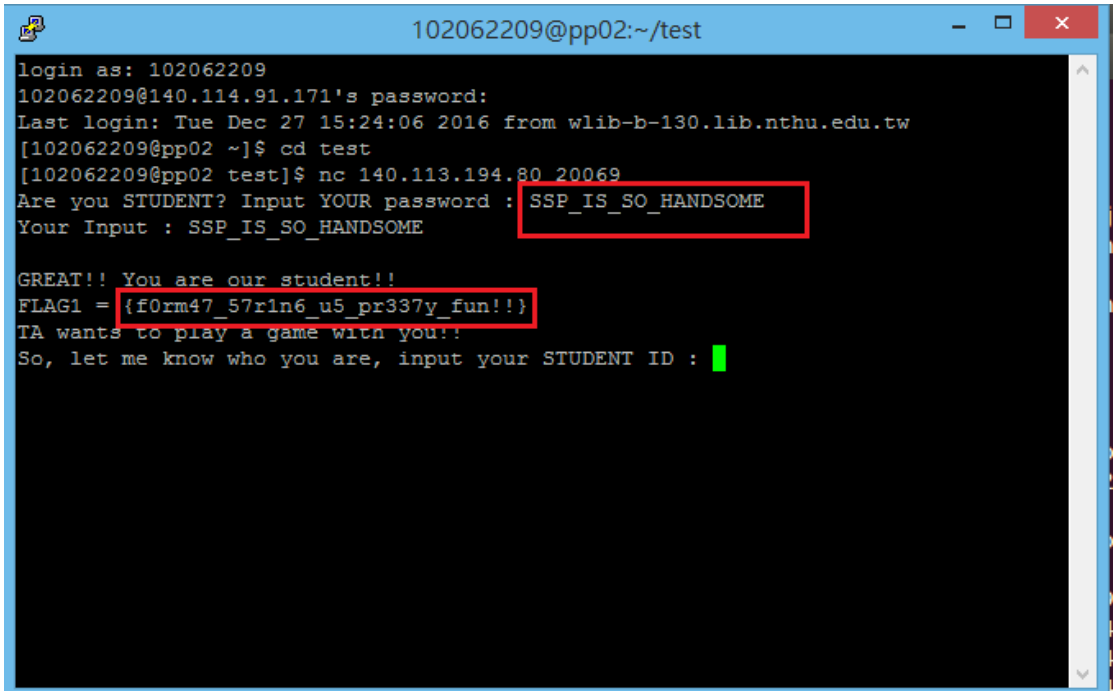
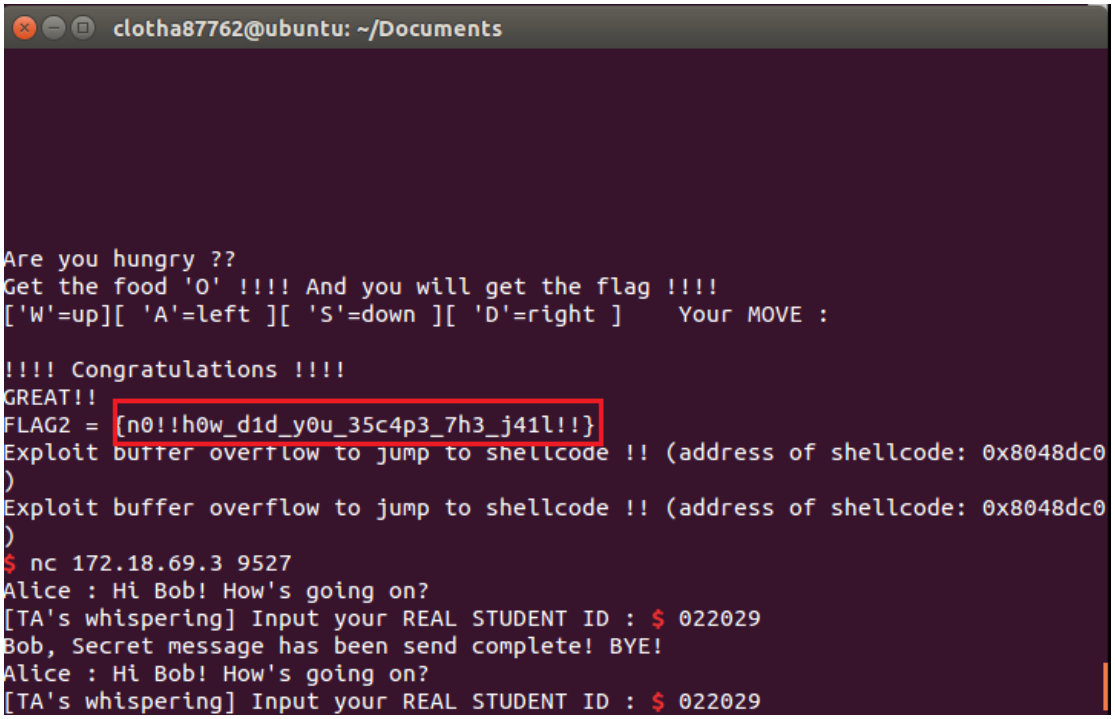
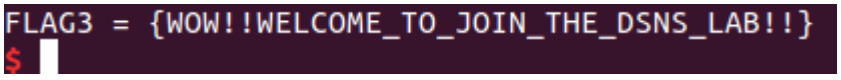
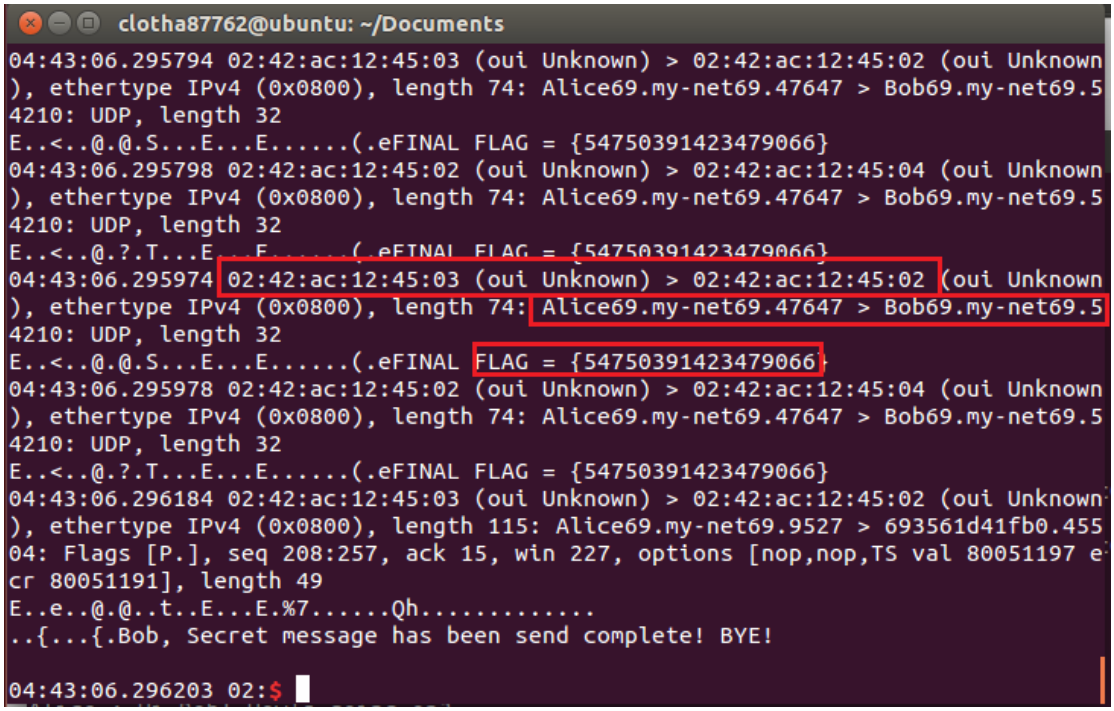
Network Security Project3 Report

A022029 邱政凱

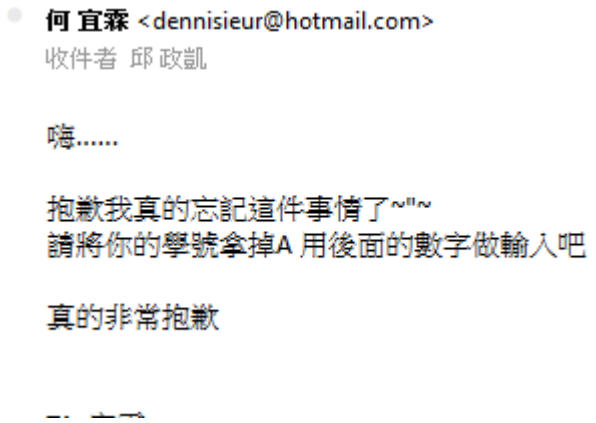








提醒助教，因為 Alice 的 server 沒辦法處理校際選修學生的學號(有英文字母)的狀況，所以助教叫我拿掉前面的 A，輸入 022029 當作學號給 ALICE，所以以上的 FLAG 是輸入 022029 之後取得的 FLAG)



Server IP / MAC : 172.18.69.2 / 02:42:ac:12:45:02

Alice IP / MAC : 172.18.69.3 / 02:42:ac:12:45:03

完成 Project 的方式：

1-1:

觀察 project3 binary 的 assembly，可以發現 PUZZLE1 函式的 stack 大小是-0x58，於是就用%N$x 的指令，從 N=0 開始一直往上執行指令。因為可能是密碼的內容的 ascii 大概都是 3x~5x(英文或數字)，所以一邊觀察因 format string 被當作參數內容噴出來的 stack 內容，在 N=28 的時候發現 stack 的內容幾乎都是 ascii 3x~5x 的值，因此認定從 N=28 開始是密碼，於是 N=29,N=30…一直到 N=32(觀察 assembly 也可以發現密碼是 18 個 byte，所以噴五個 word 出來應該差不多)，把所有內容用 little endian 的方式反轉每個 word 裡面的 byte 的順序，轉換成 ascii character，發現是 SS_IS_SO_HANDSOME

1-2

觀察 assembly，可以發現 stack ebp 的-0x14 和-0x18 應該是食物的位置，而 fgets 取得的字串會從-0x58 開始塞，因此先輸入 64 個冗餘的 byte，接著在 gdb 裡面觀察到-0x18~-0x16 都是 \x00，所以我只要再輸入一個\n(ascii value = \x0a) 把-0x15 的位置蓋掉，就發現食物出現在牢獄的正中央(因此可推斷-0x18 應是食物的 y 值，-0x14 應是 x 值)　接著走過去把食物吃掉就好了。

1-3

觀察　assembly，可以發現 fgets 從 ebp 的-0x48 開始塞。因為 return address 放在 ebp 的下一個位置，所以知道要塞 72+4 個冗餘的 byte 之後接下來塞的東西才會被放到 return address，所以先塞 76 個冗餘的 byte，接著輸入 \xc0\x8d\x04\x08(shell code 位置)。

另外一點要注意的就是我直接用 nc 連上 server 會卡死在跳到 shell code 之後，因為沒辦法接受 nc 傳回來的訊息，所以以上的步驟我都寫成 exploit.py 的 script，用 pwntools 的函式(remote 連接 server、sendline 傳輸指令、最後再跳到 shell code 之後呼叫 Interacitve()來操作 shell)。

2-1

先用 ifconfig 觀察 server 的 IP 和 MAC Address，得知 IP 是 172.19.69.2，因此要得知同一個子網內的其他電腦的資訊，我只需要用 nmap -sL 172.18.69.0/24　這個指令就可以抓出同一個子網內所有電腦的 IP。之後可以發現 Alice 的電腦是 172.18.69.3 這個位置。接著使用 nmap -p X-Y 172.18.69.3，X/Y = 0/1000 , 1001/2000 , 2001/3000…以一千個 PORT 為單位逐次掃描 Alice 的 Port，發現 9527 的 port 是開著的。(另外可以發現 Bob 是 172.18.69.4)

2-2

先用 echo　1 > ../../writable-proc/sys/net/ipv4/ip_nonlocal_bind 做好 ARP SPOOF 的前置設定(讓我可以傳送非自己 IP 位置的 ARP MESSAGE)。接著用 arping –c 1 –U –s 172.18.69.4 –I eth0 172.18.69.3 2>&1 的指令，把 Bob IP 對應的 mac address 偽裝成自己 eth0 的介面 MAC Address。

接著開另一台 terminal，進入 shell，輸入 tcpdump –e –i eth0 –A host 172.18.69.3 監聽 Alice 傳出來的訊息，轉換成 ASCII 輸出並同時印出 MAC Address。
最後直接 nc 172.18.69.3 9527，輸入學號(022029)。觀察另一台 terminal 就可以得到 flag 了。

經過這次的作業，總算是對於軟體上可能的漏洞有了一個初步的認知。以前寫 code 的時候不會 care 那麼多，經常使用很危險的 function(gets…)，從沒想過從這麼小的一個漏洞有可能造成整台電腦的控制被奪走的狀況發生。經由這次的 part 1，學到了這些漏洞的原理以及操作來攻擊的技巧，算是很新鮮的體驗。

Part2 的部分則讓我對於當 man in the middle 會是監聽資訊的方法有了更進一步的認識和操作。同時學習到了操作 arping,nmap 和 tcpdump 的方式以及 arp spoofing 的細節。沒想到用現成的工具只要幾個簡單的指令就可以使用 ARP SPOOFING 攻擊。

給 TA 的建議：

要記得以後架 server 要考慮各種學號的狀況….XD