

# ***Diferenças entre Payloads***

+ Para usar o script vuln do nmap dentro do metasploit:

```
db_nmap --open -p 445 --script vuln -Pn <host>
```

+ E a partir daí, começamos a procurar pelas falhas detectadas com o auxílio do **search**

+ Nesse vídeo veremos a diferença prática da execução de um exploit inline e um staged

+ Haverá também a usabilidade do meterpreter

+ no metasploit, quando damos um **sessions -l**, podemos ver as sessões em funcionamento  
→ Quando identificarmos a que queremos usar, **sessions -i 6** (caso seja a 6)