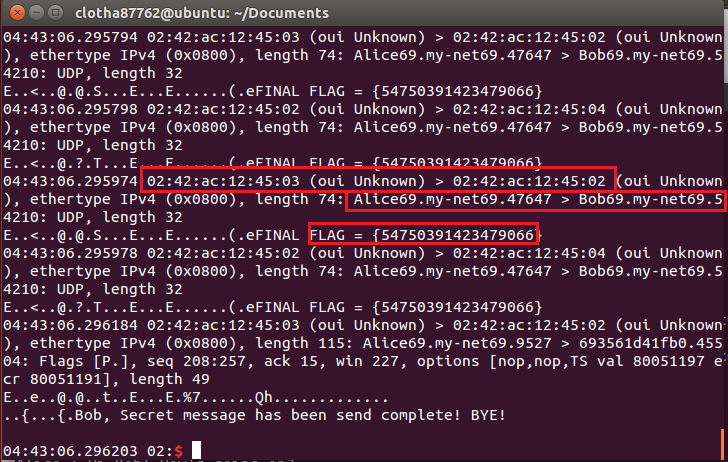
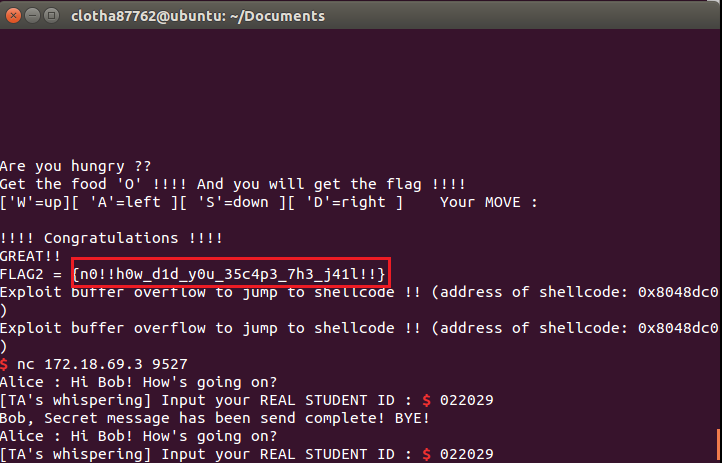
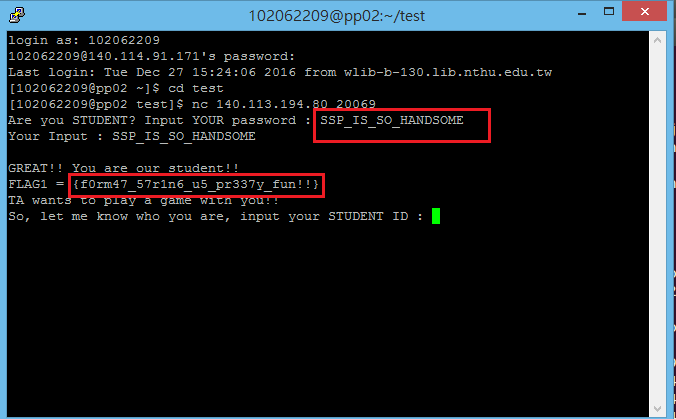
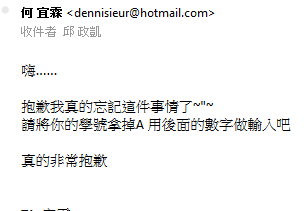
Network Security Project3 Report

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凾式的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