[SOCKS Server : CONNECT] (15 points)

1.開 Chrome，可以連到 google 首頁
2.開 Chrome，設定你的 socks server
設好之後
(1).連 google 首頁隨便搜尋某個頁面（正常） (5 points)
(2).socks server 斷線，再隨便點某個連結（失敗） (5 points)
(3).socks server 連線，再點同一個連結（正常） (5 points)

[SOCKS Server : BIND] (15 points)

1.開 FTP(使用 FlashFXP)，設定
- [Options]-[Preferences]-[Connection]-[Proxy]-[Add]-[Type:Socks 4]，填入你的 socks server

連到一個 ftp 之後 (檔案建議大於 1GB，可用 Ubuntu 16.04 的 iso 做為測試)
1. 上傳 file1，上傳成功後看 size 是否相同及能不能開 (5 points)
2. 下載 file1，下傳成功後看 size 是否相同及能不能開 (5 points)
3. 看 SOCKS Server 的 output 是否有用[BIND] protocol (5 points)

note:
1.請不要用 FileZilla
2.請使用 FlashFXP

[SOCKS Server : Messages] (5 points)
Server 需顯示相關資訊，例如以下：
<S_IP> : source ip
<S_PORT> : source port
<D_IP> : destination ip
<D_PORT> : destination port
<Command> : CONNECT or BIND
<Reply> : Accept or Reject
<Content> : Redirect socket data (show partial data ---> do not need show all)

範例：

```
VN: 4, CD: 1, DST IP: 208.97.187.201, DST PORT: 443, USERID: MOZ
Permit Src = 140.113.99.130(56540), Dst = 208.97.187.201(443)
SOCKS_CONNECT GRANTED ....
VN: 4, CD: 1, DST IP: 208.97.187.207, DST PORT: 443, USERID: MOZ
Permit Src = 140.113.99.130(56541), Dst = 208.97.187.207(443)
SOCKS_CONNECT GRANTED ....
VN: 4, CD: 1, DST IP: 149.5.128.169, DST PORT: 80, USERID: MOZ
Permit Src = 140.113.99.130(56542), Dst = 149.5.128.169(80)
SOCKS_CONNECT GRANTED ....
```

[CGI SOCKS Client] (25 points)

1. 連到自己的帳號下的 form_get2.htm，可以輸入五欄的 IP , port , filename , SocksIP , SocksPort
2. 透過 socks server 連到五台機器看輸出是否正常
3. CGI 改完記得命名為 hw4.cgi

Test Case (the same as Project III)

(1). t1.txt (5 points)

(2). t2.txt (5 points)

(3). t3.txt (5 points)

(4). t4.txt (5 points)

(5). t5.txt(5 points)

[Firewall](用 socks.conf 來設定) (10 points)

Firewall 是用於當 socks server 接收到 socks4_request 後，分析 DEST_IP 是否為允許連線的 IP。如果不是允許的 IP，回傳 reject 的 socks4_reply。

此 project 實作較為單純的 firewall，只限定 DEST IP。將允許的 IP 寫到 socks.conf 中。

(1). 允許連線至所有的 DEST IP。socks.conf 的內容為 “*.*.*.*” (不包括引號)。

(2). 只允許連線至交大(140.113.*.*)。socks.conf 的內容為 “140.113.*.*” (不包括引號)。(5 points)

(3). 只允許連線至交大(140.114.*.*)。socks.conf 的內容為 “140.114.*.*” (不包括引號)。(5 point)

==========

[code : SOCKSServer]

流程：

・master socket(listener)不斷地 listen，有連線(SRC)來就 fork 一個 process(SOCKS) 去處理，然後繼續 listen

・SOCKS 與 SRC 連線溝通

1.收 SOCKS4_REQUEST 格式封包

2.check 是否可以過防火牆(socks.conf)，並回傳 SRC SOCKS4_REPLY

3-1.如果是 CONNECT 模式：

a.從 REQUEST 裡取出 dest 的 IP 與 PORT

b.SOCKS 連線到 DEST

c.SOCKS 幫 SRC 與 DEST 做資料傳導的動作

－SRC 傳來的資料－＞傳給 DEST

－DEST 傳來的資料－＞傳給 SRC

3-2.如果是 BIND 模式：

a.SOCKS 先去 BIND 一個 port(BIND_PORT)

b.SOCKS listen 該 port，回傳給 SRC 監聽 Port，DEST 就會自己連過來

c.SOCKS accept DEST 之後，要再丟一個 SOCKS4_REPLY 給 SRC<-- 重要!!!!!!!!!

d.SOCKS 幫 SRC 與 DEST 做資料傳導的動作

－SRC 傳來的資料－＞傳給 DEST

－DEST 傳來的資料－＞傳給 SRC

寫程式的注意事項

1.SOCKS_REQUEST , SOCKS_REPLY 的 protocol 要注意

1 byte : unsigned char

2 byte : unsigned char[2]

4 byte : unsigned char[4]

2.port 格式

ex : port = 1234

unsigned char port[2]

port[0] = 4

port[1] = 210

(hint : (int)port = port[0]*256 + port[1] ==> 1234 = 4*256 + 210)

3.IP 格式

ex : IP = 140.113.1.2

unsigned char IP[4]

IP[0] = 140

IP[1] = 113

IP[2] = 1

IP[3] = 2

4.BIND mode 裡，要確定 client 與 server 的連線建好了再開始傳資料

5.測試請不要用 FileZilla

建議使用 FlashFXP

(link : http://www.flashfxp.com/)

6.FTP server 線上申請: http://5gbfree.com/ 或是自行架設: http://goo.gl/UjrFwy

[code : CGI Socks Client]

原本連到 ras server，現在變成連到 socks server，

然後把要連到 ras server 的 IP , port 放在 SOCKS_REQUEST 裡傳給 socks server，讓他去重導。

畫面如下：