



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=PcHbyGVqZk&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**

```
(kali@kali)-[~]
$ curl -v https://hackycorp.com
* Host hackycorp.com:443 was resolved.
* IPv6: (none)
* IPv4: 51.158.147.132
* Trying 51.158.147.132:443 ...
* Connected to hackycorp.com (51.158.147.132) port 443

> GET / HTTP/1.1
> Host: hackycorp.com
> User-Agent: curl/8.5.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx
< Date: Mon, 06 May 2024 22:38:17 GMT
< Content-Type: text/html
< Content-Length: 16011
< Last-Modified: Tue, 31 Mar 2020 03:12:16 GMT
< Connection: keep-alive
< ETag: "5e82b510-3e8b"
<
< Accept-Ranges: bytes
<
<!DOCTYPE html>
<html>
<head>
```



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`

```
(kali㉿kali)-[~]  
$ curl -v -H "Host: ETR00M" https://hackycorp.com  
* Host hackycorp.com:443 was resolved.  
* IPv6: (none)  
* IPv4: 51.158.147.132  
* Trying 51.158.147.132:443 ...  
* Connected to hackycorp.com (51.158.147.132) port 443  
* ALPN: curl offers h2,http/1.1  
* TLSv1.3 (OUT), TLS handshake, Client hello (1):  
* CAfile: /etc/ssl/certs/ca-certificates.crt  
* CPath: /etc/ssl/certs
```

```
> GET / HTTP/1.1  
> Host: ETR00M  
> User-Agent: curl/8.5.0  
> Accept: */*  
>  
< HTTP/1.1 200 OK  
< Server: nginx  
< Date: Mon, 06 May 2024 22:44:46 GMT  
< Content-Type: text/html  
< Content-Length: 107  
< Last-Modified: Wed, 01 Apr 2020 03:25:09 GMT  
< Connection: keep-alive  
< ETag: "5e840995-6b"  
<  
< Accept-Ranges: bytes  
<  
<h1>Well done! You solved recon_07</h1>  
The key for this exercise is  
* Connection #0 to host hackycorp.com left intact
```



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

To mark this exercise as completed, you need to submit the key that you will get by finishing this exercise:

The domain you're targeting is hackycorp.com



Congrats you have already finished this exercise!

You scored this exercise (last 5 events):

- less than a minute ago