

Ataques a Hashes: Ferramentas

+ Aprenderemos aqui a usar duas ferramentas bem poderosas nesse sentido de crackeamento de hashes

john → do John the Ripper (estripador)

hashcat

+ Para verificar as opções de usabilidade do john, basta digitarmos

```
john --help
```

+ A wordlist padrão do john é encontrada em /usr/share/john/password.lst

+ Para usar o john da maneira mais básica, podemos salvar o hash em um arquivo qualquer batizado de hash e então aplicar

```
john hash
```

→ Ele já vai usar a wordlist padrão dele para tentar decifrar nossa senha

+ Para usar o john com outra wordlist, podemos

```
john --format=Raw-MD5 --wordlist=/<caminho>
```

+ A outra ferramenta é o hashcat, que ficou conhecido por também usar a GPU para o brute force, ao invés de simplesmente a CPU, o que acelera o processo

+ Podemos usar ele da seguinte maneira:

```
hashcat -m <numero correspondente ao código da criptografia> <nome do arquivo com os dados hashes>  
<caminho da wordlist> --force
```