# THC Hydra

O Hydra, como é mais popularmente chamado é uma ferramenta para brute force, o brute force nada mais é do que um ataque feito para quebra de senhas ou logins, em um brute force nós fazemos várias tentativas diferentes tentando descobrir a senha de um painel administrativo por exemplo, porém fazer esse tipo de processo manualmente digitando várias senhas ou logins diferentes pode ser inviável e nada eficiente, por isso existem ferramentas como o THC Hydra que automatiza esse processo para nós, vamos conhecer então algumas flags dessa ferramenta e como usa-la.

Observem esse comando:

```
hydra -l admin -P wordlist.txt 192.168.0.1
```

Agora vamos por partes, nesse comando nós iniciamos o processo chamando a ferramenta digitando o nome dela, com a flag -l nós definimos um login, no caso acima o login especificado foi admin, essa flag é utilizada quando nós já sabemos o login e não queremos que a ferramenta tente descobrir algum, logo em seguida vemos o -P (lembrando que existem diferenças entre letras maiúsculas e minúsculas) essa flag define a wordlist que iremos usar para tentar fazer a quebra da senha, não sabe o que é wordlist?

**Bom, uma wordlist é um documento de texto contendo várias e várias palavras diferentes, no caso de um wordlist de senhas, é um documento de texto contendo inúmeras senhas diferentes, são as senhas contidas nesses documentos que a ferramenta irá inserir em uma aplicação web por exemplo para tentar fazer um login.**

Voltando a explicação, depois que setamos a lista de palavras que a ferramenta irá usar como base para tentar quebrar a senha nós definimos o ip alvo, em caso de um servidor ftp de um site por exemplo, nós podemos usar a URL do site seguida da porta ou do nome ftp para especificar, exemplo:

```
hydra -l admin -P wordlist.txt http://www.siteteste.com ftp
```

Caso você não saiba o login (que geralmente é o caso) você pode usar também uma wordlist com logins comuns no hydra, basta alterar a flag -l por -L, assim:

```
hydra -L loginlist.txt -P wordlist.txt 192.168.0.1
```

Uma flag interessante de se usar no hydra é a flag -v de verbose, com essa flag você vê todo processo acontecendo no seu terminal.

```
hydra -l admin -P wordlist.txt -v 192.168.0.1
```

Você pode adicionar também a flag -f no seu comando para que a ferramenta pare de trabalhar assim que achar login ou senha, além de poder usar a flag -o para que a ferramenta salve as senhas ou logins encontrados em um documento que você escolher, veja:

```
hydra -l admin -P wordlist.txt -v -f 192.168.0.1 -o > senhaencontrada.txt
```


jcesar_n

JulioCesarNSM

**Obrigado!**