CAPTURE THE FLAG – RECON 08

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

Link da Challenge: https://pentesterlab.com/exercises/recon_08/course
Nível: médio;
Categoria: *Recon*;
Tag: *Transport Layer Security* (TLS), certificados digitais, pensamento linear.

Para este Capture The Flag do **PentesterLab** o objetivo é verificar o campo "*Alternative Names*" no certificado TLS do site (http://hackycorp.com/). Conforme informado na descrição da *challenge*, alguns certificados podem ser validos para mais de um nome de domínio ou subdomínios, essa informação pode ser obtida através do campo *Alternative Names*.

OBJECTIVE

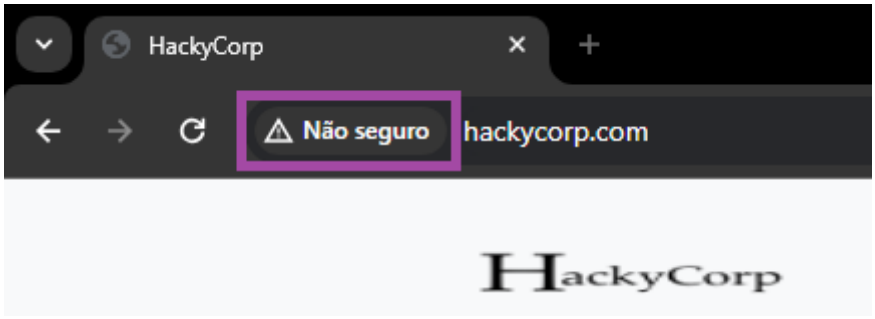
For this challenge, your goal is to access the alternative names in the certificate.

ALTERNATIVE NAMES

When accessing a TLS server, it often pays off to check the content of the certificate used. It's common for TLS servers to have certificates that are valid for more than one name (named alternative names). Looking for alternative names can be done in your client or by using **openssl**.

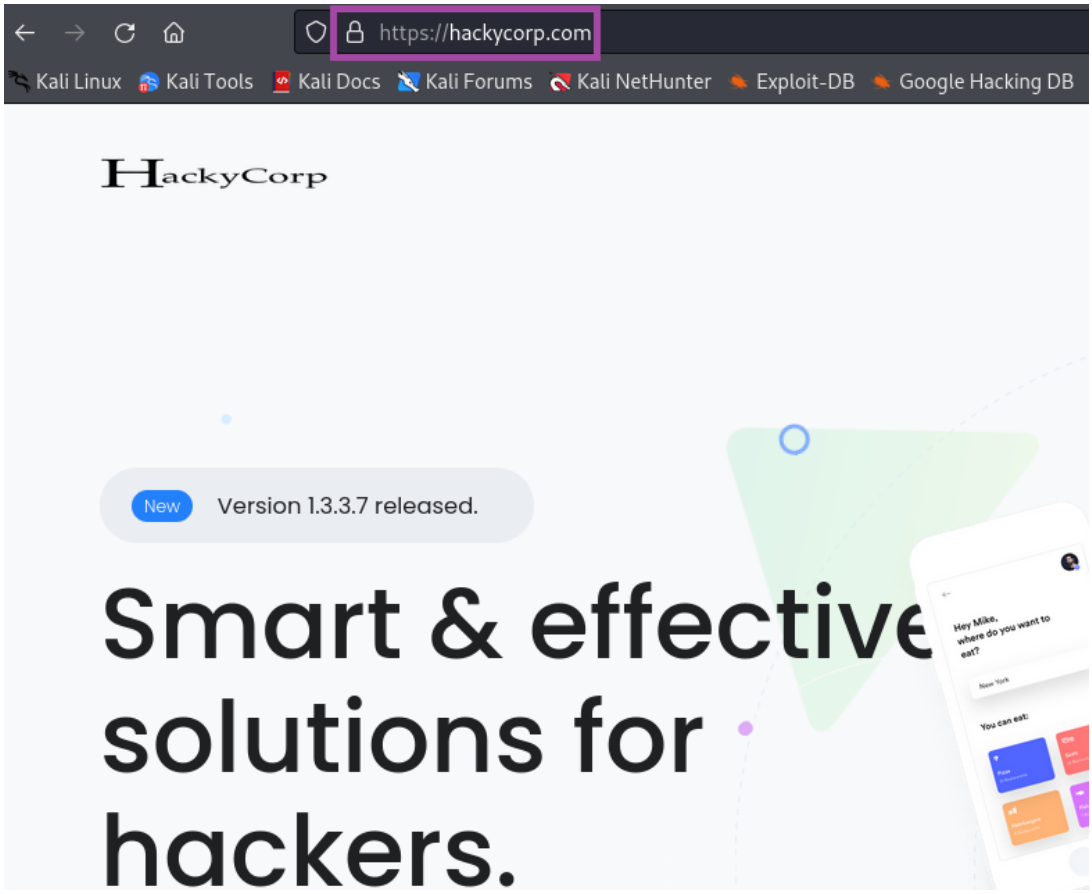
Quando acessamos um site que não possui um certificado digital válido, ou seja, não possui uma camada de segurança aplicada para troca de dados entre o cliente e o servidor os navegadores costumam informar que o site não é confiável, conforme imagem abaixo:

Comando: **http://hackycorp.com**



Como informado na descrição do desafio precisamos coletar as informações do campo *Alternative Names* do certificado TLS da página, portanto precisamos acessar o site utilizando um protocolo confiável, neste caso, substituindo o **http** por **https** na URL:

Comando: **https://hackycorp.com**

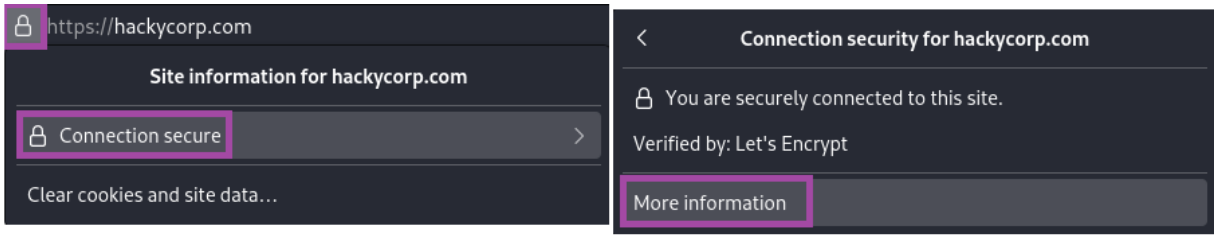


Caso você não tenha conhecimento das diferenças entre os protocolos http/https, o que são certificados digitais e o que é TLS, recomendo o estudo dos materiais abaixo antes de seguir com o *writeup*.

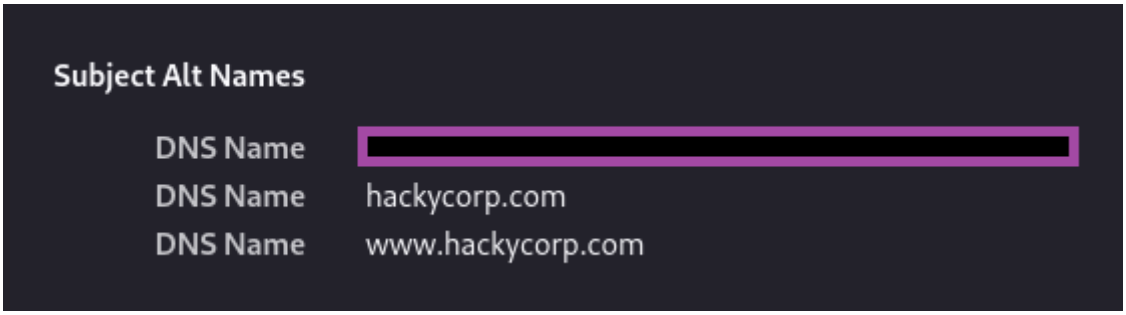
Dicas de materiais para estudo:

- https://www.youtube.com/watch?v=eOsGqXy2vmA&ab_channel=C%C3%B3digoFonteTV
- https://rockcontent.com/br/blog/tls/
- https://www.digicert.com/pt/faq/public-trust-and-certificates/what-is-a-multi-domain-san-certificate

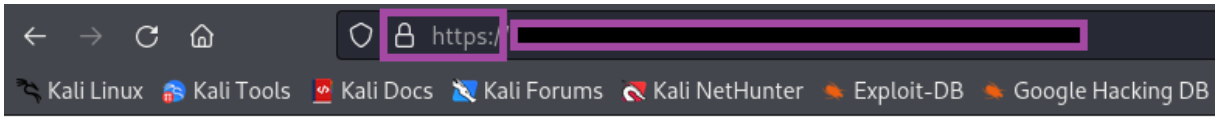
Ao clicar no simbolo de cadeado antes da URL do site no navegador (*Firefox*) teremos informações adicionais sobre o site, entre elas temos a informação de que a conexão é segura ("*Connection Secure*"), ao expandirmos esse menu de opções encontraremos a aba mais informações ("*More Information*").



Após esse processo todas as informações a respeito do certificado aplicado à página estarão disponíveis para visualização, portanto basta localizar o campo *Subject Alternative Names*, para identificar todas as páginas que o certificado é valido. Entre elas teremos uma página com nome que foge do padrão das demais.



Ao acessarmos a página coletada no passo anterior teremos como retorno a *flag* necessária para concluir o desafio:



Well done! You solved recon_08

The key for this exercise is: [redacted]

Agora basta submetermos a *flag* no campo indicado na plataforma **PentesterLab**: