Descobrindo Senhas com o John no Linux

+ Faremos os seguintes passos, caso tenhamos acesso ao root e, portanto, aos hashes
+ Primeiro

```
cat /etc/passwd
```

+ Copiar toda a saída para um arquivo qqer, digamos "passwd"
+ Depois

```
cat /etc/shadow
```

+ Jogar toda a saída para um arquivo qqer, digamos "shadow"
+ Usar o comando unshadow para trazê-las para um formato compreensível pelo john
+ A usabilidade dele se dá da seguinte maneira:

```
unshadow PASSWORD-FIL SHADOW-FILE
```

+ No caso, direcionamos a saída para um arquivo criado chamado hashes

```
unshadow passwd shadow > hashes
```

+ Por fim, executamos o john

```
john hashes
```

+ Se estivermos dentro da máquina linux e lá tivermos um john, poderemos aplicar diretamente o caminho dos arquivos no unshadow

```
unshadow /etc/passwd /etc/shadow > myhashes
```