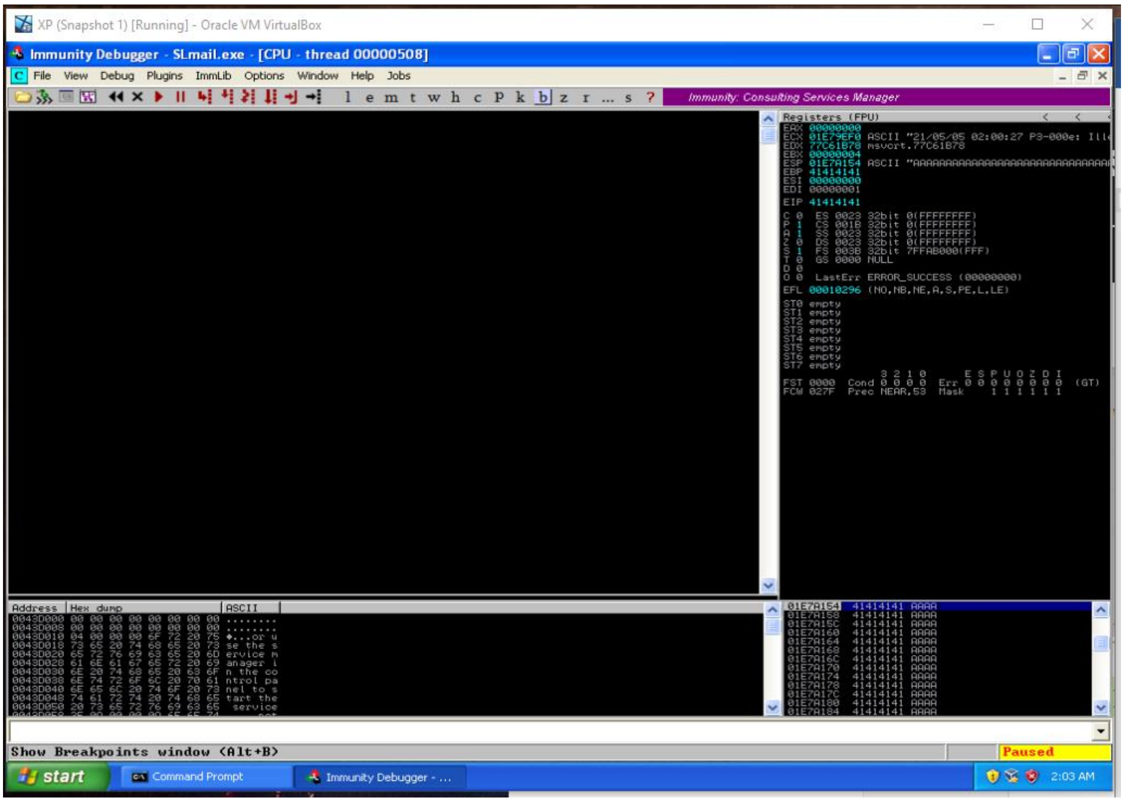
Justin Bland - 218478549
SIT379 - Task 8.1P – Week 8

Finding Exploits

Subtask 1

Fuzz SLmail by finding out how long a password string will crash the program. You should submit the following.

1. A screenshot of the SLMail crashing


XP (Snapshot 1) [Running] - Oracle VM VirtualBox
Immunity Debugger - SLmail.exe - [CPU - thread 00000508]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Manager
start
Command Prompt
Immunity Debugger - ...
2:03 AM

```
Registers (FPU)
EAX 00000000
ECX 01E79EF0 ASCII "21/05/05 02:00:27 P3-000e: Ill
EDX 77C61B78 msvcrt.77C61B78
EBX 00000004
ESP 01E7A154 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 41414141
ESI 00000000
EDI 00000001

EIP 41414141

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 1  FS 003B 32bit 7FFAB000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010296 (NO,NB,NE,A,S,PE,L,LE)

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
ST7 empty
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Address  Hex dump                 ASCII
0043D000 00 00 00 00 00 00 00 00 ........
0043D008 00 00 00 00 00 00 00 00 ........
0043D010 04 00 00 00 6F 72 20 75 ♦...or u
0043D018 73 65 20 74 68 65 20 73 se the s
0043D020 65 72 76 69 63 65 20 6D ervice m
0043D028 61 6E 61 67 65 72 20 69 anager i
0043D030 6E 20 74 68 65 20 63 6F n the co
0043D038 6E 74 72 6F 6C 20 70 61 ntrol pa
0043D040 6E 65 6C 20 74 6F 20 73 nel to s
0043D048 74 61 72 74 20 74 68 65 tart the
0043D050 20 73 65 72 76 69 63 65  service
```

```
01E7A154  41414141 AAAA
01E7A158  41414141 AAAA
01E7A15C  41414141 AAAA
01E7A160  41414141 AAAA
01E7A164  41414141 AAAA
01E7A168  41414141 AAAA
01E7A16C  41414141 AAAA
01E7A170  41414141 AAAA
01E7A174  41414141 AAAA
01E7A178  41414141 AAAA
01E7A17C  41414141 AAAA
01E7A180  41414141 AAAA
01E7A184  41414141 AAAA
```

```
Show Breakpoints window (Alt+B)                Paused
```

2. How long the string had to be before the program crashed

The password string was 2700 bytes long at the point of failure and using the pattern create/offset method we can see that the string has to be 2606 bytes long