CAPTURE THE FLAG – RECON 07

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

Link da Challenge: https://pentesterlab.com/exercises/recon_07/course
Nível: Fácil;
Categoria: *Recon*;
Tag: *HTTP header* (*virtual host: [vhost, host]*), ferramenta (**curl**), pensamento linear.

Neste CTF do **PentesterLab** o nosso objetivo é modificar o campo *Host* do cabeçalho de requisição HTTP, esse *Capture the Flag* é bastante semelhante ao desafio anterior (*Recon 06*), a única modificação que faremos é utilizar a versão TLS do site, sendo assim, acessaremos sua versão segura HTTPS: (https://hackycorp.com/).

OBJECTIVE

For this challenge, your goal is to access the default virtual host ("vhost") over TLS.

DEFAULT VHOST OVER TLS

When accessing a new webserver, it often pays off to replace the hostname with the IP address or to provide a random **Host** header in the request. To do this, you can either modify the request in a web proxy or use:

```
1  curl -H "Host: ...."
```

This time you need to check the TLS version of the website to get the key

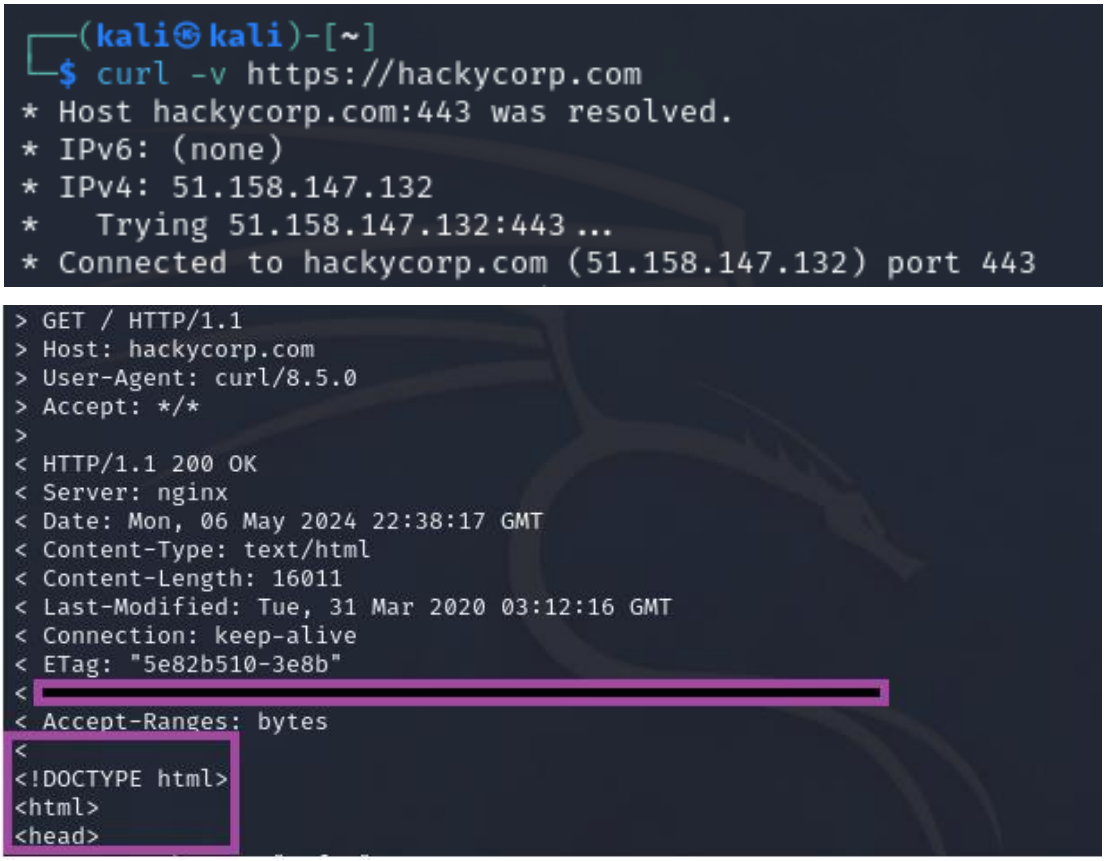
Como proposto pelo desafio, utilizaremos a ferramenta **curl** para verificar as informações presentes no cabeçalho HTTP e realizar o *host header injection*. Caso você não tenha conhecimentos sobre sobre *Header HTTP* e seus campos de requisição e resposta, além do uso básico do **curl**, recomendo 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

Primeiramente avaliaremos o comportamento padrão da aplicação ao efetuar o **curl** na página web sem quaisquer modificações nos atributos do cabeçalho HTTP.

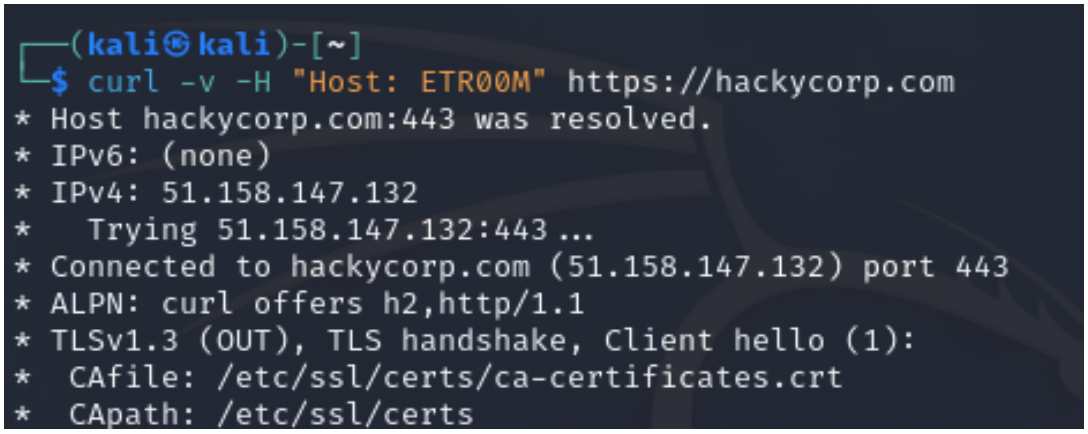
Comando: **curl -v https://hackycorp.com**

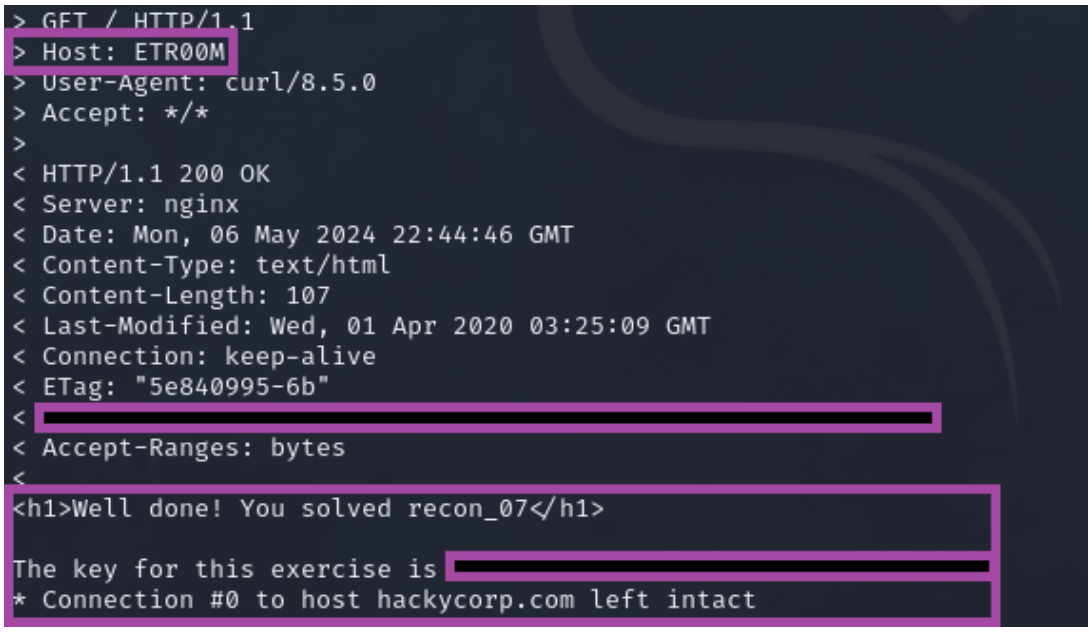


Conforme podemos avaliar o campo *Host* no cabeçalho identifica qual aplicação web estamos solicitando ao servidor, caso o domínio solicitado seja localizado, o servidor nos responderá com o conteúdo do site.

Para coletar com sucesso a *flag* e completarmos o desafio precisaremos modificar o valor do atributo *Host* solicitando uma página inexistente no servidor.

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





Com isso, agora basta submetermos a *flag* na plataforma do **PentesterLab** para completarmos a *challenge*.