# MsfPayload formats

There are 2 formats in msfvenom. Executable formats and transform formats (see [Metasploit unleashed](https://www.offensive-security.com/metasploit-unleashed/msfvenom/)). The first one will create an executable of some sort. exe will create a Windows executable. Elf will create a Linux executable. Psh will create a powershell script you can execute right away. And so on. The transform formats format the payload in the given format so that you can include it in a program of the same format. if you provide "C" here you will get an array of unsigned char. Up to you to use it in your C source code. You will most probably use the transform-format when writing an exploit and sending the payload over the network. If the exploit is written in ruby you'll want the payload as ruby array. I just tried format "raw": It seems to output the payload as pure binary executable code.

If your victim is a 32-bit machine, then you can use *post/multi/recon/local\_exploit\_suggester*  to find privilege escalation vulnerabilities

When creating .jsp based reverse\_shell, don’t use windows/unix exploit with payload format of jsp. Instead use, java/jsp/reverse\_shell.

Encoders *Unicode/mixed* & *Unicode/upper* have very poor [manual] ‘reliability’. So, AVOID them.

Jobs -k <job\_id > // to kill a background job

## Few important points to keep in mind

* If for a given configuration (service & OS), you have more than one exploit, then choose one with highest rank. For RANKING refer [here](https://github.com/rapid7/metasploit-framework/wiki/Exploit-Ranking)
* After running an exploit, if you are not getting the expected behavior, then try different payload. I cam across instances when payload was the problem.
* After you got a meterpreter run help command to see what commands are available. Depending upon what process meterpreter exploited, you will get different capabilities.
  + Run *getuid* to know your user account.
  + If this is failing OR your meterpreter do not have ‘good-capabilities’, then *migrate* meterpreter to different process. You may have to try more than one process to get right permissions.