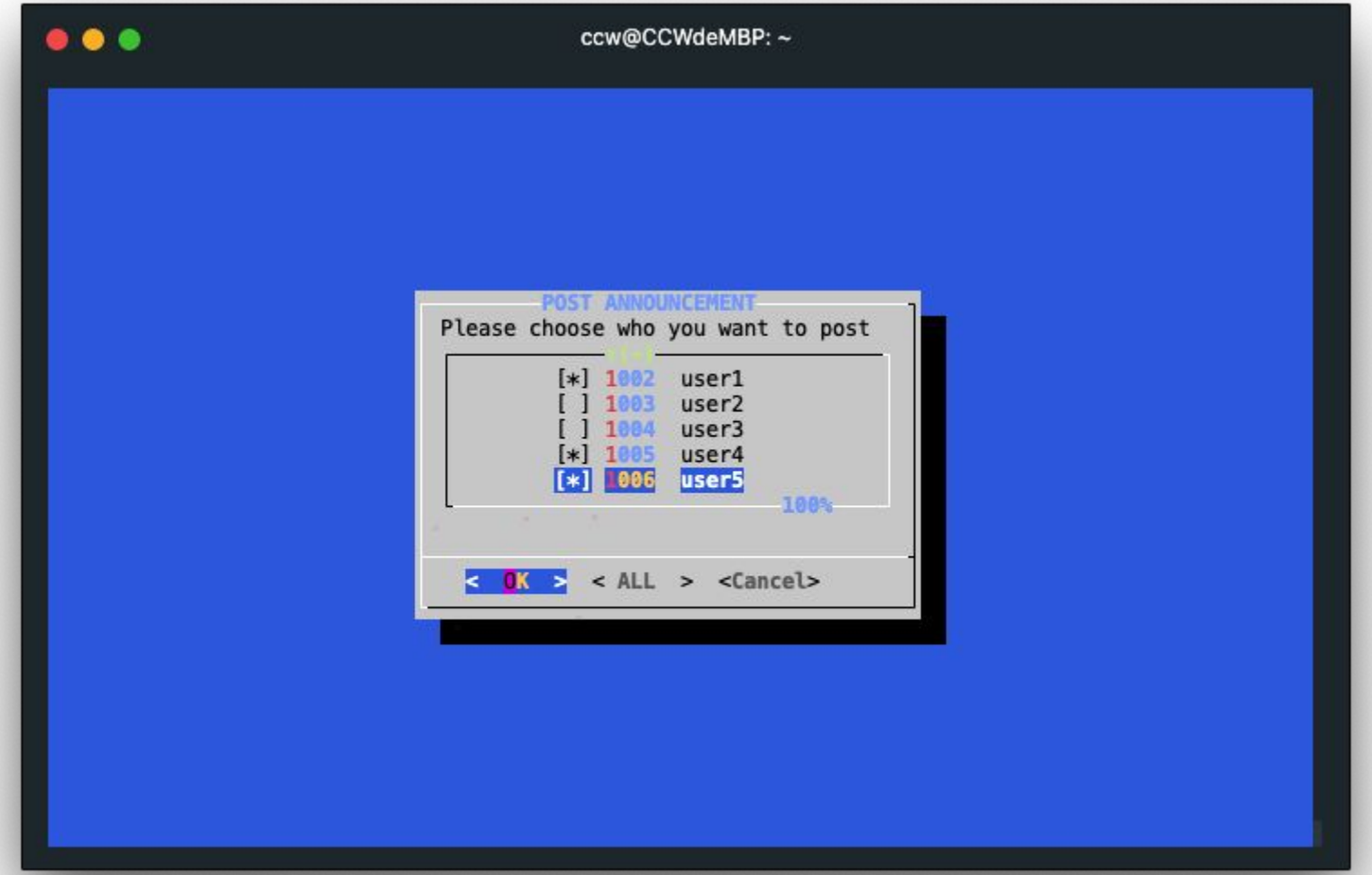
Announcement

- Page - 5%
  - Entrance: show “Announcement” and “Users” two options.
  - User list: list all loginable user, and multi select.
  - Input message
  - You need make use flow here. (follow P.16)
- You can send broadcast message to specify users - 5%

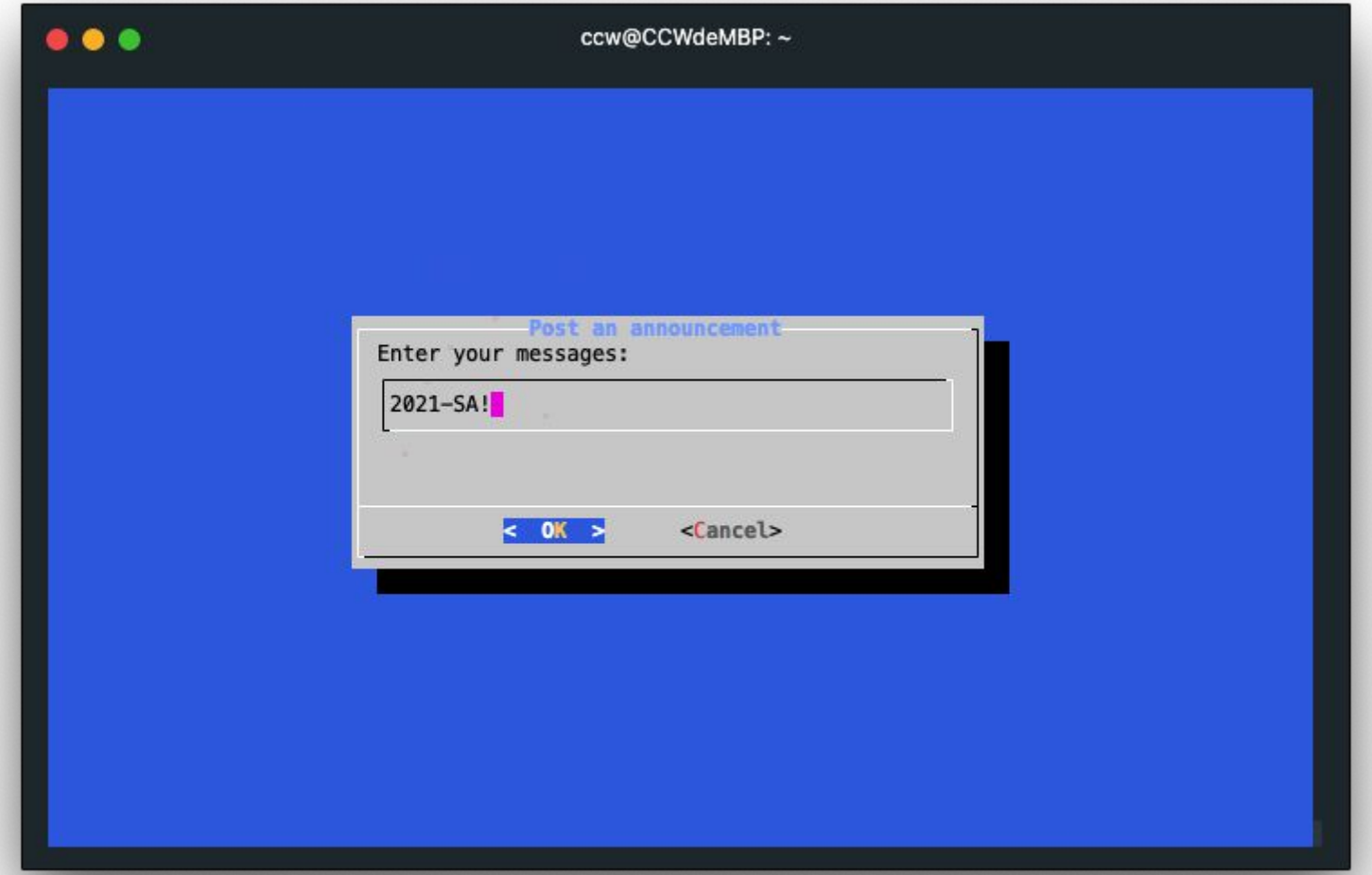
Hint:

- /etc/passwd

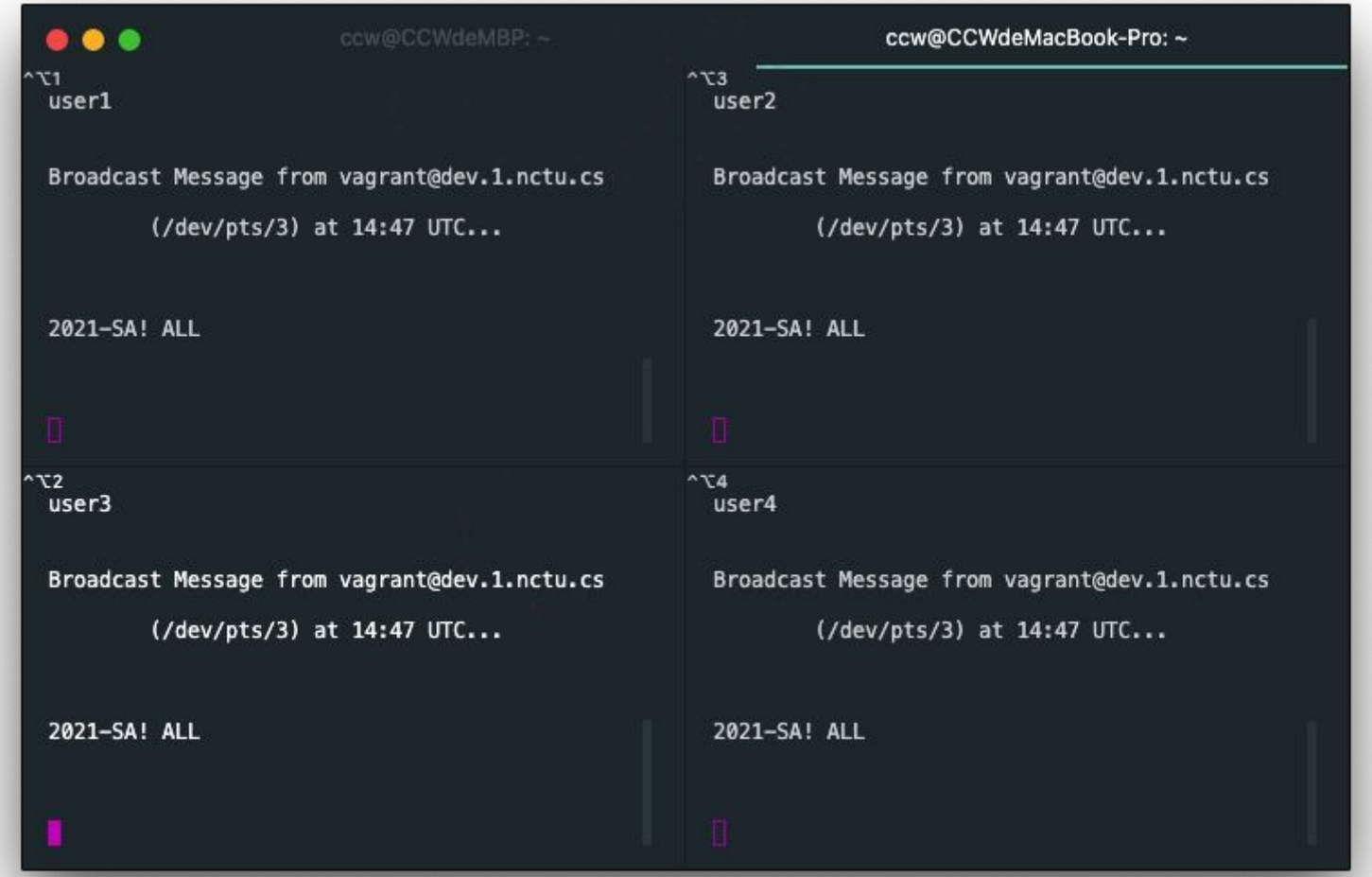
Announcement



Announcement



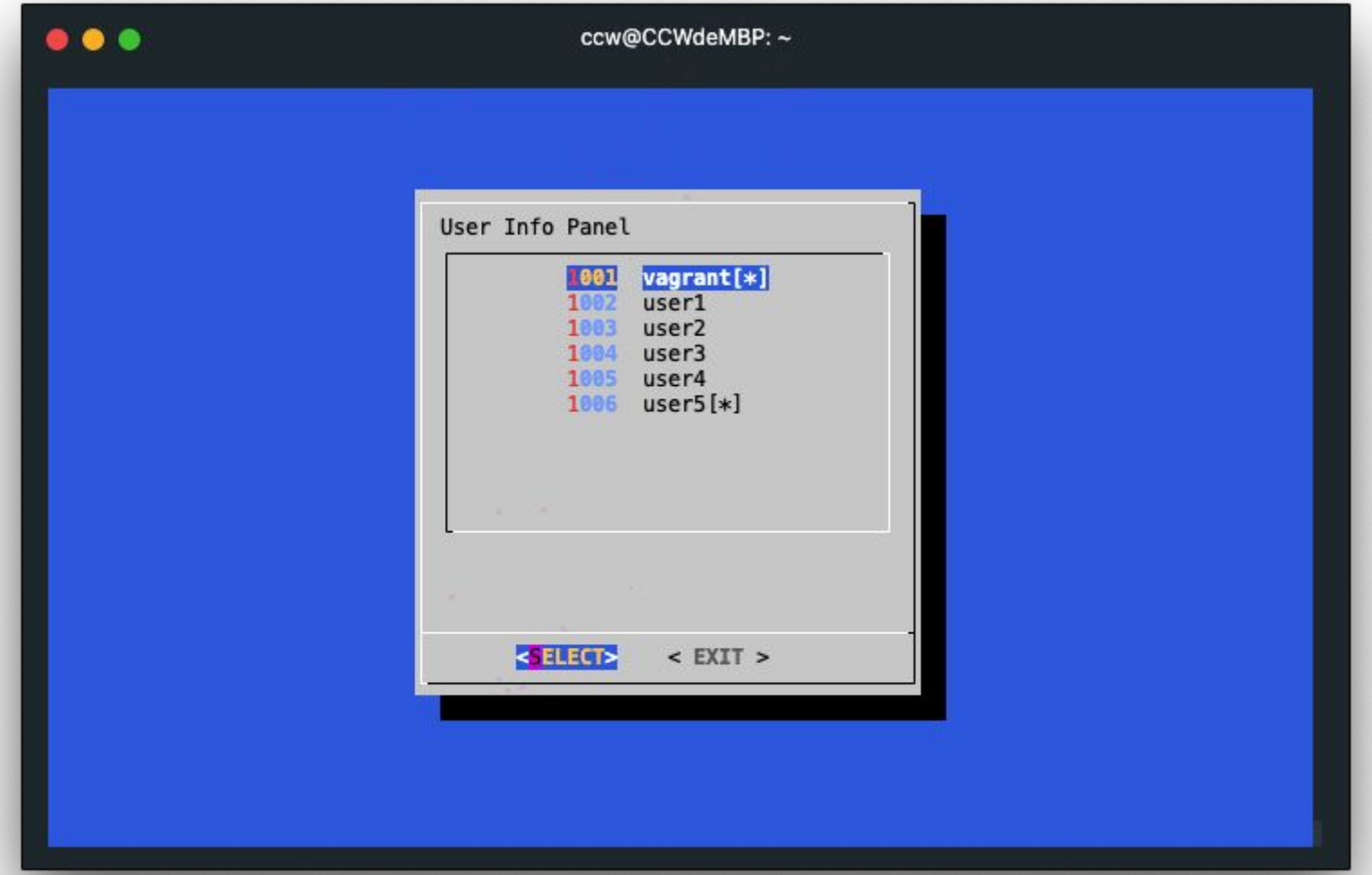
Announcement - Type Msg (Cont.)



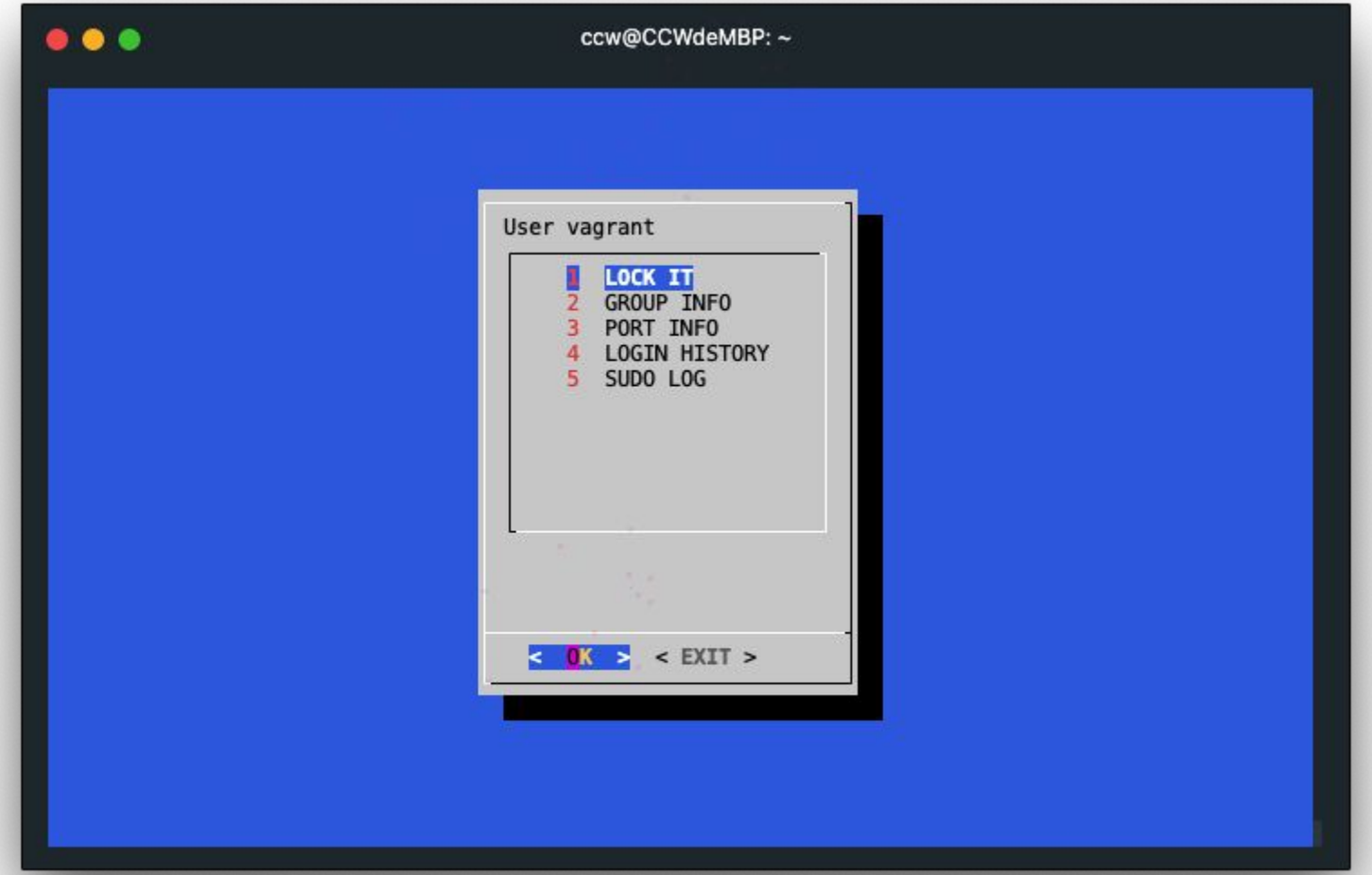
Users

- Page - 6%
  - User List: list all loginable user, and mark online user with star.
    - Hint: `who`
  - User Action: display groups, ports, login history, sudo log, block user, total 5 options.

User List


ccw@CCWdeMBP: ~
User Info Panel
1001 vagrant[*]
1002 user1
1003 user2
1004 user3
1005 user4
1006 user5[*]
<SELECT>
< EXIT >

User Action


ccw@CCWdeMBP: ~
User vagrant
1 LOCK IT
2 GROUP INFO
3 PORT INFO
4 LOGIN HISTORY
5 SUDO LOG
< OK >
< EXIT >

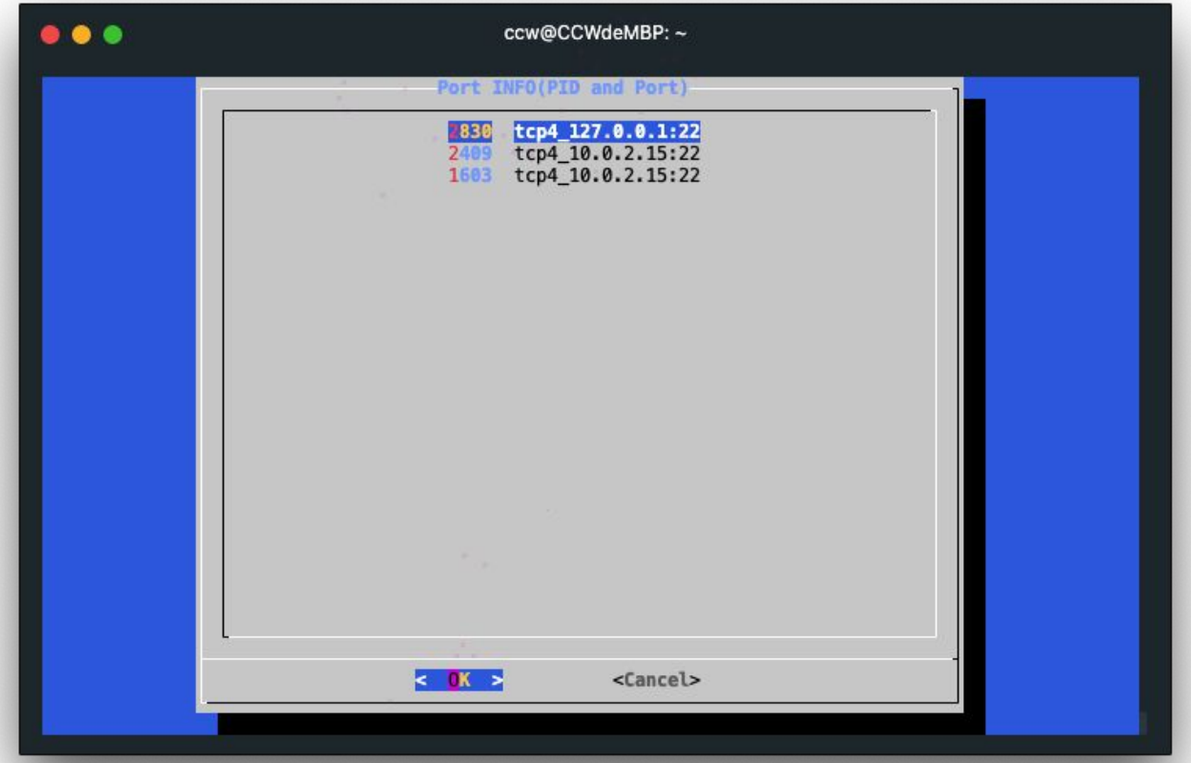
Groups (5%)

- List groups that specify user belongs to.
- Need group id and group name column.

Hint: `groups`

Ports (5%)

- List specify user used port listening on tcp and udp
  - List only ipv4
- Can get port detail info in next page
- If the list is too long, make it scrollable



Hint: [sockstat (1)]

Ports

- Each port is used by one process.
- Get process detail that specify port used.

Hint: `ps`

Lock / Unlock (10%)

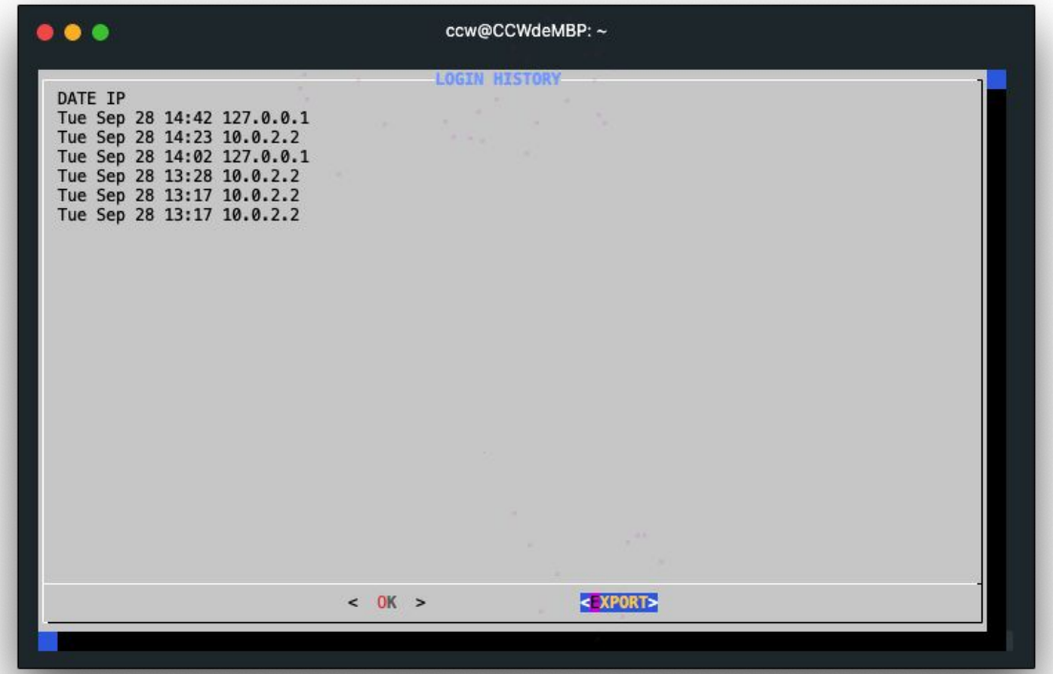
- Lock (or unlock) user login.
- When specify user already lock, then options in User Action page show “unlock” text.

Hint: `pw`

Login History (5%)

- Show specify user login history
- Recently 10 times login history
  - datetime, login ip

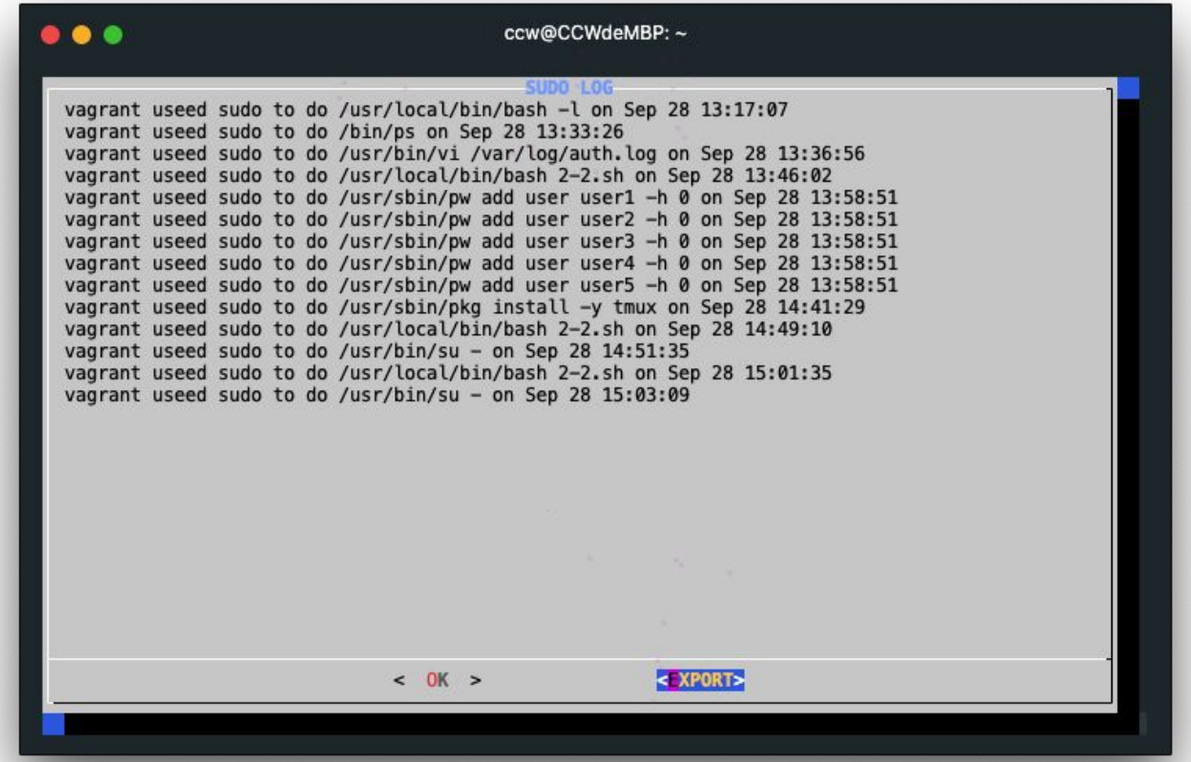
Hint: `last(1)`



Sudo Log (5%)

- Show specify user sudo command usage log.
- Show recent 30 days log.

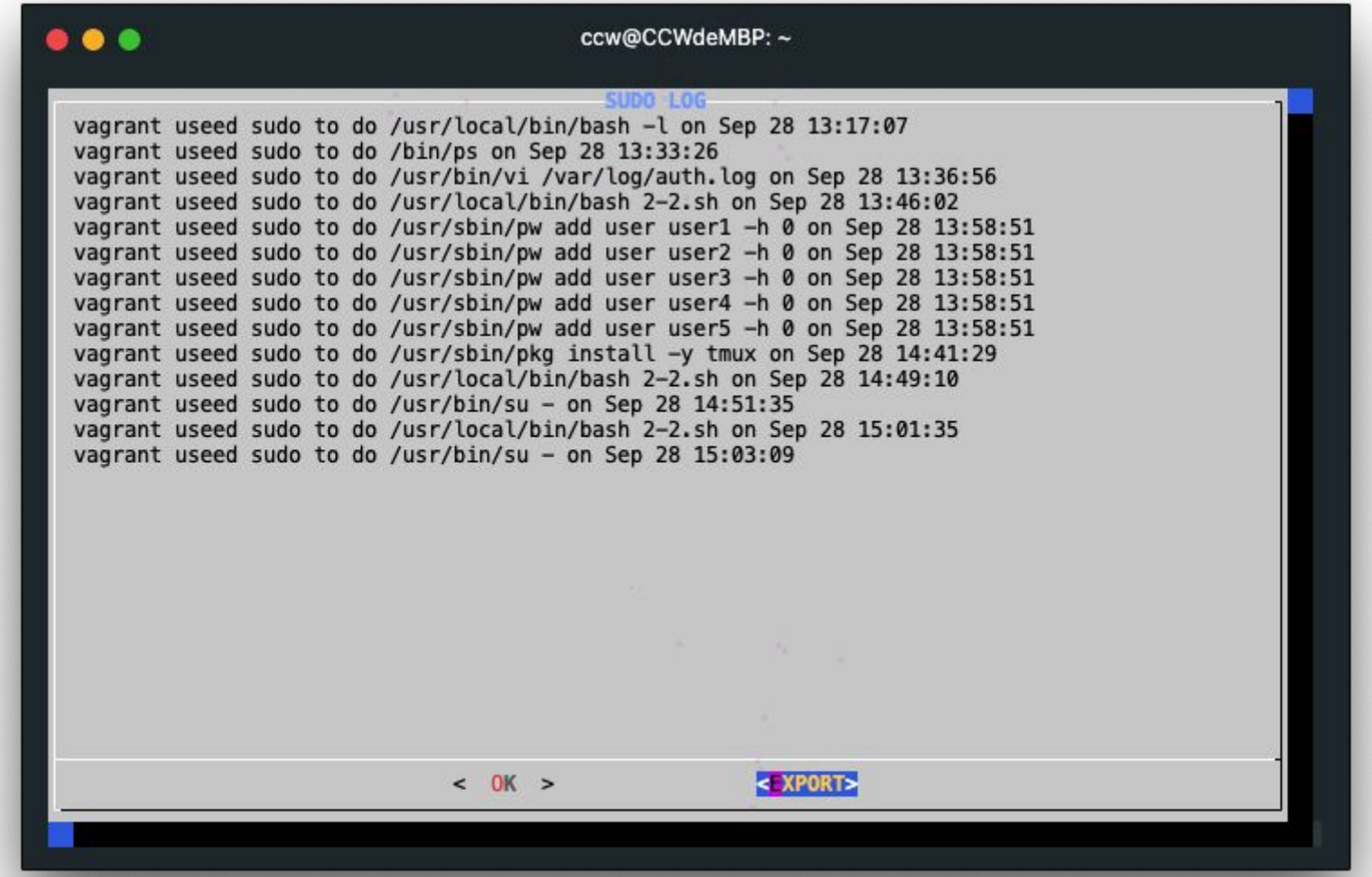
Hint: auth.log



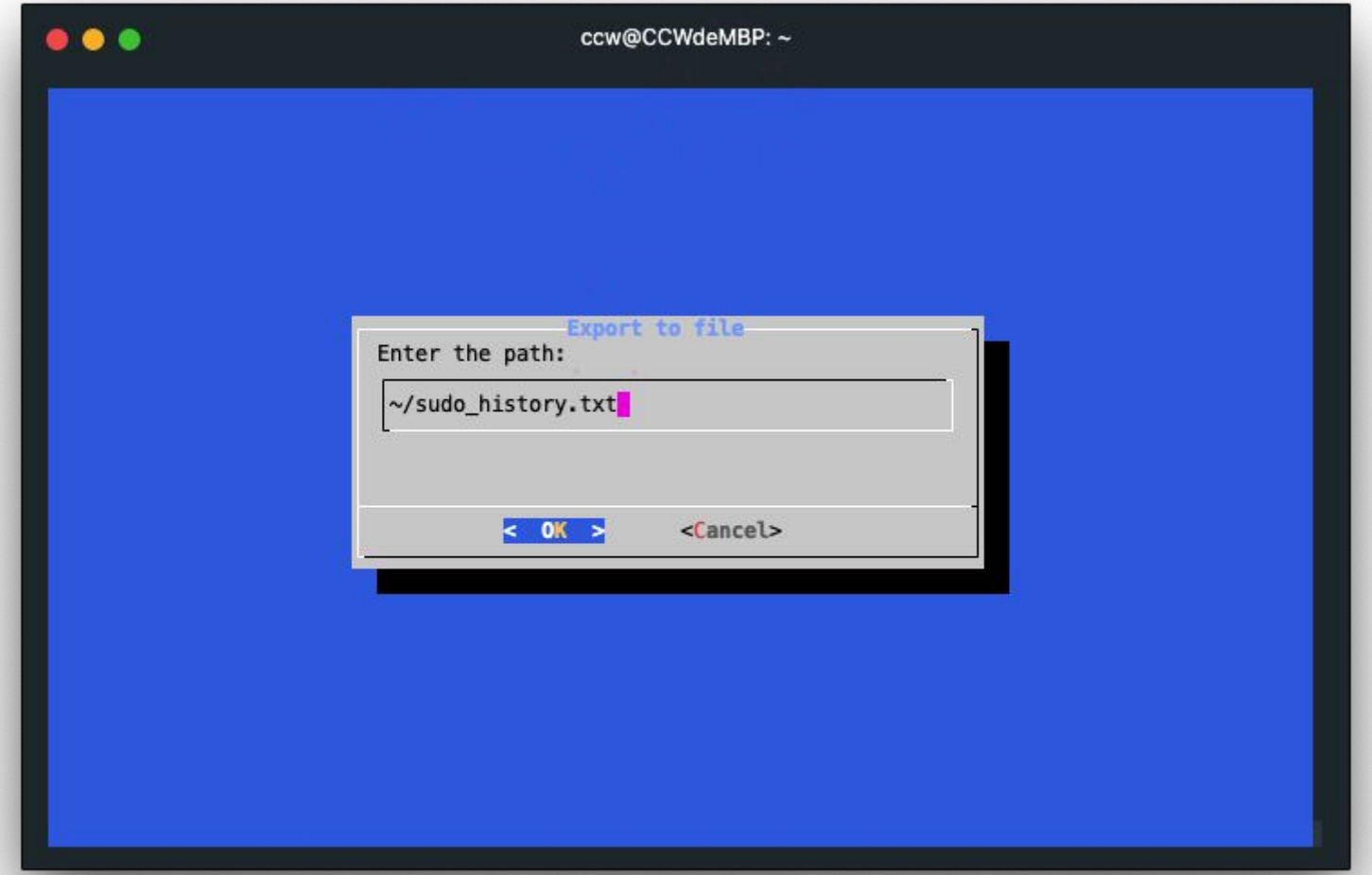
Export (10%)

- Export dialog text into file
- Use dialog to ask user on where to save and save the output to file
  - User could input absolute path or relative path based on user's home directory
    - e.g. res -> /u/gcs/109/309551019/res
- Export button in each info page (group, port, sudo log, login history)

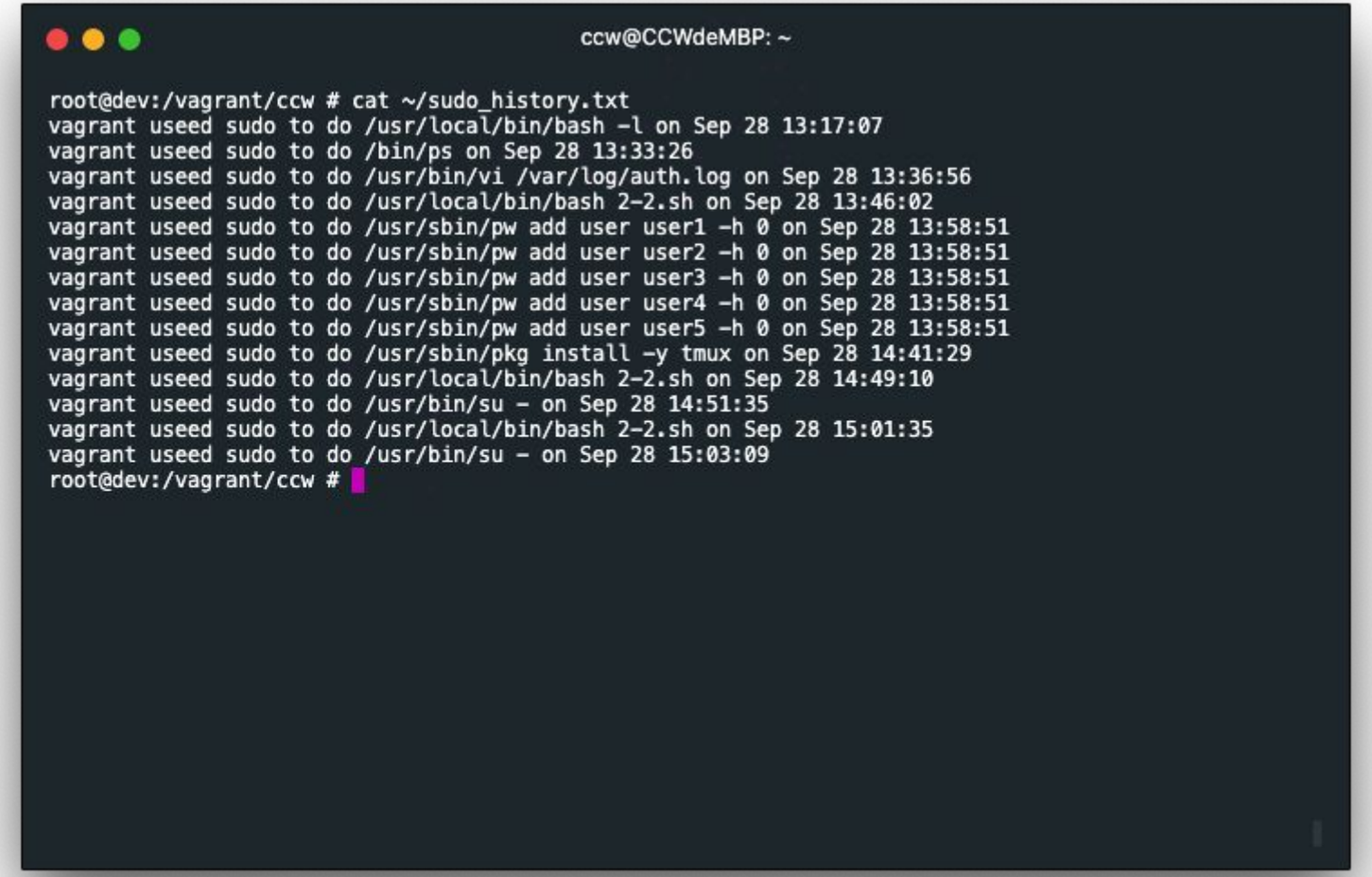
Export


ccw@CCWdeMBP: ~
SUDO LOG
vagrant useed sudo to do /usr/local/bin/bash -l on Sep 28 13:17:07
vagrant useed sudo to do /bin/ps on Sep 28 13:33:26
vagrant useed sudo to do /usr/bin/vi /var/log/auth.log on Sep 28 13:36:56
vagrant useed sudo to do /usr/local/bin/bash 2-2.sh on Sep 28 13:46:02
vagrant useed sudo to do /usr/sbin/pw add user user1 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user2 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user3 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user4 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user5 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pkg install -y tmux on Sep 28 14:41:29
vagrant useed sudo to do /usr/local/bin/bash 2-2.sh on Sep 28 14:49:10
vagrant useed sudo to do /usr/bin/su - on Sep 28 14:51:35
vagrant useed sudo to do /usr/local/bin/bash 2-2.sh on Sep 28 15:01:35
vagrant useed sudo to do /usr/bin/su - on Sep 28 15:03:09
< OK >
<EXPORT>

Export


ccw@CCWdeMBP: ~
Export to file
Enter the path:
~/sudo_history.txt
< OK >
<Cancel>

Export

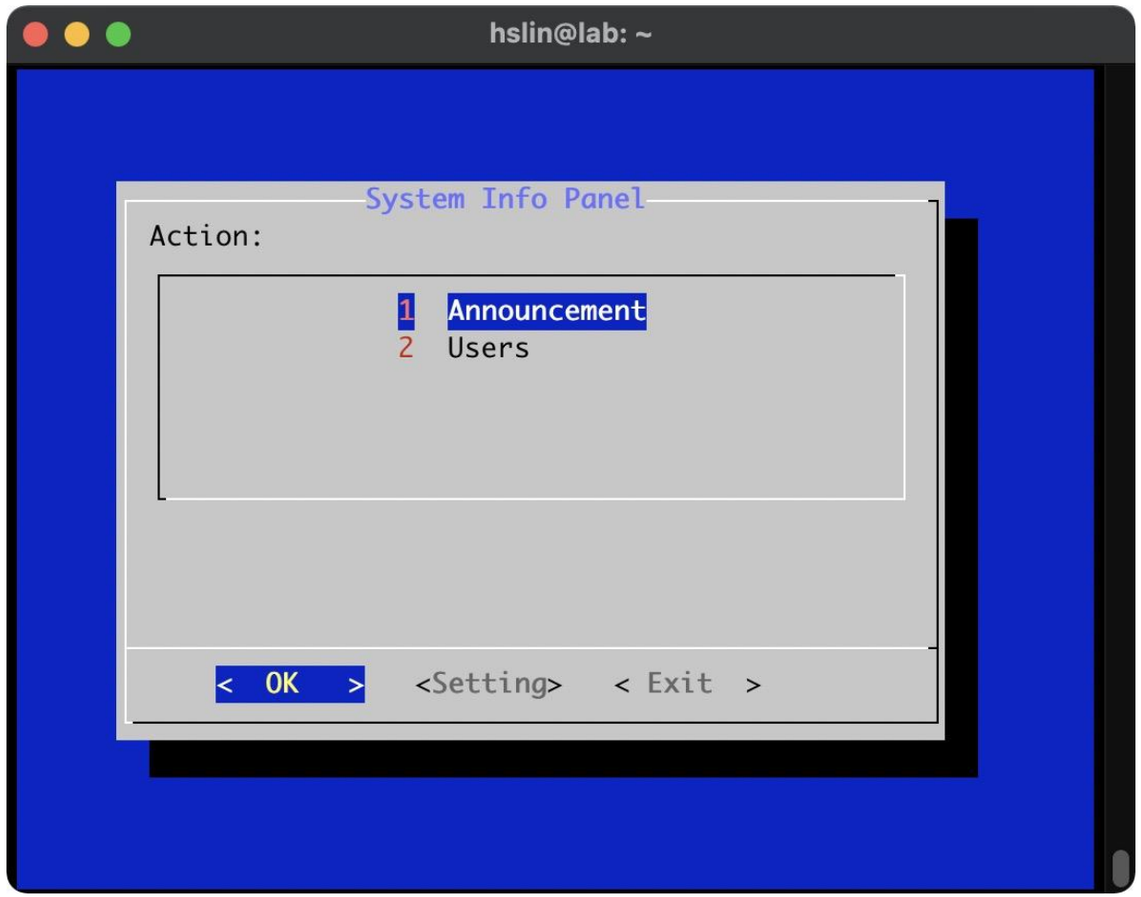

ccw@CCWdeMBP: ~
root@dev:/vagrant/ccw # cat ~/sudo_history.txt
vagrant useed sudo to do /usr/local/bin/bash -l on Sep 28 13:17:07
vagrant useed sudo to do /bin/ps on Sep 28 13:33:26
vagrant useed sudo to do /usr/bin/vi /var/log/auth.log on Sep 28 13:36:56
vagrant useed sudo to do /usr/local/bin/bash 2-2.sh on Sep 28 13:46:02
vagrant useed sudo to do /usr/sbin/pw add user user1 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user2 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user3 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user4 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pw add user user5 -h 0 on Sep 28 13:58:51
vagrant useed sudo to do /usr/sbin/pkg install -y tmux on Sep 28 14:41:29
vagrant useed sudo to do /usr/local/bin/bash 2-2.sh on Sep 28 14:49:10
vagrant useed sudo to do /usr/bin/su - on Sep 28 14:51:35
vagrant useed sudo to do /usr/local/bin/bash 2-2.sh on Sep 28 15:01:35
vagrant useed sudo to do /usr/bin/su - on Sep 28 15:03:09
root@dev:/vagrant/ccw #

Return Code (4%)

- Program Return codes and stdout:
  - 0 for cancel (program successfully finished)
    - echo Exit. to stdout
  - 1 for Esc
    - echo Esc pressed. to stderr
  - 2 for Ctrl + C
    - echo Ctrl + C pressed. to stdout

System Info Panel - Bonus (5%)

- If user login fail >= 3, auto lock this user
  - Enable / Disable this feature in “system info panel” setting



System Info Panel - Grading

- Each page & control flow (11%) - This is required.
- Post an announcement to online users (5%)
- User
  - Get this user's group (5%)
  - Query the port used by this user (5%)
    - And get process (used port) detail
  - User login history (5%)
  - Sudo usage log (5%)
  - BLOCK / UNBLOCK this user (10%)
- Return Code (4%)
- EXPORT the information of each page (10%)

Attention!

- You are restricted to use only sh to complete your work
  - That is, no other shell and no other programming language.
  - If you're not sure what's allowed, contact TAs.
  - TAs reserve the right of final explanations. Specs are subject to change without notice.
- Your output does not have to be exactly the same as mine.
  - You could design your own ways the information is presented in as you please.

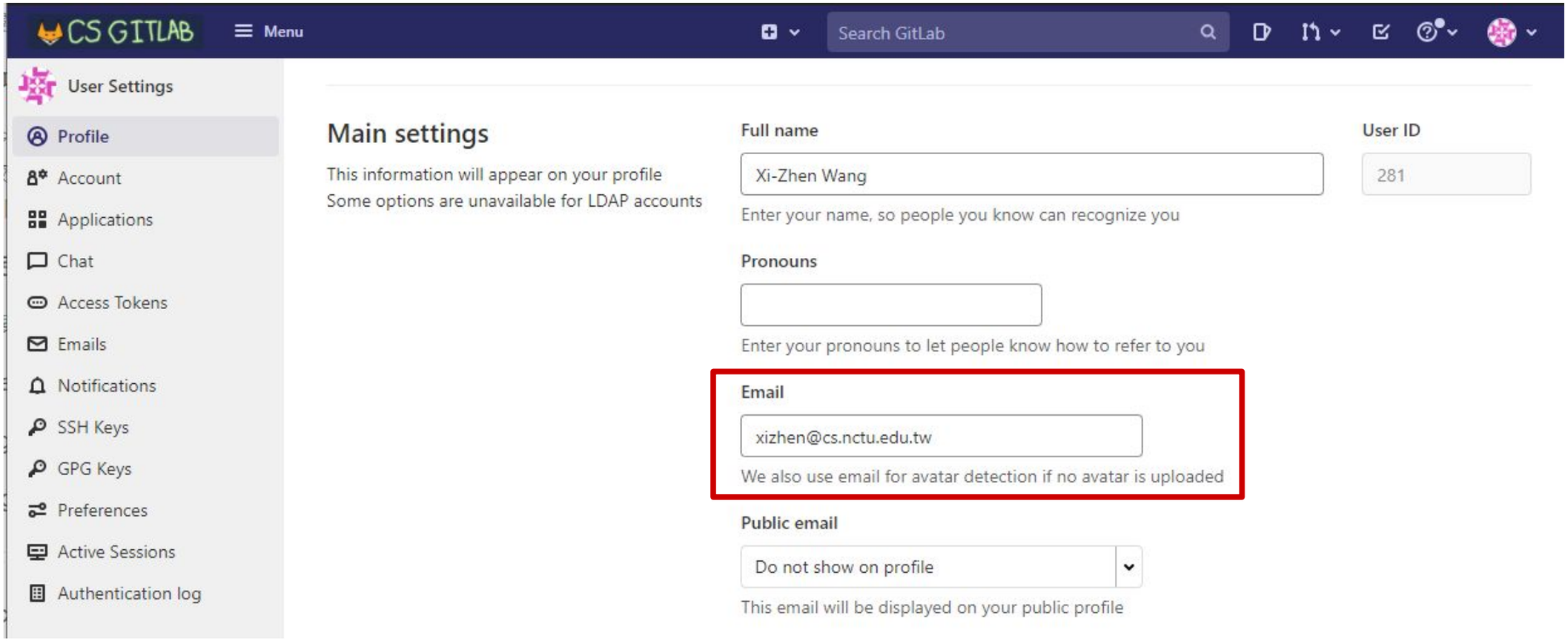
How to use git.cs

git.cs

- You should have a **cc account** and use this account to sign in git.cs. **https://git.cs.nctu.edu.tw/**
- Note: You must sign in before 10/01 23:59 (Fri.)

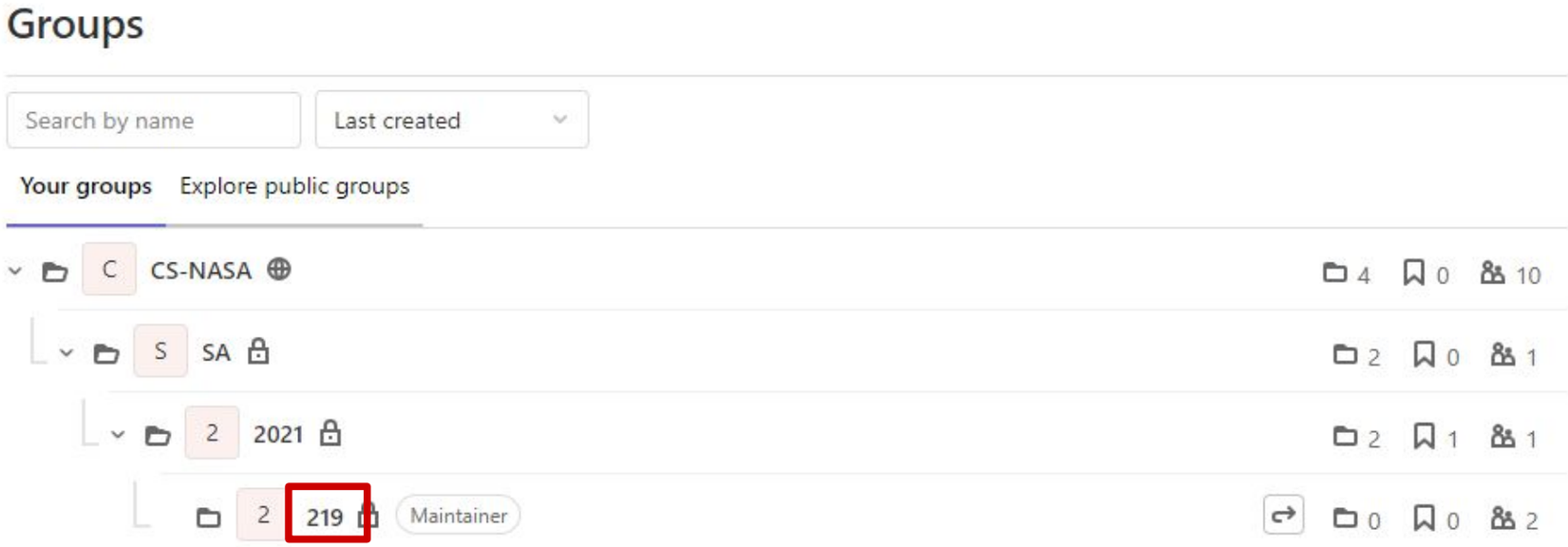
git.cs: application

- Update your email on the Profile page.
- Remember to confirm an email address in your mailbox.

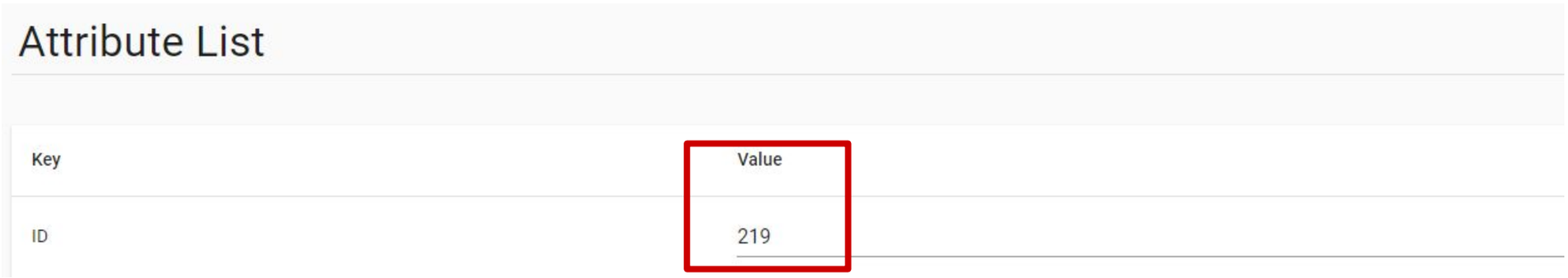


git.cs: CS-NASA Group

- Find your the group in “CS-NASA”

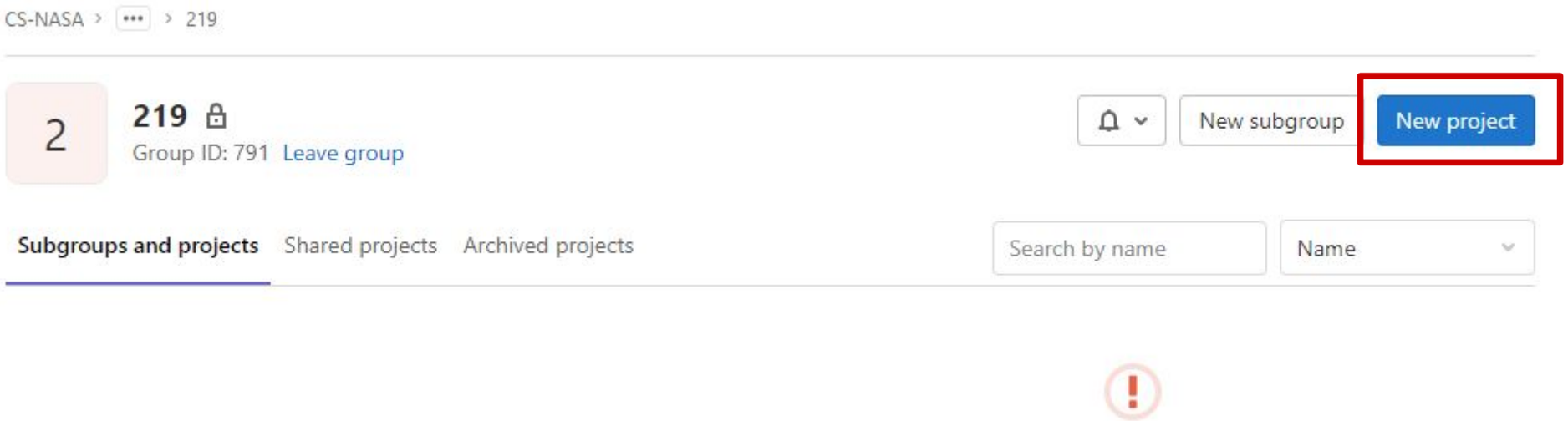


- The name of your group is your ID in Online Judge：

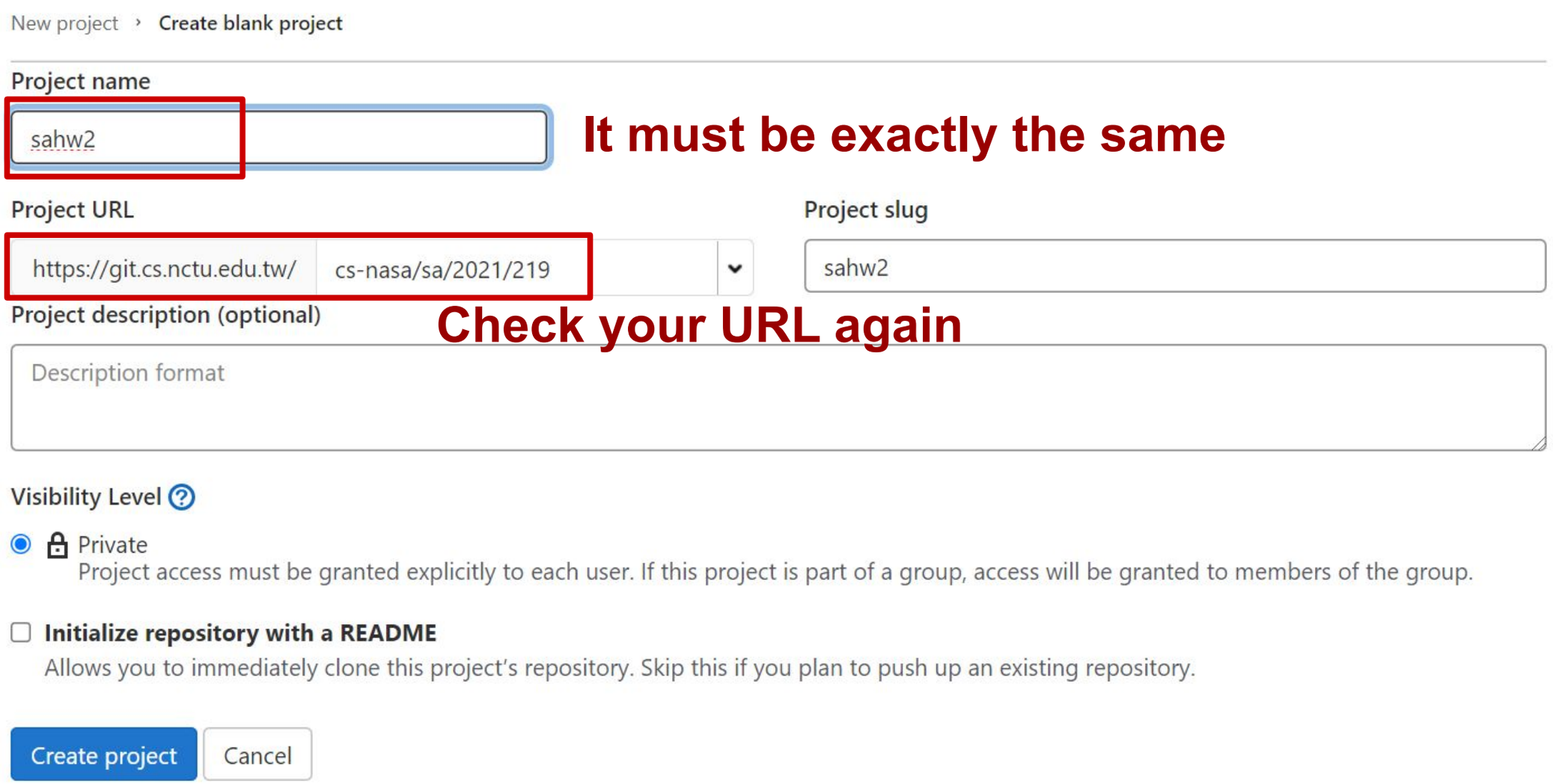


git.cs: New Project

- Create a new project



git.cs: New Project (Cont.)

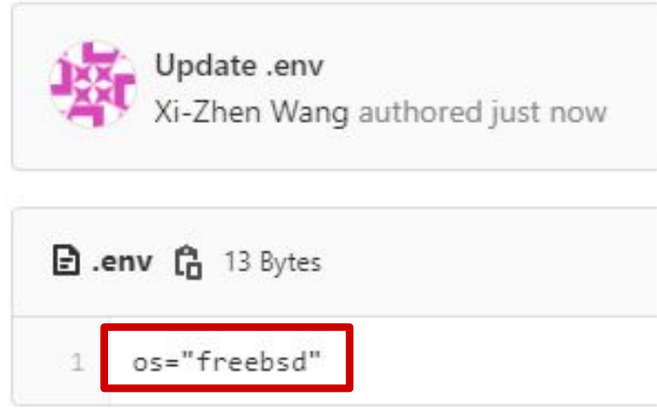


ans.sh

- Make sure your directory structure is like this:

```
xizhen@          ~/hw2/sahw2 (master*?) $ tree
.
├── hw2-1
│   └── ans.sh
├── hw2-2
│   └── ans.sh
└── os_env
2 directories, 3 files
```

os="freebsd" / "centos" ...



- Check your permission:

```
xizhen@          ~/hw2/sahw2 (master) $ ll hw2-1/ans.sh
-rwxr-xr-x. 1 xizhen xizhen 741 Sep 29 20:09 hw2-1/ans.sh
```

x: execute

Debug HW2-1: Student answer not found

```
Please make sure you have the correct access rights
and the repository exists.
Command: /bin/sh -c GIT_SSH_COMMAND="ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no" git clone
==== Start Judging ====
Making answer...
./judge-2.sh: line 22: stu_repo/hw2-1/ans.sh: No such file or directory
Student answer not found.
0;0;0;
```

Debug HW2-1: 0;0;0; Wrong Answer

```
-----------------------------------
Your ID: 144
Your IP: 10.113.0.144
[debug]   ID: 144
[debug] CMD1: GIT_SSH_COMMAND="ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no" git clone --quiet git@git.cs.nct
[debug] CMD2: cd sa-judge-hw2 && ./judge-2.sh
==== Preparing Judge Environment ====
Warning: Permanently added 'git.cs.nctu.edu.tw' (ECDSA) to the list of known hosts.
Cloning student repo...
Warning: Permanently added 'git.cs.nctu.edu.tw' (ECDSA) to the list of known hosts.
[OK].
Cloning answer repo...
Warning: Permanently added 'git.cs.nctu.edu.tw' (ECDSA) to the list of known hosts.
[OK].
==== Start Judging ====
Making answer...
[OK].
Judging...
Section 1 error. (In case 1)
Finished Section 1.
Section 2 error. (In case 1)
Finished Section 2.
Section 3 error. (In case 1)
Finished Section 3.
0;0;0;
```

0 = Wrong answer, 1 = accepted

Attention!

- You will get zero points if you just copy code from other students
- You will get zero points if you tamper with TA's system / file
- You can use our workstations to complete your homework
- **HW 2-1 → Online Judge & Check Manually**
  - We will check whether your script meets one-liner manually.
  - Online Judge only support FreeBSD currently.
- **HW 2-2 → Submit Code & Offline Judge**
  - TA Judging Time: 10/22 (Fri.) and 10/29 (Fri.)
  - TA will clone your project from gitlab and release scores on next monday.
- Due date: 10/29 23:59 (Fri.)

Attention!

- TA will use these operating systems to judge your homework
  - FreeBSD 12
  - CentOS Stream 8
- Online Judge only supports **built-in commands**.

Help me! TA!

- Questions about this homework
  - Ask questions on https://groups.google.com/g/nctunasa
  - We MIGHT give out hints on google group
    - Be sure to join the group :D
  - Do not email us directly
  - Do not use E3 to email us
- TA time : Wed. 15:00 - 17:00 at EC 324 (PC Lab)
  - You must use email to make an appointment first.
    - ta@nasa.cs.nctu.edu.tw
  - You must ask questions on google group first.
  - You can bring your laptop or use PC lab.
  - If there are too many people, we will announce another time slot.

Good Luck!