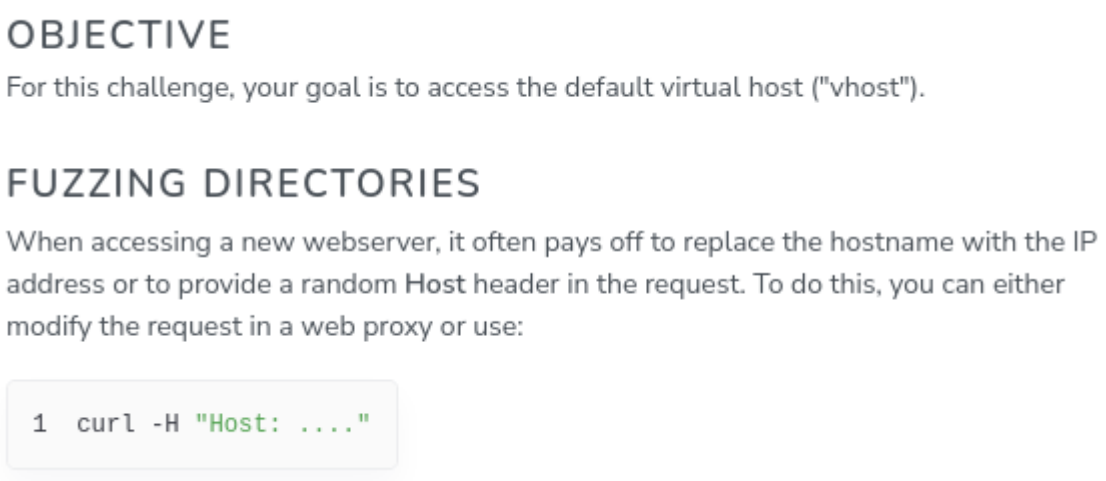
CAPTURE THE FLAG – RECON 06

Autor: ETR00M
Github: https://github.com/ETR00M/
Linkedin: https://www.linkedin.com/in/ls-anderson/

Link da Challenge: https://pentesterlab.com/exercises/recon_06/course
Nível: Fácil;
Categoria: *Recon*;
Tag: *HTTP header* (*virtual host: [vhost, host]*), ferramenta (**curl**), pensamento linear.

Neste Capture The Flag do **PentesterLab** nosso objetivo é acessar o cabeçalho de requisição e resposta do site (http://hackycorp.com/), com o intuito de modificar o campo *Host* e coletar a *flag* do desafio.



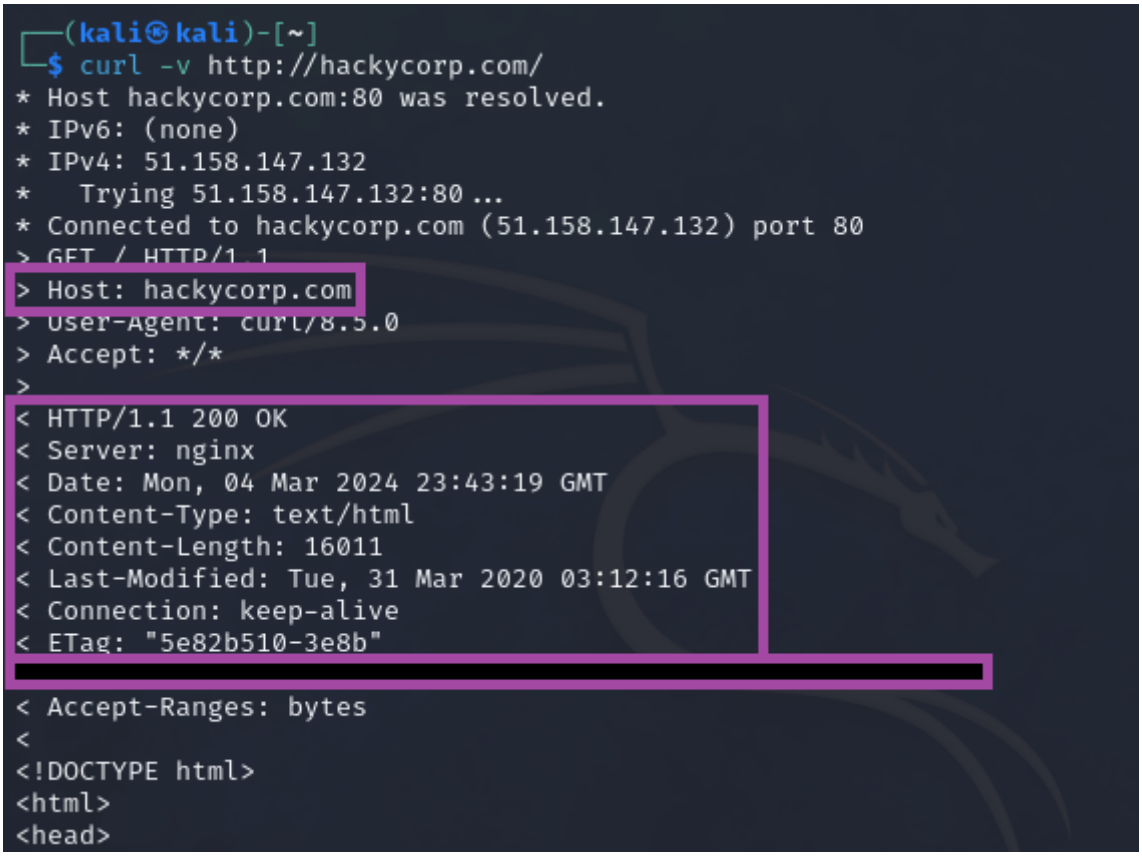
Conforme recomendado pela descrição do desafio utilizaremos a ferramenta **curl** para modificar o campo *Host* do cabeçalho HTTP, caso você não tenha conhecimento sobre *Header HTTP* e seus campos de requisição e resposta, além do uso básico do **curl**, recomendo o estudo desses assuntos antes de seguir com o *writeup*.

Dicas de materiais para estudo:

- https://www.youtube.com/watch?v=PcHbyGVoqZk&ab_channel=Refatorando
- https://www.youtube.com/watch?v=0U4xXjg_qB0&ab_channel=GuiaAn%C3%B4nima
- https://www.youtube.com/watch?v=2fze_G-G2oU&ab_channel=RicardoLongatto

Para avaliar o comportamento padrão da aplicação durante o *request* e *response* da página utilizaremos o comando abaixo coletando o cabeçalho de comunicação entre o cliente e o servidor web:

Comando: **curl -v http://hackycorp.com/**



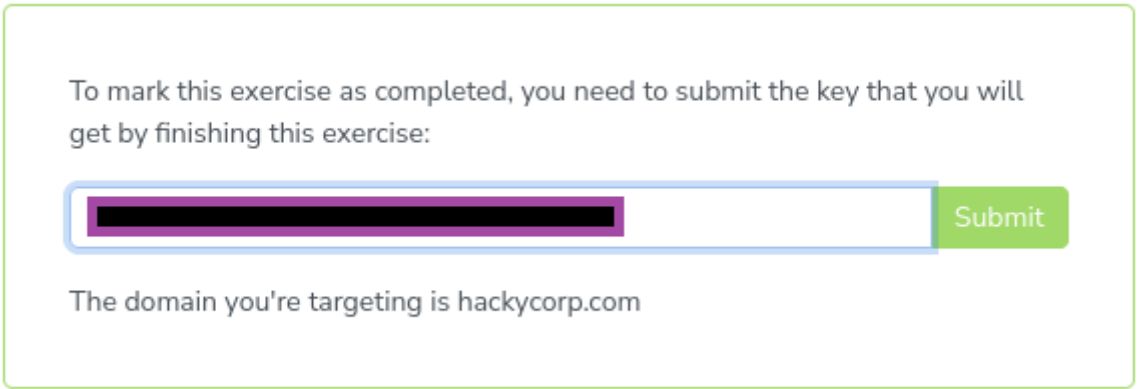
Podemos verificar que o campo *Host* identifica qual aplicação web estamos solicitando, caso o domínio seja localizado no servidor ele nos responderá com o conteúdo da página solicitada. Para completar a *challenge* precisaremos modificar o campo *Host* requisitando uma página inexistente no servidor, realizando assim um ataque chamado: *host header injection*.

Comando: **curl -H "Host: ETR00M" -v http://hackycorp.com/**

```
┌──(kali㉿kali)-[~]
└─$ curl -H "Host: ETR00M" -v http://hackycorp.com/
* Host hackycorp.com:80 was resolved.
* IPv6: (none)
* IPv4: 51.158.147.132
*   Trying 51.158.147.132:80 ...
* Connected to hackycorp.com (51.158.147.132) port 80
> GET / HTTP/1.1
> Host: ETR00M
> User-Agent: curl/8.5.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx
< Date: Mon, 04 Mar 2024 23:45:41 GMT
< Content-Type: text/html
< Content-Length: 108
< Last-Modified: Wed, 01 Apr 2020 02:55:52 GMT
< Connection: keep-alive
< ETag: "5e8402b8-6c"
<
< Accept-Ranges: bytes
<
<h1>Well done! You solved recon_06 </h1>

The key for this exercise is
* Connection #0 to host hackycorp.com left intact
```

Como resposta a esta solicitação foi encaminhado com sucesso a *flag* correspondente, sendo assim, basta a submetermos na plataforma do **PentesterLab** para completar o desafio.



Congrats you have **already finished** this exercise!

You scored this exercise (last 5 events):

- less than a minute ago