

# ***Pesquisa via Requisições HTTP***

+ Faremos a captura do HEAD no business e no rh.business na porta 80

```
nc -v businesscorp.com.br 80
```

ou

```
nc -v rh.businesscorp.com.br 80
```

```
HEAD / HTTP/1.0
```

→ isso irá retornar informações acerca do servidor apache e do php

+ Para entender os métodos que o servidor suporta, podemos mandar uma requisição do tipo OPTIONS

OPTIONS /desec HTTP/1.0

```
root@pentest:~/Desktop# nc -v businesscorp.com.br 80
DNS fwd/rev mismatch: businesscorp.com.br != ip225.ip-37-59-174.eu
businesscorp.com.br [37.59.174.225] 80 (http) open
HEAD / HTTP/1.0
Host:businesscorp.com.br

HTTP/1.1 200 OK
Date: Thu, 26 Sep 2019 08:25:44 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Wed, 25 Sep 2019 17:05:45 GMT
ETag: "20463-1bb6-59363a9ea0957"
Accept-Ranges: byte
Content-Length: 7094
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```