CAPTURE THE FLAG – RECON 03

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

Link da Challenge: https://pentesterlab.com/exercises/recon_03/course
Nível: fácil;
Categoria: *Recon*;
Tag: páginas web (diretórios comuns), ferramentas (dirb, gobuster), *Directory Listing*, pensamento linear.

Para este Capture The Flag do **PentesterLab** o objetivo é localizar um diretório no servidor que permita a listagem de arquivos (*Directory Listening*) e acessar o arquivo exposto no site (http://hackycorp.com/).

OBJECTIVE

For this challenge, your goal is to find a directory with directory listing in the main website for hackycorp.com.

DIRECTORY LISTING

When accessing a directory on a webserver, multiple things can happen:

- an "index" file is present and it will get returned. N.B.: the file is not necessarily named index, this can be configured. But most of the time, the file will benamed index.html
- no "index" file is present and the webserver will list the content of the directory. This can obviously leak information.

Indexing directory can be disabled on most webservers. For example, with Apache, you need to use the option: -Indexes.

To find directories, with indexing turned on. You need to browse the source of the HTML pages and look at the directories used to store files. Once you have a list of directories, you can access each of them individually.

Para cumprir este desafio primeiramente precisamos entender o que é o *Directory Listening*, o autor do desafio já descreve brevemente como essa falha de configuração ocorre. Quando acessamos um servidor web uma das situações abaixo pode ocorrer:

- O diretório possui uma página HTML (HyperText Markup Language), geralmente nomeada como "index.html", que será exibida ao acessarmos o servidor a partir de um navegador.
- O diretório não possui uma página HTML a ser exibida, nesse caso o servidor web irá listar todo o conteúdo deste diretório, causando o *Directory Listing* que pode expor dados sensíveis.

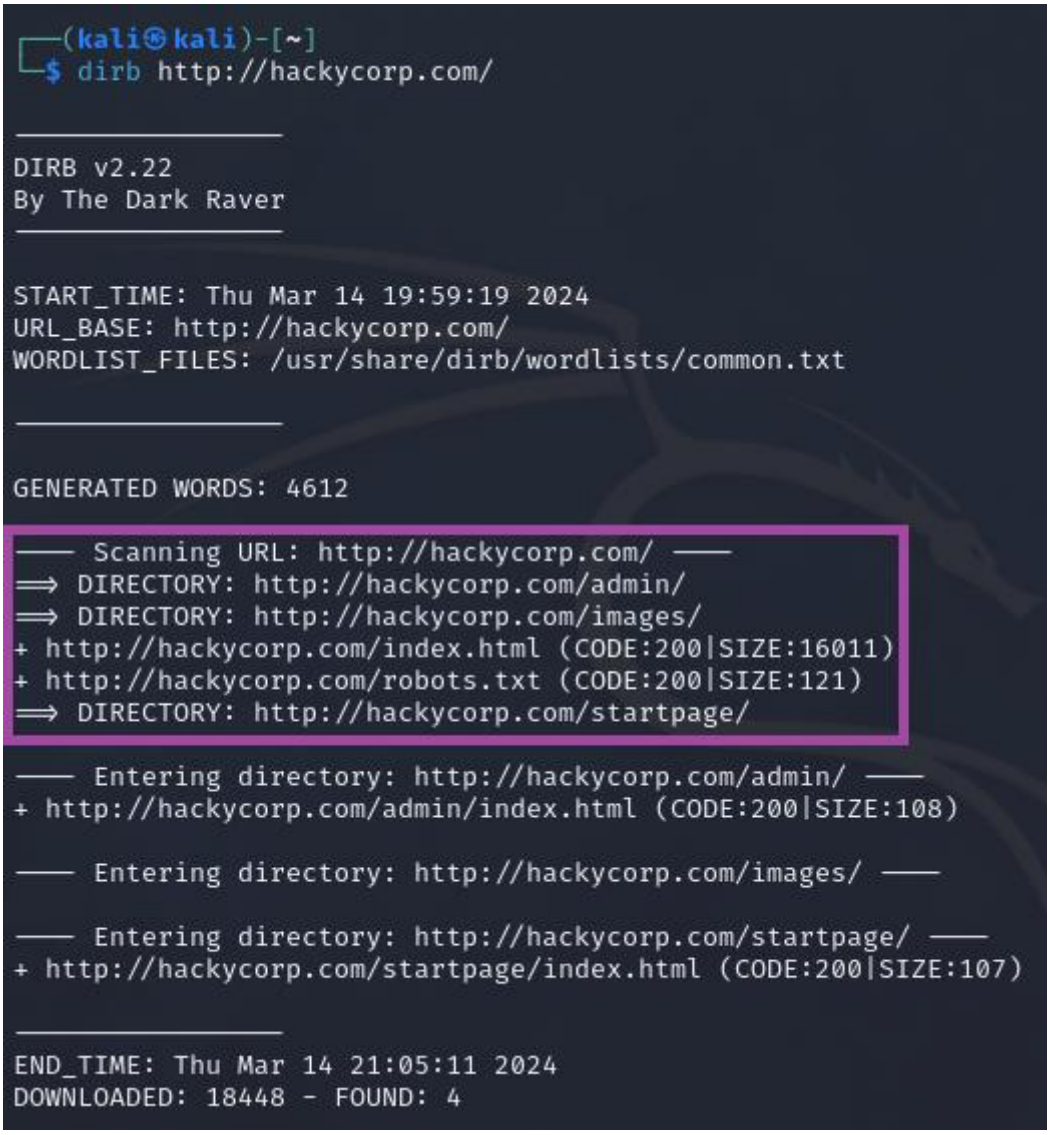
Para avançar nesta *challenge* precisamos identificar um diretório em que a listagem de diretórios pode ocorrer, temos diferentes maneiras de fazer isso, porém utilizarei a ferramenta **dirb**, recomendo o entendimento do que ela faz e como utilizá-la antes de seguir com o *writeup*.

Dicas de materiais para estudo:

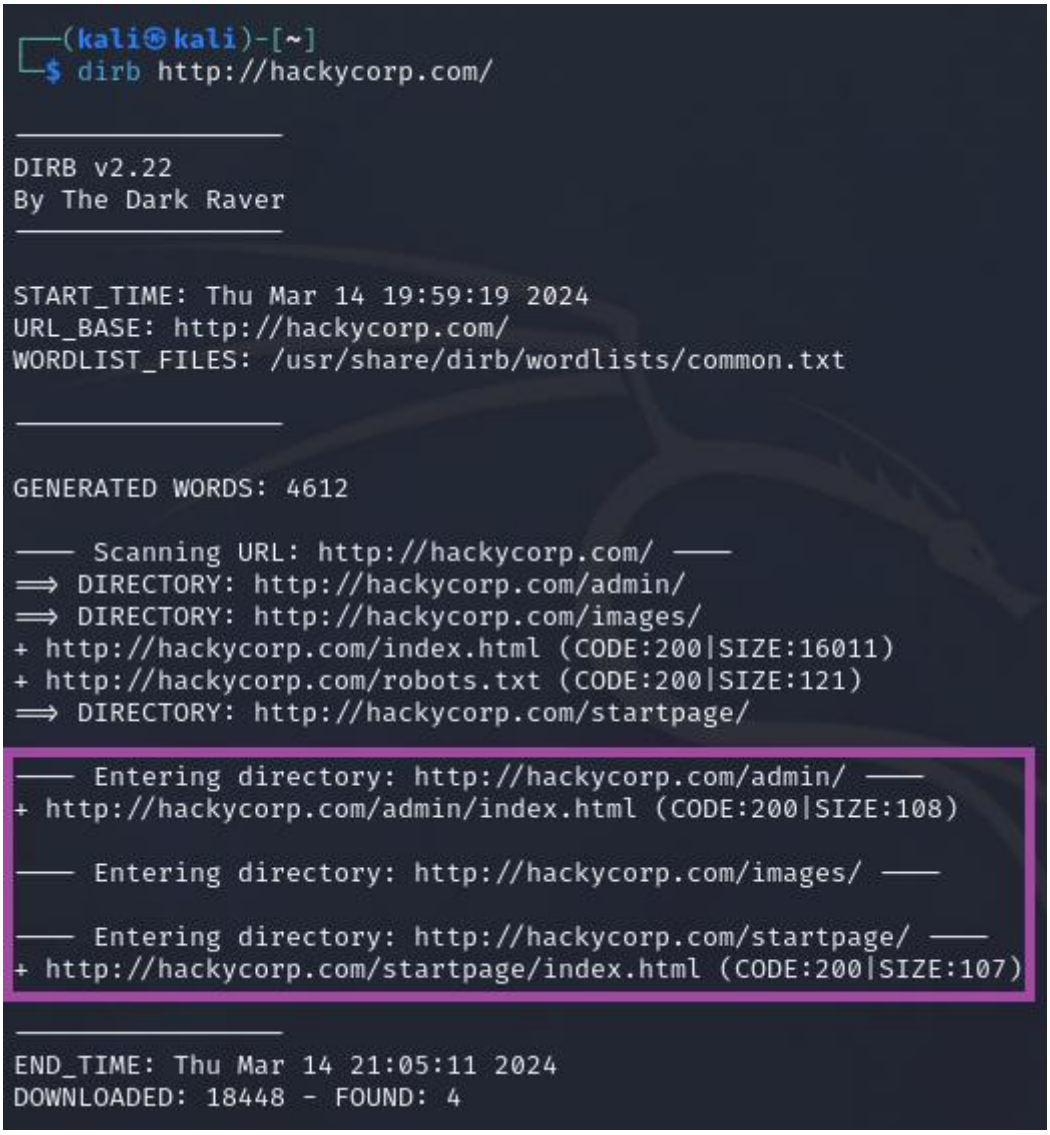
- https://www.youtube.com/watch?v=hGZPjnrGzKg&ab_channel=RicardoLongatto
- https://medium.com/@marquesag/como-obter-os-diret%C3%B3rios-de-um-servidor-coleta-de-informa%C3%A7%C3%B5es-dirb-a5407fd42310

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

Com o comando acima, utilizaremos a *wordlist* padrão do **dirb** ("*common.txt*"), podemos notar que foram encontrados 3 diretórios (identificados pelas linhas iniciadas por: "**==> DIRECTORY**"), sendo eles: *admin*, *images* e *startpages*:

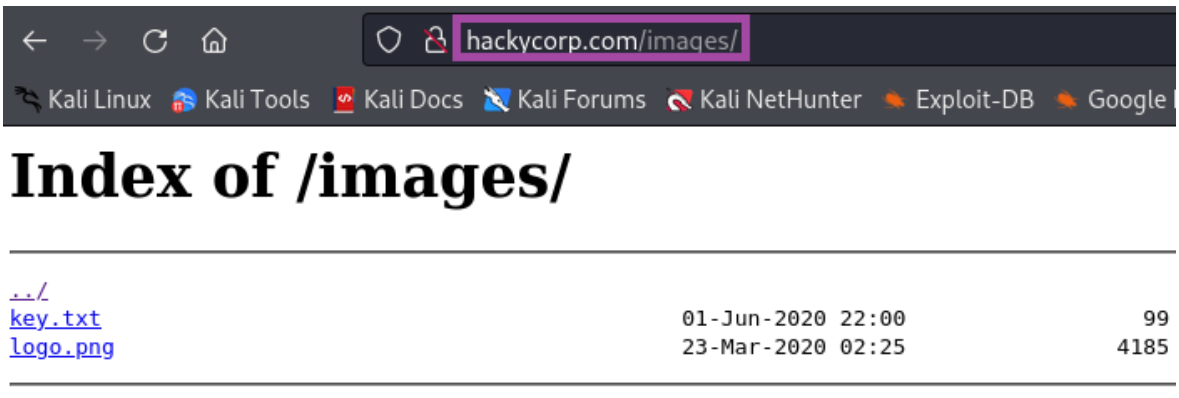


Ao finalizar a identificação dos arquivos e diretórios na raiz do servidor web o **dirb** tentou localizar novos arquivos e diretórios dentro de cada diretório encontrado anteriormente (*admin, images* e *startpage*), como resultado podemos identificar que apenas o diretório *images* não possui uma página "*index.html*", sendo assim caso não tenha sido aplicado nenhum controle de acesso poderemos listar seu conteúdo evidenciando a falha *Directory Listing*:

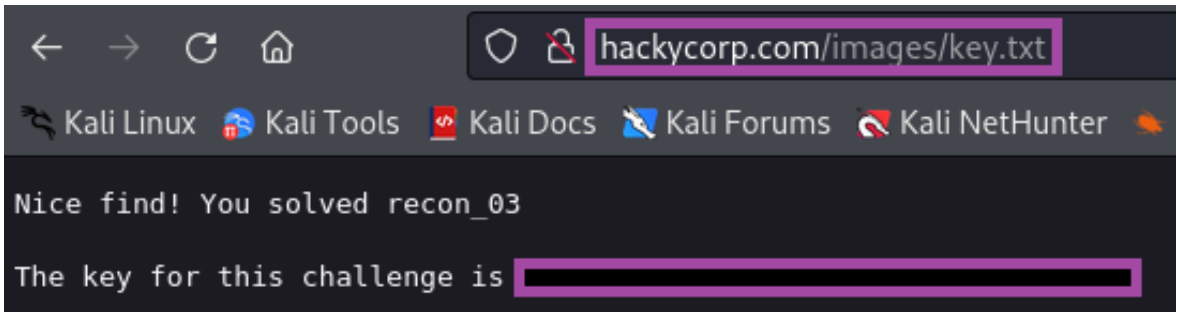


Ao acessar o diretório *images* a partir do navegador temos como retorno a listagem de dois arquivos: "*key.txt*" e "*logo.png*":

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



No conteúdo do arquivo "*key.txt*" localizaremos a *flag* para concluir este desafio.



Agora basta submetermos a *flag* na plataforma do **PentesterLab**: