CAPTURE THE FLAG – RECON 05

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

Link da Challenge: https://pentesterlab.com/exercises/recon_05/course
Nível: médio;
Categoria: *Recon*;
Tag: *Brute Force* e *Fuzzing* (conceito), ferramentas (dirb), pensamento linear.

Neste desafio do **PentesterLab** o objetivo é localizar e acessar um diretório que não é referenciado no código fonte do site (http://hackycorp.com/), portanto teremos que utilizar o método de *fuzzing* a partir de uma ferramenta automatizada.

OBJECTIVE

For this challenge, your goal is to find a directory that is not directly accessible.

FUZZING DIRECTORIES

When accessing a new webserver, it often pays off to brute force directories. To do this, you can use many tools like patator, FFUF or WFuzz (amongst many others).

Conforme indicado na descrição do desafio, durante a fase de reconhecimento frequentemente precisaremos realizar a descoberta de diretórios em um servidor web, na maioria das vezes utilizaremos métodos de *Brute Force* buscando essa identificação.

Caso você não tenha conhecimento prévio sobre utilização de ferramentas para *Brute Force* e *Fuzzing* de diretórios, recomendo o estudo do assunto antes de seguir com o *writeup*:

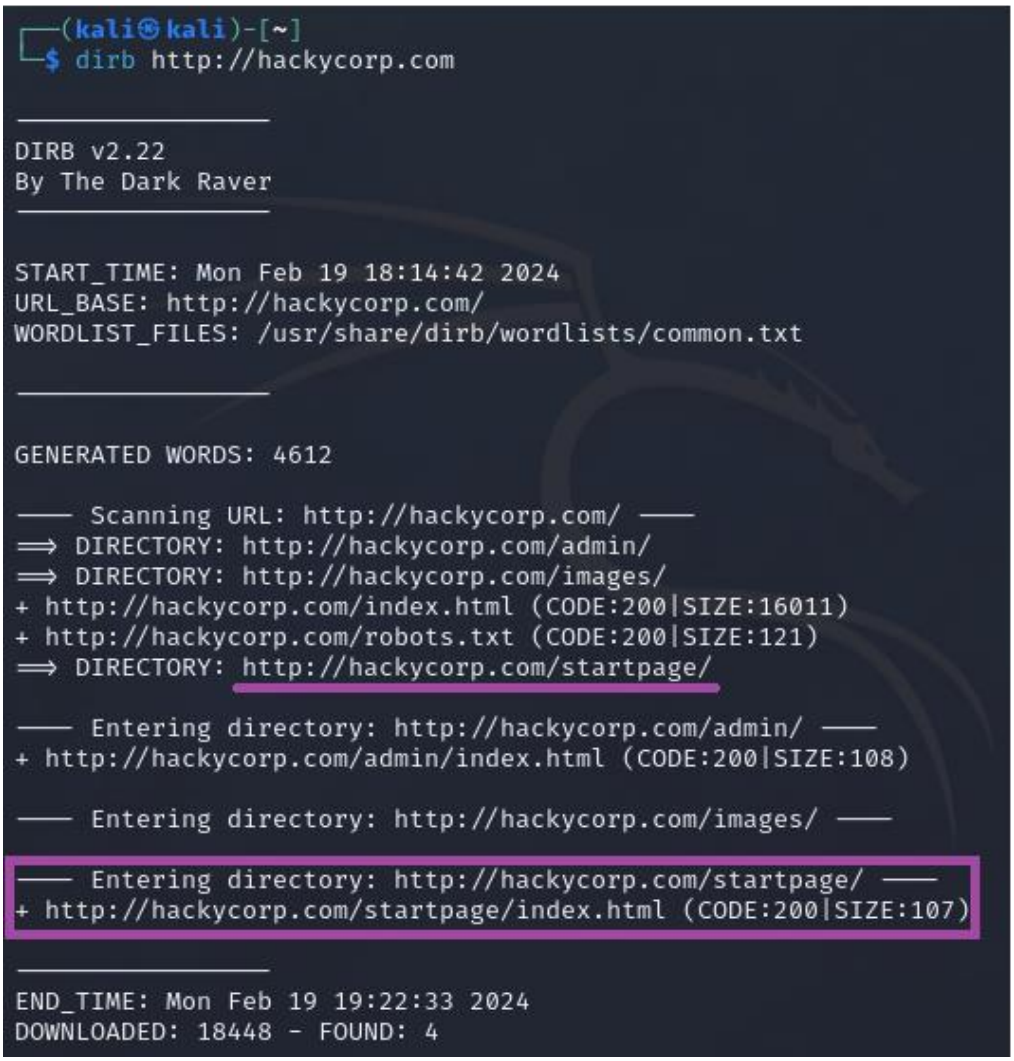
Dicas de materiais para estudo:

- https://medium.com/@marquesag/como-obter-os-diret%C3%B3rios-de-um-servidor-coleta-de-informa%C3%A7%C3%B5es-dirb-a5407fd42310
- https://www.youtube.com/watch?v=hGZPjnrGzKg&ab_channel=RicardoLongatto
- https://www.youtube.com/watch?v=LznuaFjebQ4&ab_channel=RicardoLongatto
- https://www.youtube.com/watch?v=F4545IWnaAA&ab_channel=SolydOffensiveSecurity

Para realizar o *Fuzzing* de diretórios podemos utilizar diversas ferramentas com este propósito, porém utilizarei o **dirb**.

O **dirb** utilizará por padrão a *wordlist "common.txt"* quando não for especificado qual arquivo nós queremos utilizar, para este desafio a *wordlist* padrão será suficiente para o *Brute Force* bem-sucedido.

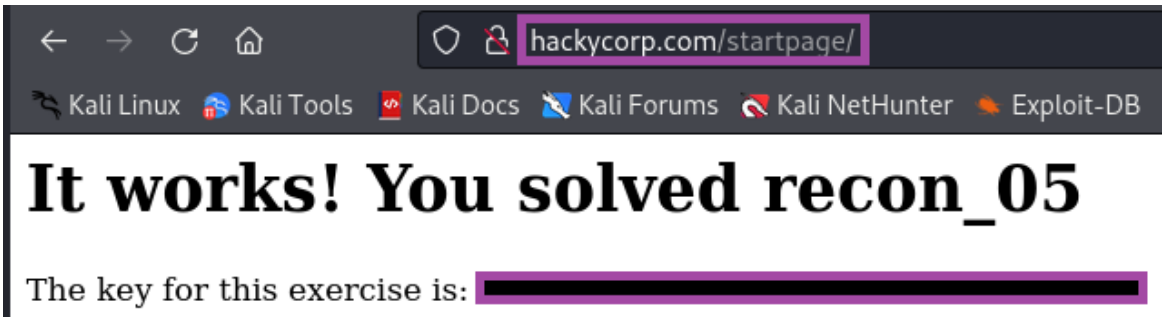
Comando: **dirb http://hackycorp.com**



Com o comando acima identificamos três diretórios na raiz do servidor web, sendo eles: *admin*, *images* e *startpage*, após finalizar as tentativas a partir da *wordlist* o **dirb** automaticamente iniciará outro *Brute Force* dentro dos diretórios encontrados anteriormente na tentativa de localizar novos arquivos e diretórios.

Com a finalização do processo de *Fuzzing* localizamos dois diretórios que possuem uma página **index**, */admin* e */startpage*, ao realizar o acesso conseguiremos a *flag* para completar o desafio:

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



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