2021 Computer Network Lab

acpang@csie.ntu.edu.tw
http://www.csie.ntu.edu.tw/~acpang
Prof. Ai-Chun Pang
Graduate Institute of Networking & Multimedia,
Dept. of Computer Science and Engineering
National Taiwan University

LABII
Security
Wireless LANs

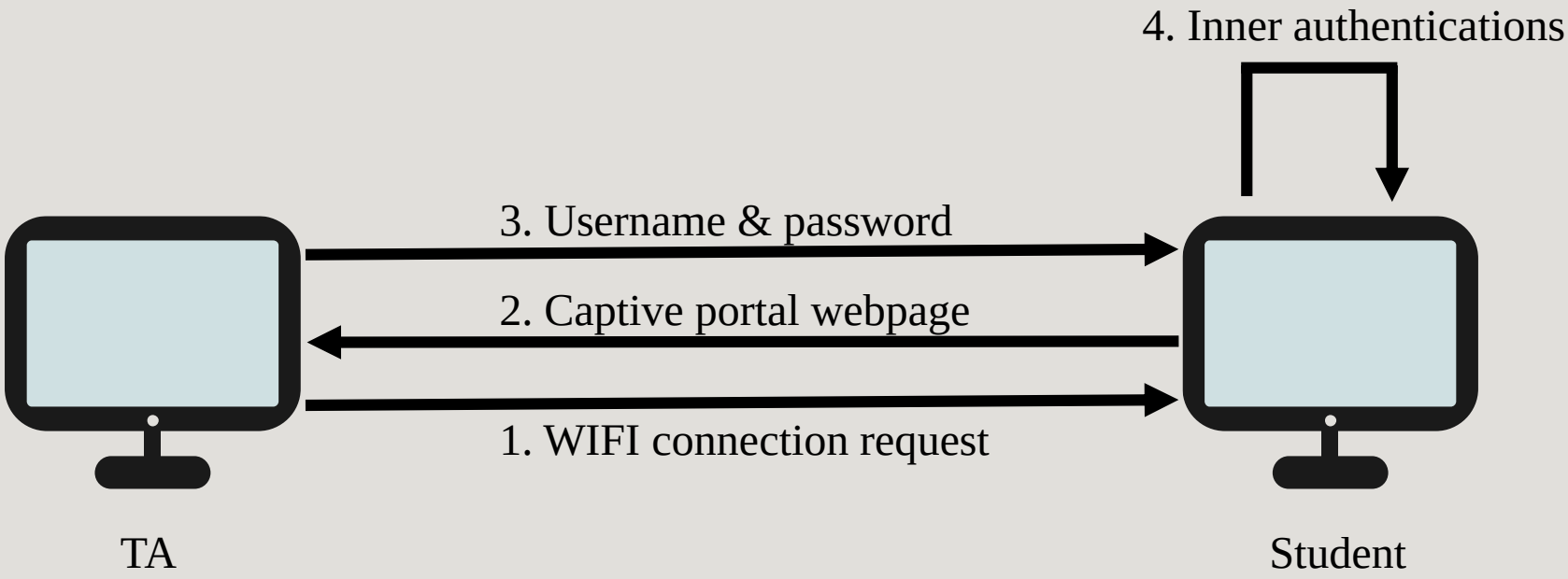
Outline

- Purpose of the Experiment
- Environment
- Procedure
- Grading Policy
- Deadline

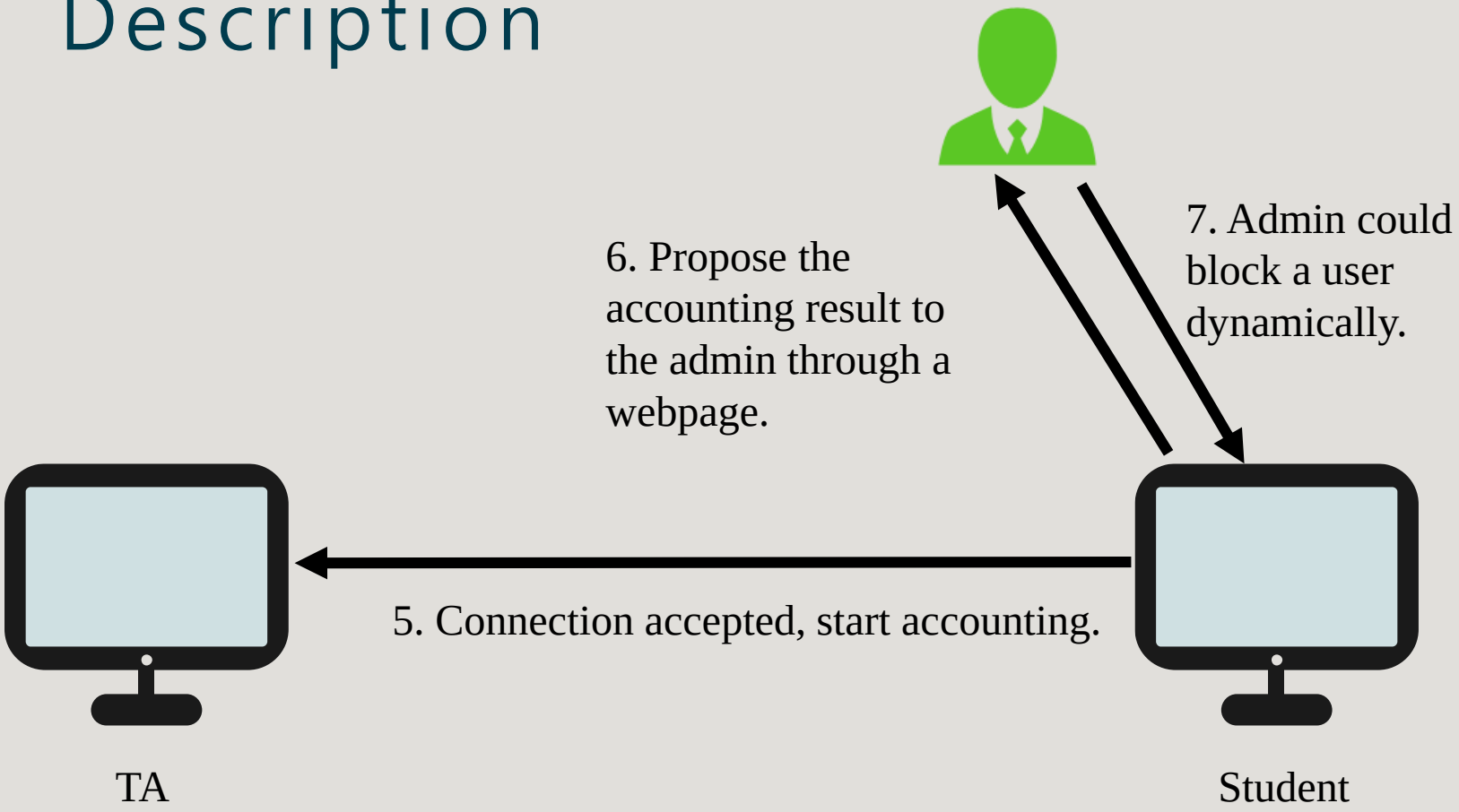
Target

- The target of the experiment is to design a WLAN user authentication mechanic, while accounting how much resource a user has used. Furthermore, students should implement traffic control and monitor mechanism.
- You are also required to offer user interface for the foregoing functions.

Description



Description



Environment

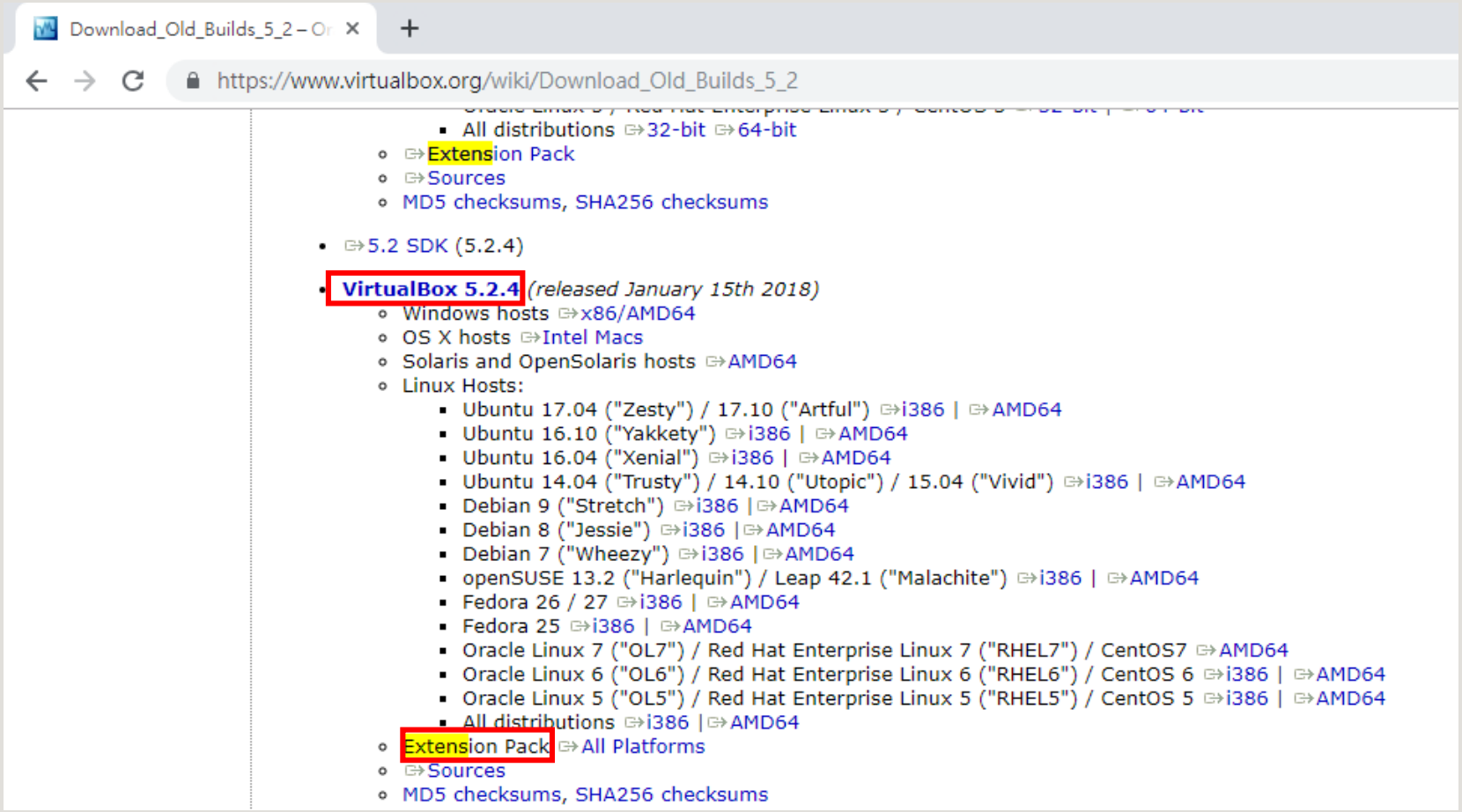
- OS: ubuntu(recommended)
- Virtual box ova file, password: cnlab2021
  - Dropbox: https://reurl.cc/Kx011q
  - Google drive: https://reurl.cc/Q7XqA9
  - USB
- You can start with our sample code in NTU COOL.

Environment

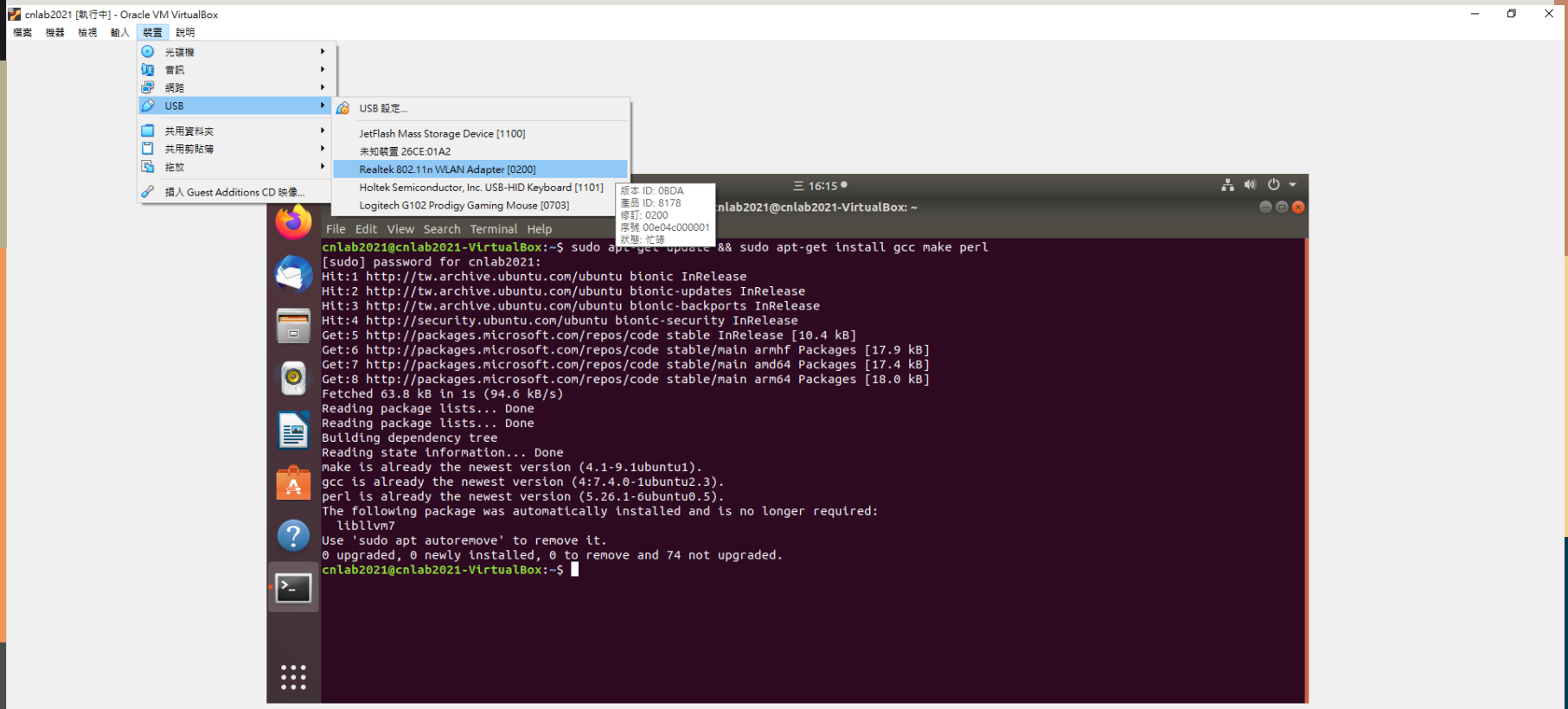
- Language and software to implement the functions are not restricted.
- During class, TAs mainly give lecture of nodejs + express + iptables.

Environment

You have to install the Virtualbox extension pack, so that it can access the USB wireless interface.



Environment



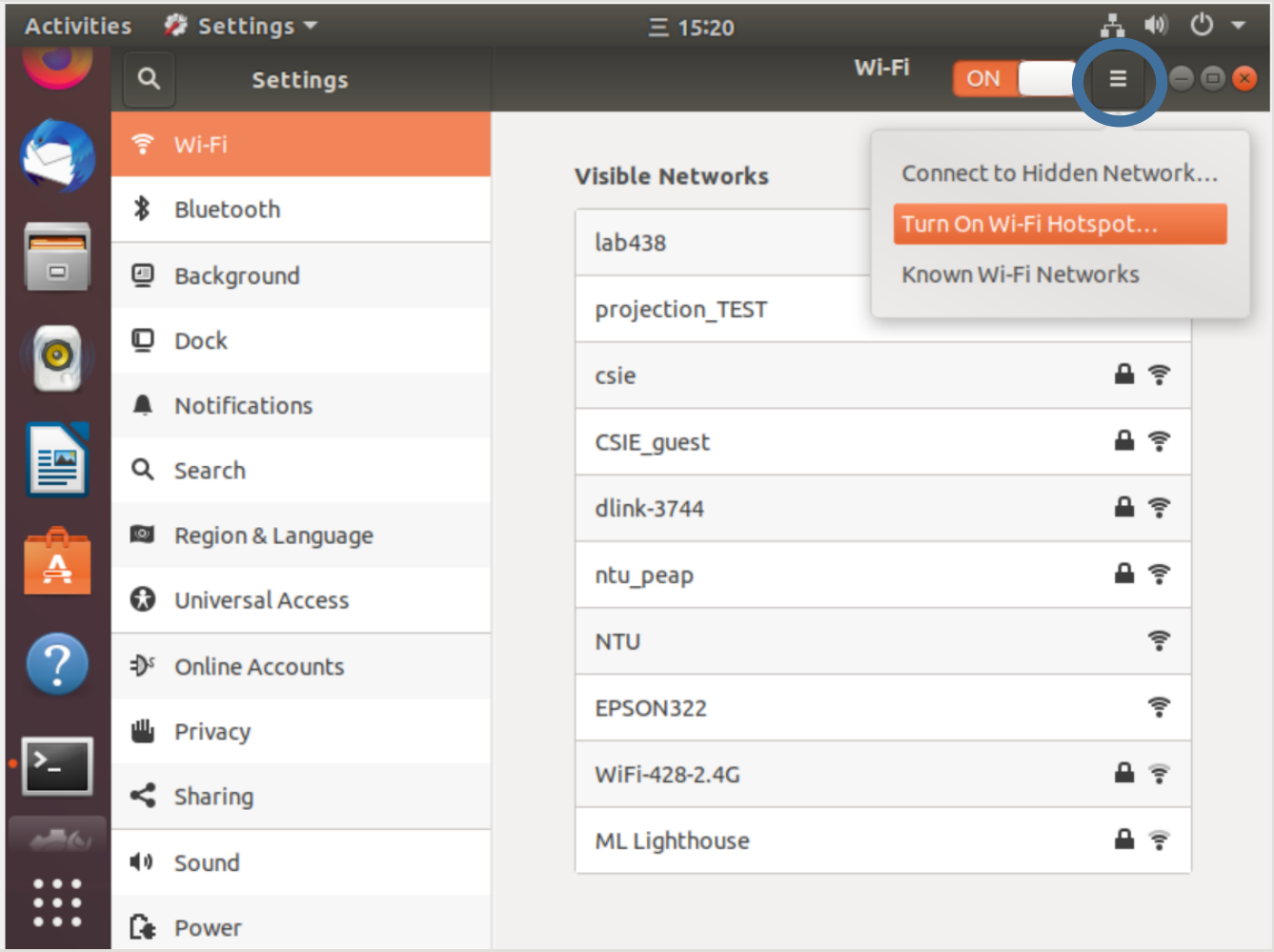
Procedure

- Turn on the Hotspot function
- Setup the environment
- Setup login page and authentication mechanic at backend.
- Redirect all traffics from the WLAN to login page.
- As for the Authenticated users, add new firewall rules.
- Keep monitoring the users, show the data by a simple webpage.
- As for users blocked by the admin, add new firewall rules.

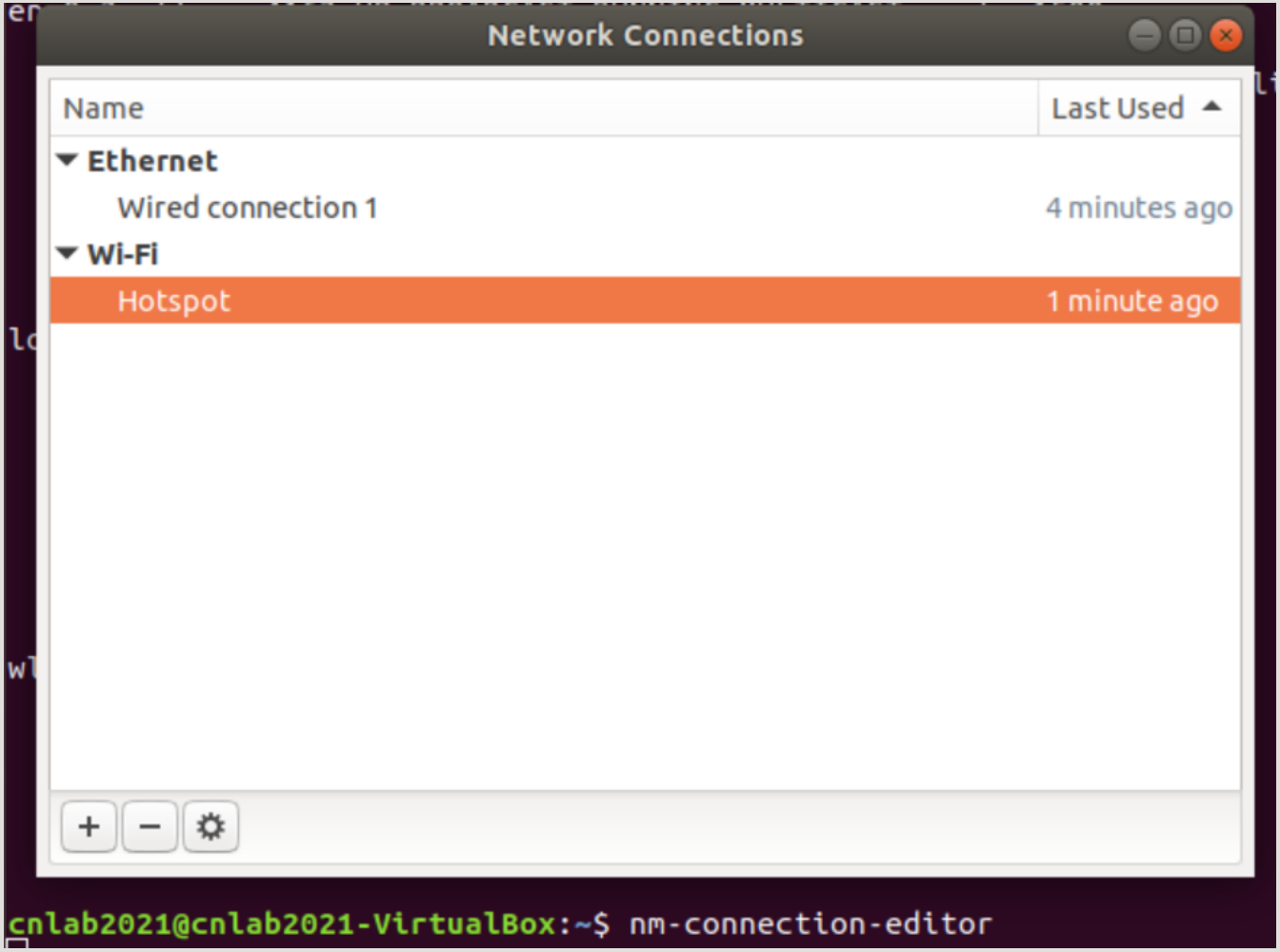
Procedure

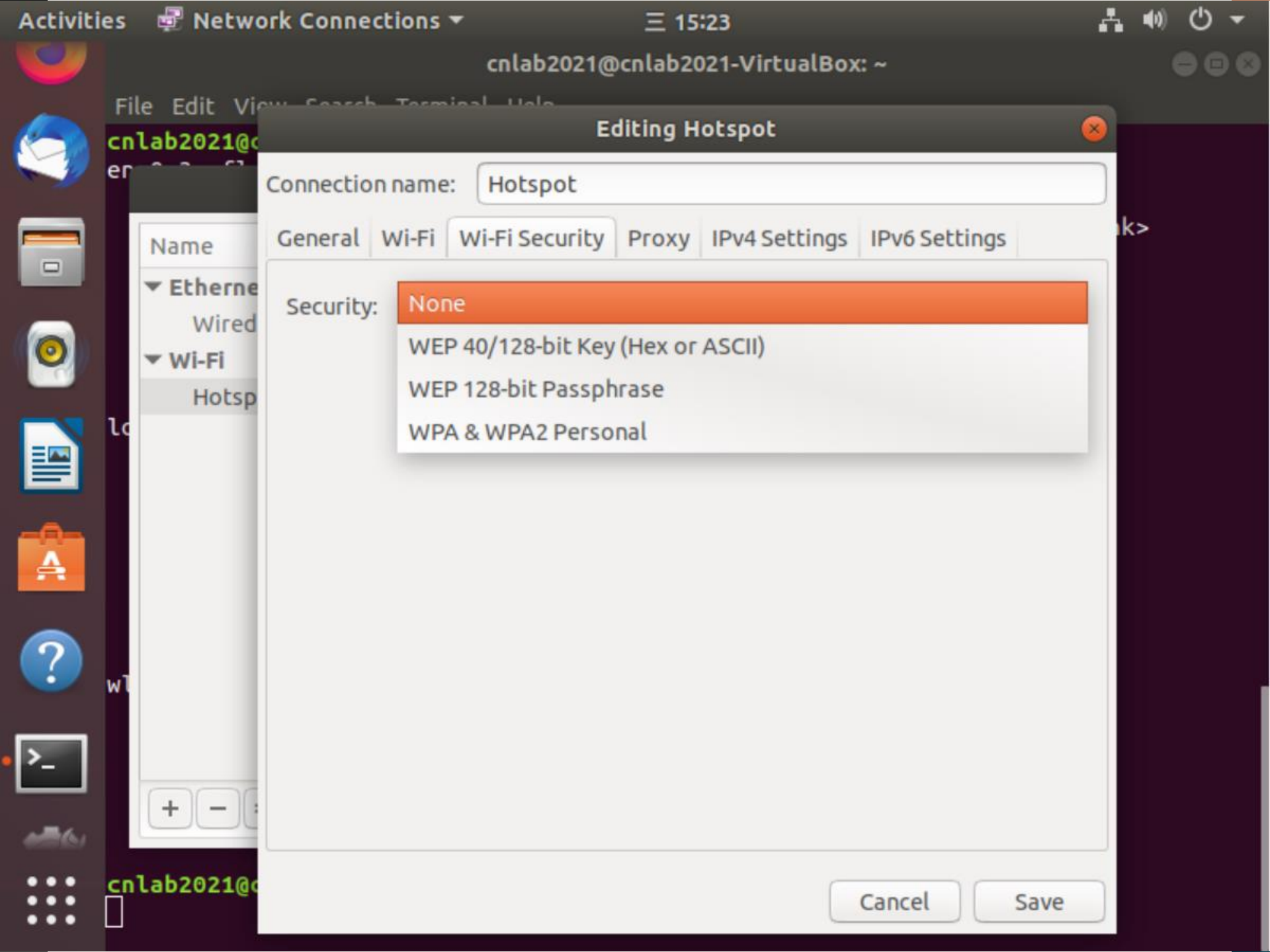
- Turn on the Hotspot function
- Setup the environment
- Setup login page and authentication mechanic at backend.
- Redirect all traffics from the WLAN to login page.
- As for the Authenticated users, add new firewall rules.
- Keep monitoring the users, show the data by a simple webpage.
- As for users blocked by the admin, add new firewall rules.

Procedure


Activities
Settings
15:20
Settings
Wi-Fi
ON
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Visible Networks
Connect to Hidden Network...
Turn On Wi-Fi Hotspot...
Known Wi-Fi Networks
lab438
projection_TEST
csie
CSIE_guest
dlink-3744
ntu_peap
NTU
EPSON322
WiFi-428-2.4G
ML Lighthouse

Procedure


Network Connections
Name
Last Used
Ethernet
Wired connection 1
4 minutes ago
Wi-Fi
Hotspot
1 minute ago
cnlab2021@cnlab2021-VirtualBox:~$ nm-connection-editor


Activities
Network Connections
15:23
cnlab2021@cnlab2021-VirtualBox: ~
File Edit
Editing Hotspot
Connection name:
Hotspot
General
Wi-Fi
Wi-Fi Security
Proxy
IPv4 Settings
IPv6 Settings
Security:
None
WEP 40/128-bit Key (Hex or ASCII)
WEP 128-bit Passphrase
WPA & WPA2 Personal
Cancel
Save
Name
Wi-Fi

Procedure

- Turn on the Hotspot function
- Setup the environment
- Setup login page and authentication mechanic at backend.
- Redirect all traffics from the WLAN to login page.
- As for the Authenticated users, add new firewall rules.
- Keep monitoring the users, show the data by a simple webpage.
- As for users blocked by the admin, add new firewall rules.

Procedure

[Nodejs official website: https://nodejs.org/en/](https://nodejs.org/en/)

The downloaded file should be binary, there is no need to compile it.

```
cnlab2021@cnlab2021-VirtualBox:~/Downloads$ tar Jxvf node-v14.16.0-linux-x64.ta
r.xz\
> cd node-v14.16.0-linux-x64\
> sudo cp -R * /usr
```

Procedure

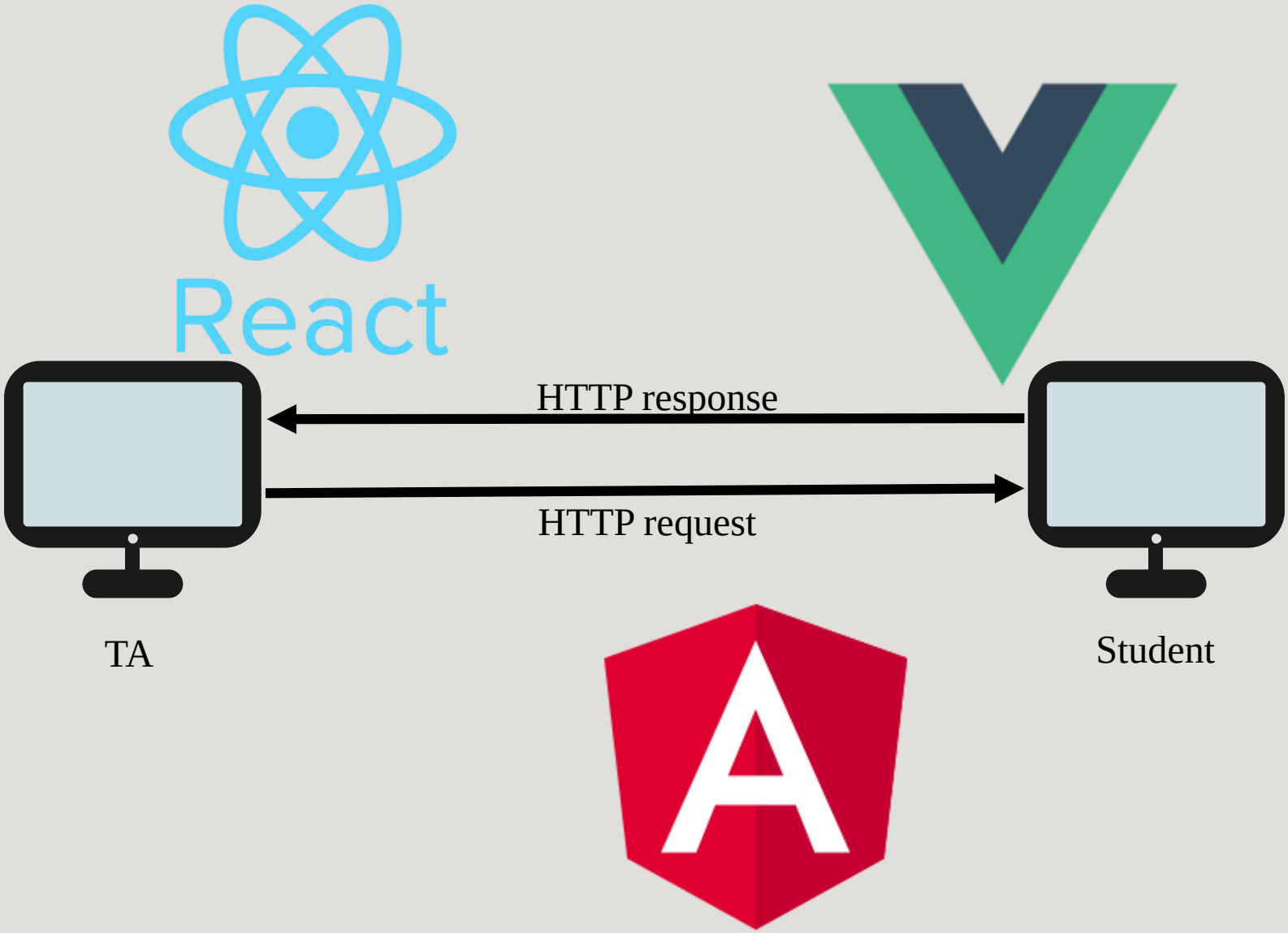
```
cnlab2021@cnlab2021-VirtualBox:~$ mkdir lab2
cnlab2021@cnlab2021-VirtualBox:~$ cd lab2/
cnlab2021@cnlab2021-VirtualBox:~/lab2$ npm init
```

```
cnlab2021@cnlab2021-VirtualBox:~/lab2$ npm install express body-parser
npm notice created a lockfile as package-lock.json. You should commit this file
.
npm WARN lab2@1.0.0 No description
npm WARN lab2@1.0.0 No repository field.

+ express@4.17.1
+ body-parser@1.19.0
added 50 packages from 37 contributors and audited 51 packages in 4.455s
found 0 vulnerabilities

cnlab2021@cnlab2021-VirtualBox:~/lab2$
```

Procedure

- Turn on the Hotspot function
- Setup the environment
- Setup login page and authentication mechanic at backend.
- Redirect all traffics from the WLAN to login page.
- As for the Authenticated users, add new firewall rules.
- Keep monitoring the users, show the data by a simple webpage.
- As for users blocked by the admin, add new firewall rules.

Procedure



Procedure

app.js ● captive_portal.py

```
19  const express = require("express");
20  const bodyParser = require("body-parser");
21
22  let app = express();
23  app.use(bodyParser.urlencoded({ extended: true }));
24
25  app.get(/\/*/, (req, res) => {
26      let ip = req.headers['x-forwarded-for'] || req.connection.remoteAddress;
27      console.log(`${ip} is asking for wifi!`);
28      res.setHeader("Content-type", "text/html")
29      res.send(`
30      <html>
31          <form action="login" method="post">
32              name: <input type="text" name="name" />
33              </br>
34              password: <input type="password" name="password" />
35              </br>
36              <button>GO!</button>
37          </form>
38      </html>
39      `);
40  });
41  app.post("/login", (req, res) => {
42      console.log(req.body)
43      let name = req.body.name;
44      let password = req.body.password;
45      let ip = req.headers['x-forwarded-for'] || req.connection.remoteAddress;
46      console.log(ip)
47      if(name == "cnlab" && password == "mycnlab") {
48          res.send("<h1>登入成功</h1>")
49          // 修改防火牆，並且把此人的IP記下來
50
51
52
53
54      } else {
55          res.send("<h1>帳號或密碼有誤 QQ</h1>")
56      }
57  });
58
59  app.listen(8888);
60  console.log("start listening!")
```

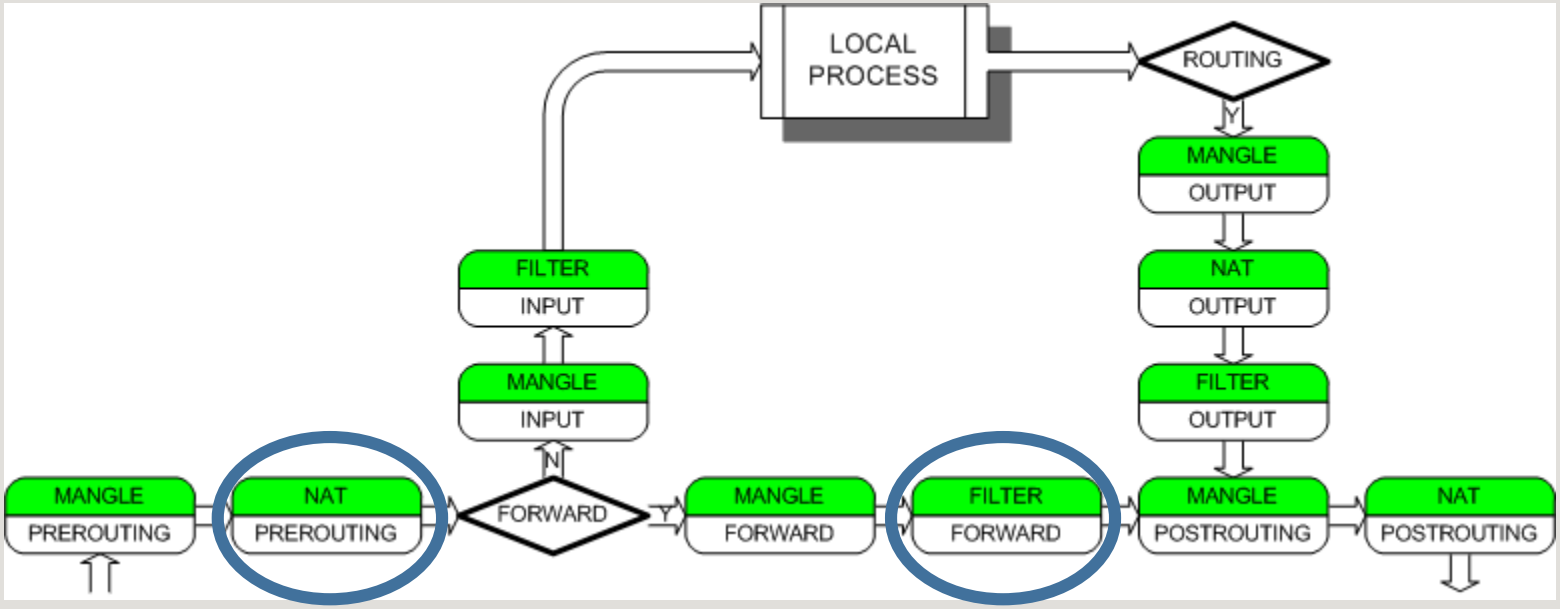
Procedure

- Turn on the Hotspot function
- Setup the environment
- Setup login page and authentication mechanic at backend.
- Redirect all traffics from the WLAN to login page.
- As for the Authenticated users, add new firewall rules.
- Keep monitoring the users, show the data by a simple webpage.
- As for users blocked by the admin, add new firewall rules.

Procedure

Iptables is a User Space firewall software. It processes and redirects packages by controlling Netfilter in the Linux kernel.

- Elements of iptables are tables, chains, and rules



Procedure

- **Filter table** is the default one. If no other table is specified, this table will be used. Filter table is usually used to filter packages. It contains:
  - INPUT, packets toward local machine go through the chain.
  - OUTPUT, packets form local machine go through the chain.
  - FORWARD, packets forwarded by the local machine go through the chain.
- **Nat table** is used to transform addresses. It contains:
  - PREROUTING, packets go through the chain before routing. It is usually used to transform destination address (DNAT).
  - POSTROUTING, packets go through the chain after routing. It is usually used to transform source address.
  - OUTPUT, similar to PREROUTING, but it process packets from local machine.

Procedure

10.0.2.15 is the interface to the Internet. 10.42.0.0/24 are users connected

```
cnlab2021@cnlab2021-VirtualBox:~/lab2$ sudo sh show.sh

================== iptables -L ==================
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootps
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:bootps
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             10.42.0.0/24         state RELATED,ESTABLISHED
ACCEPT     all  --  10.42.0.0/24         anywhere
ACCEPT     all  --  anywhere             anywhere
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
DROP       all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

================== iptable -L -t nat ==================
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere             tcp dpt:http to:10.0.2.15:9090
DNAT       tcp  --  anywhere             anywhere             tcp dpt:https to:10.0.2.15:9090

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  10.42.0.0/24        !10.42.0.0/24
```

Procedure

10.0.2.15 is the interface to the Internet. 10.42.0.0/24 are users connected

```
ACCEPT     all  --  anywhere             10.42.0.0/24         state RELATED,ESTABLISHED
ACCEPT     all  --  10.42.0.0/24         anywhere
```

Ensure that packets toward users won't be drop.

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere             tcp dpt:http to:10.0.2.15:9090
DNAT       tcp  --  anywhere             anywhere             tcp dpt:https to:10.0.2.15:9090
```

All packets toward the internet is redirected to the 9090 port (the login page)

Procedure

- Turn on the Hotspot function
- Setup the environment
- Setup login page and authentication mechanic at backend.
- Redirect all traffics from the WLAN to login page.
- As for the Authenticated users, add new firewall rules.
- Keep monitoring the users, show the data by a simple webpage.
- As for users blocked by the admin, add new firewall rules.

Procedure

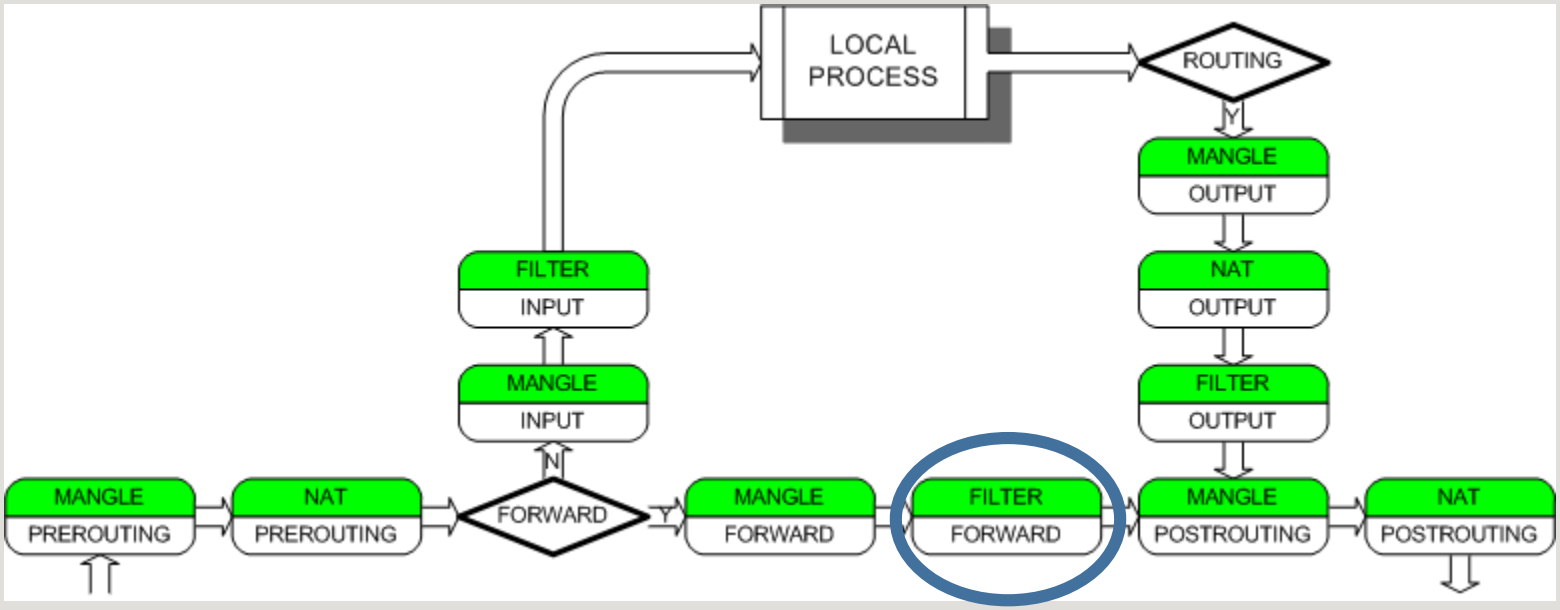
```
========== iptables -L -t nat ==============

Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             10.42.0.105
ACCEPT     all  --  10.42.0.105          anywhere
DNAT       tcp  --  anywhere             anywhere            tcp dpt:http to:10.0.2.15:9090
DNAT       tcp  --  anywhere             anywhere            tcp dpt:https to:10.0.2.15:9090
```

10.42.0.105 is an authorized user. Add new rules so that he/she is not redirected by the DNAT rule.

Procedure

- Turn on the Hotspot function
- Setup the environment
- Setup login page and authentication mechanic at backend.
- Redirect all traffics from the WLAN to login page.
- As for the Authenticated users, add new firewall rules.
- Keep monitoring the users, show the data by a simple webpage.
- As for users blocked by the admin, add new firewall rules.

Procedure


LOCAL PROCESS
ROUTING
Y
MANGLE
OUTPUT
NAT
OUTPUT
FILTER
OUTPUT
FILTER
INPUT
MANGLE
INPUT
N
MANGLE
PREROUTING
NAT
PREROUTING
FORWARD
Y
MANGLE
FORWARD
FILTER
FORWARD
MANGLE
POSTROUTING
NAT
POSTROUTING

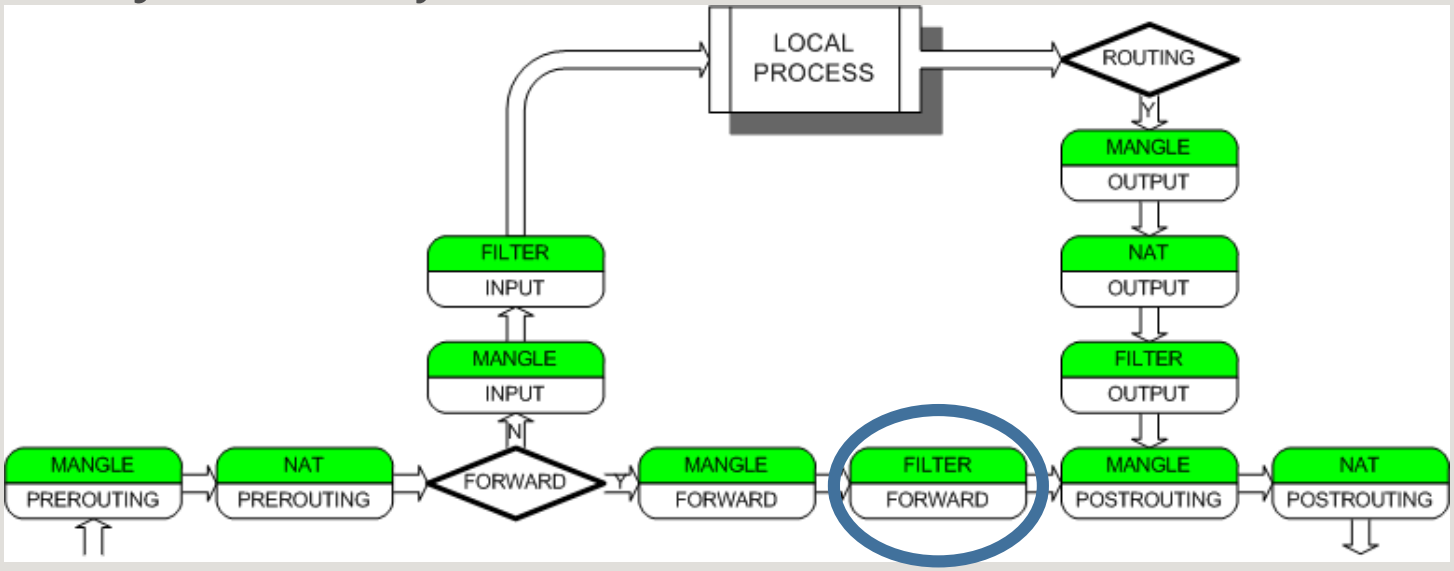
Procedure

```
Chain INPUT (policy ACCEPT 82 packets, 8592 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       1      333 ACCEPT     udp  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0           udp dpt:67
       0        0 ACCEPT     tcp  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0           tcp dpt:67
      33     2184 ACCEPT     udp  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
       0        0 ACCEPT     tcp  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
     484   370555 ACCEPT     all  --  *      *       0.0.0.0/0            10.42.0.105
     461   200268 ACCEPT     all  --  *      *       10.42.0.105          0.0.0.0/0
      20     1386 ACCEPT     all  --  *      wlx74da38f8c760  0.0.0.0/0            10.42.0.0/24        state RELATED,ESTABLISHED
      19     2531 ACCEPT     all  --  wlx74da38f8c760 *       10.42.0.0/24         0.0.0.0/0
       0        0 ACCEPT     all  --  wlx74da38f8c760 wlx74da38f8c760  0.0.0.0/0            0.0.0.0/0
       0        0 REJECT     all  --  *      wlx74da38f8c760  0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreachable
       0        0 REJECT     all  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreachable
       0        0 ACCEPT     tcp  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
       0        0 ACCEPT     udp  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
       0        0 ACCEPT     tcp  --  wlx74da38f8c760 *       0.0.0.0/0            10.0.2.15           tcp dpt:9090
       0        0 DROP       all  --  wlx74da38f8c760 *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 104 packets, 11100 bytes)
    pkts      bytes target     prot opt in     out     source               destination
```

- Iptables –L –v -x
- List the detailed data of **filter table**
  - -v: show the amount of packets and the total traffic.
  - -x: show the specific byte count of the total traffic

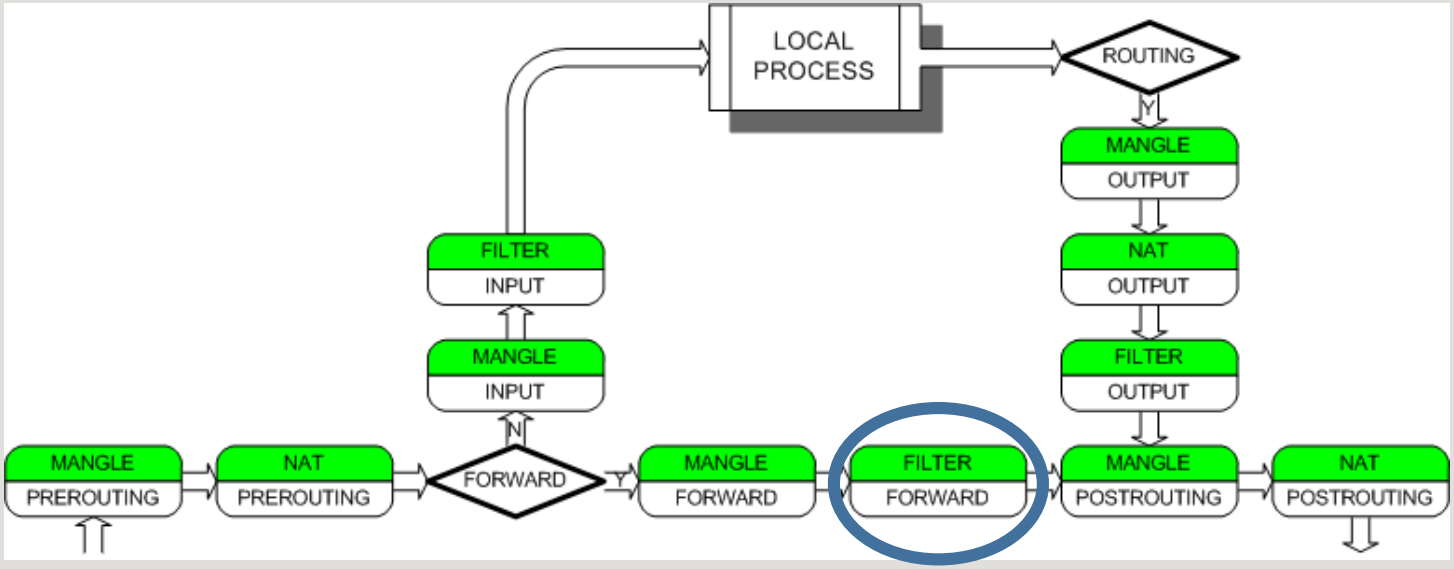
Brief Introduction to iptables

- iptables -A FORWARD -i ${wlan0} -p tcp --dport 53 -j ACCEPT
- iptables -A FORWARD -i ${wlan0} -p udp --dport 53 -j ACCEPT
  - -A: append, append to a chain
  - -i: the network interface
  - --dport 53: toward port 53, representing a DNS query.
  - -j is fallow by rules.



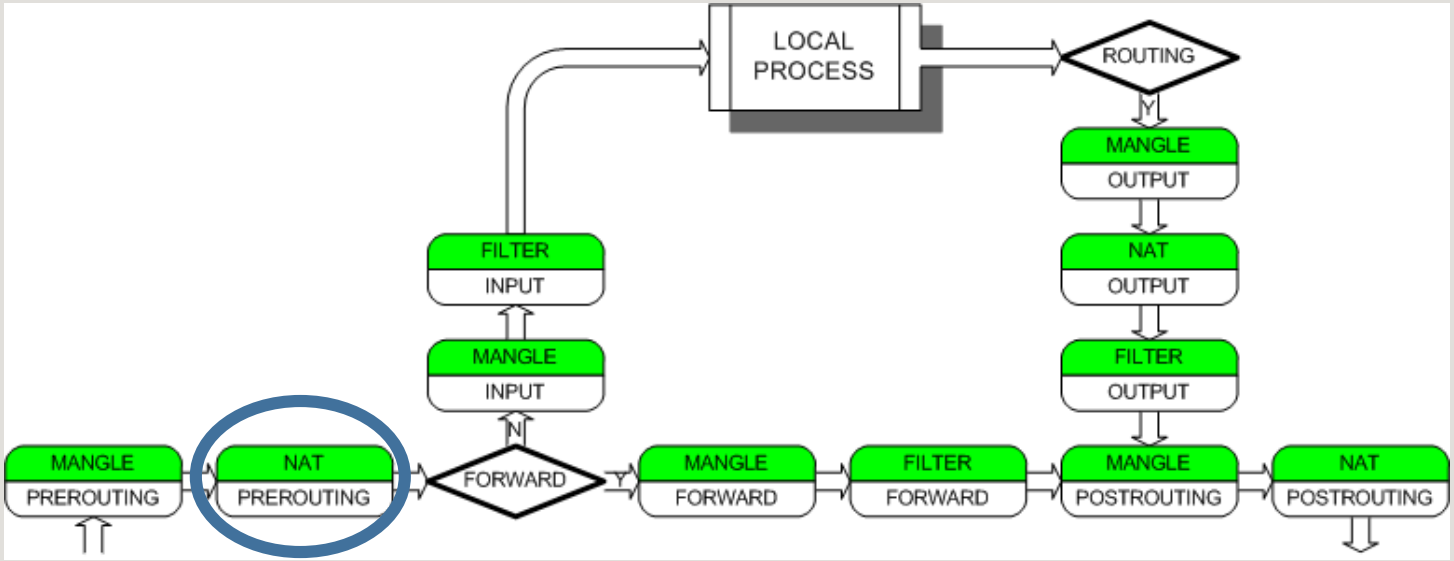
Brief Introduction to iptables

- iptables -A FORWARD -i ${wlan0} -j DROP
  - Allows accessing login page from the WLAN, otherwise drop them (You can’ t see the login page outside the LAN).



Brief Introduction to iptables

- iptables -t nat -A PREROUTING -i ${wlan0} -p tcp --dport 80 -j DNAT --to-destination `${MY_IP}:9090`
- iptables -t nat -A PREROUTING -i ${wlan0} -p tcp --dport 443 -j DNAT --to-destination `${MY_IP}:9090`
  - --to-destination is followed by the address to redirect.



Brief Introduction to iptables

- Allowing users to access the Internet / Block a specific user.
  - Try it yourself!

```
if(name == "cnlab" && password == "mycnlab") {
    res.send("<h1>登入成功</h1>")
    // 修改防火牆，並且把此人的IP記下來
    spawn("iptables", ["-t", [redacted], "-I", "[redacted]", "1", [redacted], remote_IP, "-j", "ACCEPT"])
    spawn("iptables", ["-t", "nat", "-I", "[redacted]", "1", "-d", [redacted] "-j", [redacted]])
    spawn("iptables", ["-I", [redacted], "-s", remote_IP, "-j", [redacted]])
    spawn("iptables", ["-I", [redacted], "-d", [redacted], "-j", "ACCEPT"])
```

Brief Introduction to iptables

- Allowing users to access the Internet / Block a specific user.
  - Try it yourself!

```
if(name == "cnlab" && password == "mycnlab") {
    res.send("<h1>登入成功</h1>")
    // 修改防火牆，並且把此人的IP記下來
    spawn("iptables", ["-t", [redacted], "-I", "[redacted]", "1", [redacted], remote_IP, "-j", "ACCEPT"])
    spawn("iptables", ["-t", "nat", "-I", "[redacted]", "1", "-d", [redacted] "-j", [redacted]])
    spawn("iptables", ["-I", [redacted], "-s", remote_IP, "-j", [redacted]])
    spawn("iptables", ["-I", [redacted], "-d", [redacted], "-j", "ACCEPT"])
```

Grading Policy

- Demo (50%)
  - Showing login page on the local machine (10%)
  - Directing user to the page (10%)
  - Users should access the Internet after login (10%)
    - You are allowed to hardcode username & password in the code.
  - Monitoring the user through a UI (10%)
  - Blocking specific user dynamically (10%)
- Report (30%)
  - Team number, member list, environment and language.(10%)
  - Briefly describe how packets go through the iptables. (10%)
  - Describe how your program (server & webpage) interact with the iptables. (10%)

Grading Policy

- Situational questions(20%)
  - Your website is working on port 8080 and can only be accessed by 140.112.0.0/16.
    How to modify your iptables to block unavailable users.(10%)
  - Behind the machine, there is a ssh server which locates at 192.168.10.2 in the eth1.
    People who want to connect to ssh server from eth0 need to connect the machine at port 2222 and the machine will redirect the flow to the ssh server at port 22.
    How to configure the iptable? We only check two commands for PREROUTING and POSTROUTING.(10%)

Deadline

- 4 / 15 Demo
- 4 / 22 23:59:59
  - Submit report and source code to NTU cool
  - Report has to be in pdf format