CAPTURE THE FLAG – RECON 10

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

Link da Challenge: https://pentesterlab.com/exercises/recon_10/course
Nível: médio;
Categoria: *Recon*;
Tag: desenvolvimento de *scripts* (variáveis, *if-else* e *for*), ferramentas (Aquatone), pensamento linear.

O objetivo deste desafio da plataforma **PentesterLab** é realizar um *visual reconnaissance* nos sites presentes nos subdomínios da **hackycorp.com**.

OBJECTIVE

For this challenge, your goal is to use visual reconnaissance. You will need to find the website with the key in red.

VISUAL RECONNAISSANCE

For this challenge, the web applications are hosted under: 0x["%02x"].a.hackycorp.com as in:

- 0x00.a.hackycorp.com
- 0x01.a.hackycorp.com
- ...
- 0x0a.a.hackycorp.com
- 0x0b.a.hackycorp.com
- ...

If you haven't done visual reconnaissance before, you can try to use the tool Aquatone to get images that you can browse easily to find the right key.

Conforme a descrição da *challenge* existem diferentes aplicações web hospedadas nos subdomínios **0x[**].a.hackycorp.com**, porém somente uma delas conterá uma *string* escrito em vermelho representando a *flag* necessária para completar o desafio.

O autor do desafio nos recomenda a utilização da ferramenta **Aquatone** para realizar a análise (https://github.com/michenriksen/aquatone/releases/), caso você não tenha conhecimento sobre hexadecimal, ferramenta **Aquatone**, linguagem de programação ou desenvolvimento de scripts básico (variável, *if-else, for*) e comandos Linux, recomendo o estudo dos materiais abaixo antes de seguir com o *writeup*.

Dicas de materiais para estudo:

- https://www.youtube.com/watch?v=H9ggk9_IKV8&ab_channel=Eai...Qualteupapo%3F
- https://www.youtube.com/watch?v=EOLPUc6oo-w&list=PLucm8g_ezqNrYgjXC8_CgbvHbvI7dDfhs&ab_channel=B%C3%B3sonTreinamentos

Comando: **unzip aquatone_linux_amd64_1.7.0.zip**

Conforme já visto na descrição do desafio, a *flag* pode estar em qualquer subdomínio seguindo o padrão de nomenclatura **0x[**].a.hackycorp.com**, sendo que a parte indicada por "**[**]**" é variável, podendo conter quaisquer valores hexadecimal de dois caracteres, sendo assim, desde **00** até **FF** totalizando **256** possibilidades (16^2).

Podemos efetuar a automatização desses valores de diversas formas, porém desenvolverei um *script* em Python que gere todas as combinações possíveis mencionadas acima.

Comando: **vi etrhexgen.py**

```
http_protocol = 'http://'
target_domain = '.a.hackycorp.com'

for i in range(256):
    if i < 16:
        print(f'{http_protocol}0x{format(i, "02x")}{target_domain}')
    else:
        print(f'{http_protocol}{hex(i)}{target_domain}')
```

Após a codificação do *script* irei executá-lo redirecionando sua saída para um arquivo "**txt**", dessa forma será criado uma *wordlist* contendo todos os subdomínios que serão avaliados pela ferramenta **Aquatone**.

Comando: **python3 etrhexgen.py > etrhexout.txt**

```
┌──(kali㉿kali)-[~/Documents/Myscripts/generator]
└─$ python3 etrhexgen.py > etrhexout.txt
```

Em seguida, utilizaremos a *wordlist* no **Aquatone** para efetuar o teste de conexão nos subdomínios e capturar uma imagem de sua tela inicial.

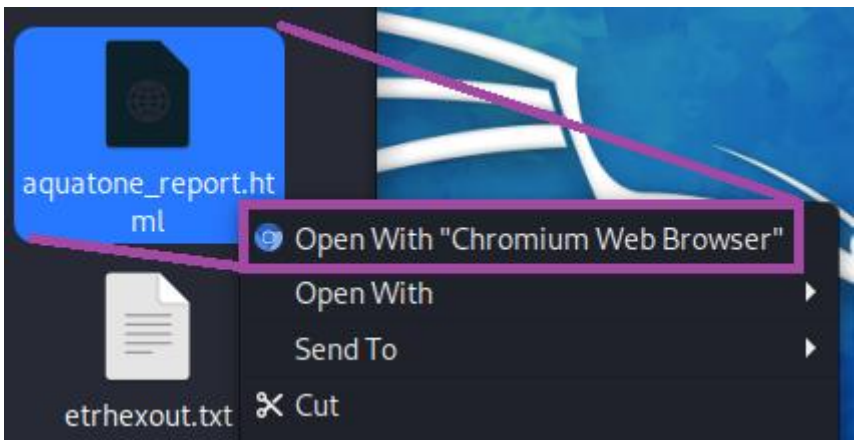
Comando: **cat etrhexout.txt | ./aquatone**

```
┌──(kali㉿kali)-[~/Documents/HackingTools/aquatone]
└─$ cat etrhexout.txt | ./aquatone
aquatone v1.7.0 started at 2024-03-19T19:52:53-04:00

Targets    : 256
Threads    : 2
Ports      : 80, 443, 8000, 8080, 8443
Output dir : .

http://0x00.a.hackycorp.com: 200 OK
http://0xf3.a.hackycorp.com: 200 OK
http://0x02.a.hackycorp.com: 200 OK
http://0x01.a.hackycorp.com: 200 OK
http://0x03.a.hackycorp.com: 200 OK
http://0x04.a.hackycorp.com: 200 OK
http://0x05.a.hackycorp.com: 200 OK
http://0x06.a.hackycorp.com: 200 OK
http://0x07.a.hackycorp.com: 200 OK
http://0x08.a.hackycorp.com: 200 OK
http://0x09.a.hackycorp.com: 200 OK
http://0x0a.a.hackycorp.com: 200 OK
http://0x0b.a.hackycorp.com: 200 OK
http://0x0c.a.hackycorp.com: 200 OK
http://0x0d.a.hackycorp.com: 200 OK
http://0x0e.a.hackycorp.com: 200 OK
```

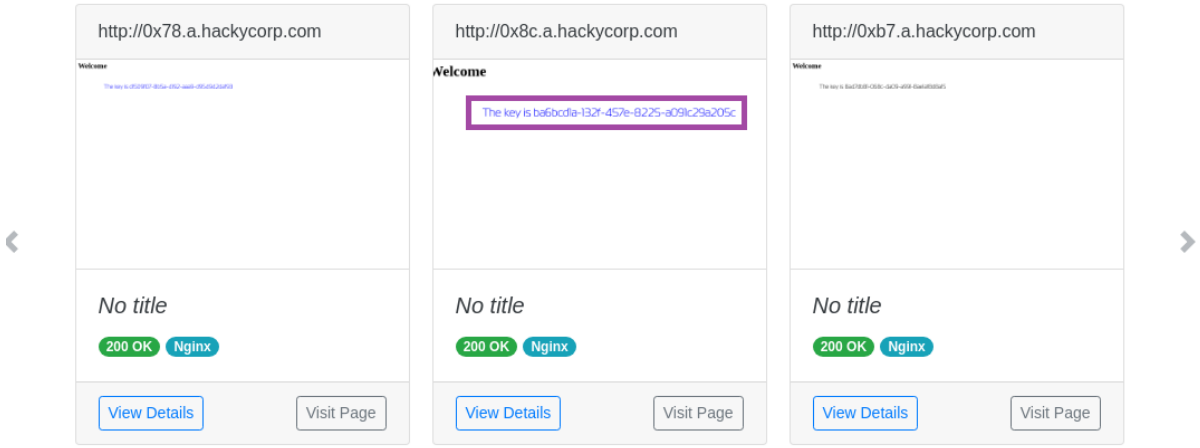
Quando a ferramenta finalizar a análise receberemos como retorno a quantidade de requisições e capturas de tela efetuadas com sucesso, o resultado será armazenado como um relatório no arquivo: "**aquatone_report.html**" para investigação manual.

```
http://0×f2.a.hackycorp.com: screenshot successful
http://0×f4.a.hackycorp.com: screenshot successful
http://0×f5.a.hackycorp.com: screenshot successful
http://0×f7.a.hackycorp.com: screenshot successful
http://0×f6.a.hackycorp.com: screenshot successful
http://0×f8.a.hackycorp.com: screenshot successful
http://0×f9.a.hackycorp.com: screenshot successful
http://0×fb.a.hackycorp.com: screenshot successful
http://0×fe.a.hackycorp.com: screenshot successful
http://0×fd.a.hackycorp.com: screenshot successful
http://0×ff.a.hackycorp.com: screenshot successful
Calculating page structures ... done
Clustering similar pages ... done
Generating HTML report ... done

Writing session file ... Time:
 - Started at  : 2024-03-19T19:52:53-04:00
 - Finished at : 2024-03-19T19:58:07-04:00
 - Duration    : 5m14s

Requests:
 - Successful : 251
 - Failed     : 5

 - 2xx : 251
 - 3xx : 0
 - 4xx : 0
 - 5xx : 0

Screenshots:
 - Successful : 251
 - Failed     : 0

Wrote HTML report to: aquatone_report.html
```

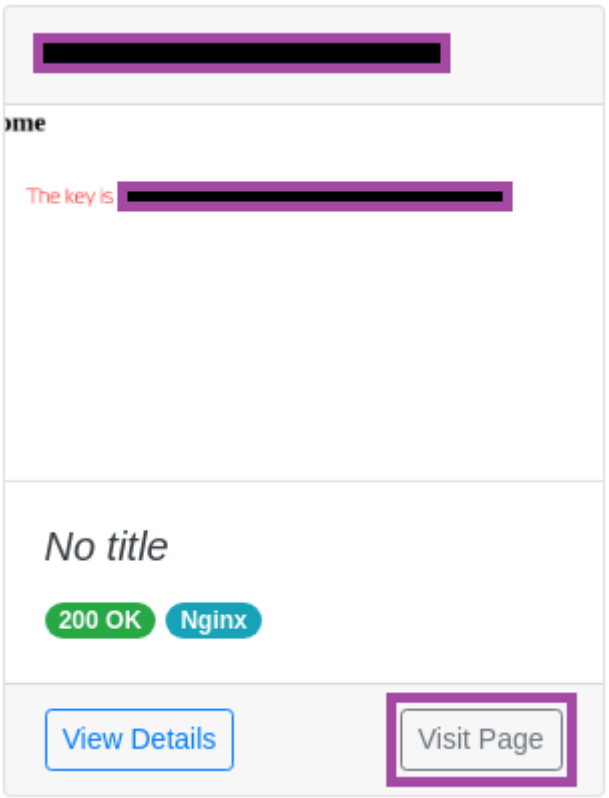
Com o resultado acima, foi possível identificar que foram encontrados 251 subdomínios, o relatório final deve ser avaliado a partir do navegador **Chromium** para melhor compatibilidade.

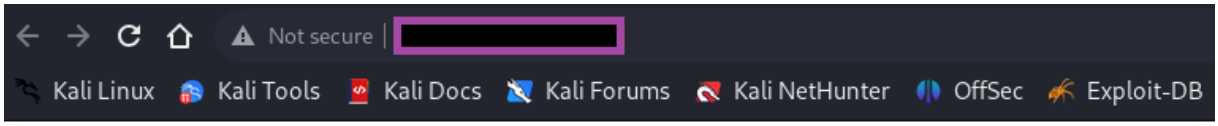


Ao abrir o relatório podemos identificar que para cada URL localizada teremos uma miniatura apresentando a captura de tela de sua página inicial, assim como detalhes da conexão efetuada, cabeçalhos coletados, status, visualização da página completa etc.



Após navegar por algum tempo no relatório analisando as capturas das páginas coletadas teremos um único resultado contendo um texto escrito em vermelho, ao clicar no botão "***Visit Page***" podemos acessá-la em outra aba do navegador, conforme abaixo:





Welcome

The key is [redacted]

Copiando o valor da *flag* podemos submetê-la na plataforma **PentesterLab** para completar o desafio.