CAPTURE THE FLAG – RECON 04

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

Link da Challenge: https://pentesterlab.com/exercises/recon_04/course
Nível: médio;
Categoria: *Recon*;
Tag: páginas web (diretórios comuns), pensamento linear.

Para este Capture The Flag do **PentesterLab** o objetivo é conhecer diretórios e arquivos comuns a serem avaliados durante os testes em aplicações web, neste caso conforme a descrição da *challenge* precisaremos apenas acessar o diretório "**/admin/**" no site (http://hackycorp.com/).

OBJECTIVE

For this challenge, your goal is to find a directory that is commonly used to manage applications.

INTERESTING DIRECTORIES

When accessing a new webserver, it often pays off to manually check for some directories before starting to brute force using a tool. For example, you can manually check for /admin/.

Durante a fase de reconhecimento e levantamento de informações iniciais é muito importante conhecer os padrões de desenvolvimento, diretórios e arquivos comuns passíveis de serem encontrados em uma aplicação web.

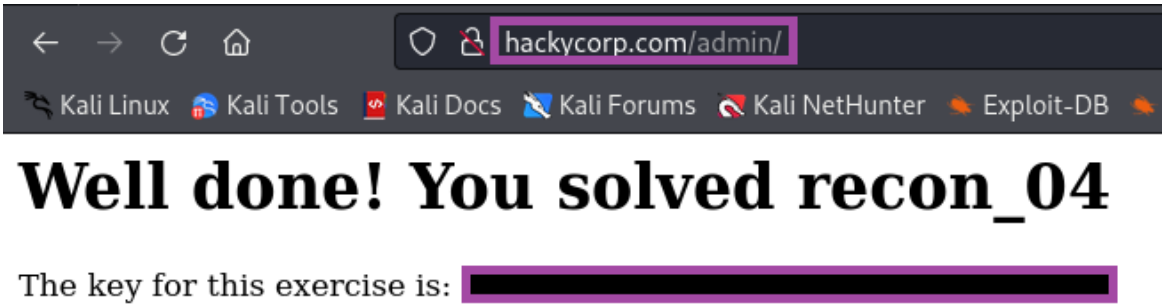
Entre elas as páginas administrativas são pontos de entrada relevantes que devem ser mapeados durante o reconhecimento, caso você não conheça sobre este tema recomendo estudar o assunto antes de seguir com o *writeup*.

Dicas de materiais para estudo:

- https://www.youtube.com/watch?v=-0Napp_9mFg&ab_channel=RicardoLongatto

A verificação da estrutura de um site pode ser feita de diferentes formas, manualmente ou a partir de ferramentas automatizadas, porém como na descrição do CTF o autor nos informou qual diretório devemos acessar, iremos direto para ele:

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



Após acessar com sucesso o diretório **/admin/** teremos como retorno uma página web informando a *flag* necessária para completar o desafio, portanto basta a submeter na plataforma para completar esta *challenge*.