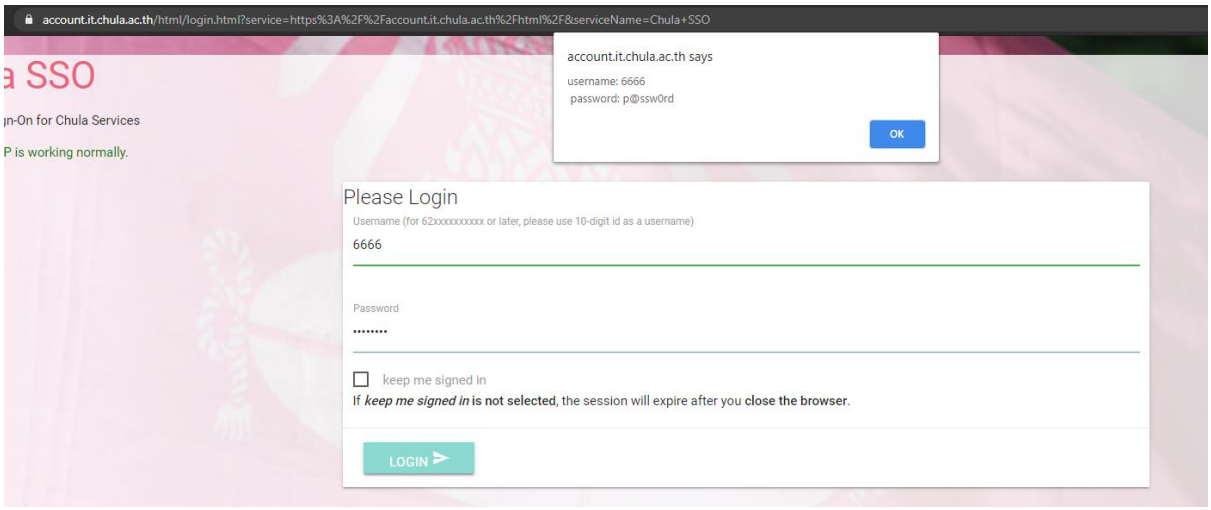
Activity III – Physical Security

1. JavaScript Injection

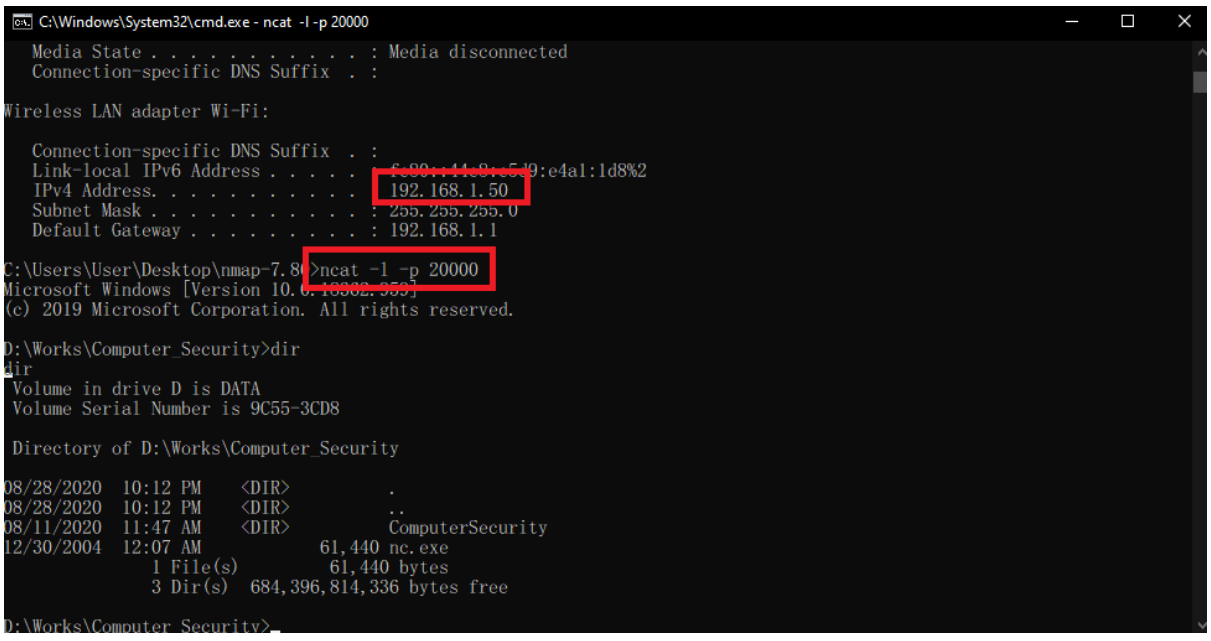


Code:

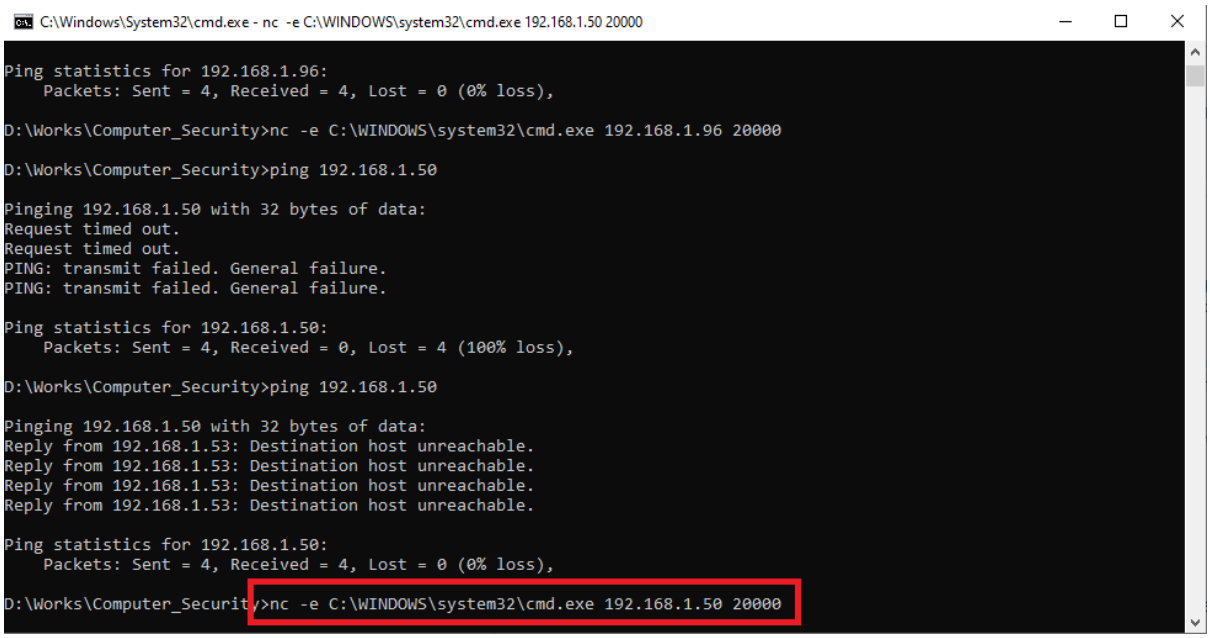
```
document.getElementById('btn_signin').addEventListener('click',
function(){alert('username: ' + document.forms[0].username.value + '\n password: '
+ document.forms[0].password.value)})
```

2. Worm Attack

Attacker's Machine:



Victim's Machine:



Notes: Attacker uses ncat from nmap instead of netcat due to problems installing netcat on attacker's pc (virus alert, and I cannot turn off Windows Defender)

Source: https://nmap.org/ncat/

3. Write an essay to summarize the lesson that you have learned in this activity. In particular, explain the worst case scenario that can happen. As a user, how will you prevent yourself from being a victim to such attacks?

JavaScript Injection

I have learned that browsers are easily modified through console, not only visually modified but also functionally (with the injection). Worse case that could happen could be if the injection includes HTTP request to some kind of server that store our username and password data, that way the hacker will have a database full with login attempts of that particular website. From now on I will prevent getting hacked from this method by refreshing the webpage a few times before I attempt to login when I am using a public computer.

Worm Attack

I also have learned how dangerous it is to install programs from unknown publisher, as netcat and two lines of command could possibly let the hacker taken over my computer entirely. Worse case would be if the worm comes with any free download, or pirated program on the Internet and someone downloaded it, the worm installed itself along with netcat and run the command, while the hacker is just waiting to control victim's machines. With this knowledge I will try to not download or install any programs from unknown publishers as they all can be malicious to my machine.