Estudando Like a Pro - WHOIS

+ O objetivo é aprender a aprender sobr o funcionamento de uma ferramenta usando o whois como exemplo.

+ Usaremos o wireshark, que é um analisador de protocolos, para ver o funcionamento do WHOIS em etapas

+ Aplica-se o filtro: tcp or udp port 43
OBS: porta 43 é a do DNS

+ Vemos que a primeira etapa é a resolução do DNS

+ Depois ele realiza a comunicação após completar o 3WHS na porta 53

+ Realiza uma query (consulta)
→ Query: businesscorp.com.br\r\n

+ Temos então a resposta (Answer)

+ Por fim, encerra-se a comunicação (FIN, ACK)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Com os resultados obtidos podemos repetir o processo fazendo conexão via netcat

```
apt install ncat
nc -v -6 2001:12ff:0:2::3 43
```

→ esse endereço grande é o ipv6, instalamos o ncat pois ele suporta esse protocolo

+ Depois de conectar, fazemos a query: businesscorp.com.br

FATO IMPORTANTE: O protocolo whois não é o mesmo para todas as regiões. Por isso está sendo substituído pelo RDAP
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~