HGAME 2021 Week2 Writeup

Misc

DNS

- 考点：流量分析 DNS
- 出题人：Akira
- 分值：100

  利用**统计**中的**协议分级**发现HTTP占了极大比重，将其过滤出来，得到：

  ```
  71 26.622102874  192.168.43.11      172.67.148.67      HTTP      427 GET / HTTP/1.1
  77 26.888779402  172.67.148.67      192.168.43.11      HTTP       60 HTTP/1.1 200 OK  (text/html)
  80 27.571341945  192.168.43.11      172.67.148.67      HTTP      410 GET /favicon.ico HTTP/1.1
  84 27.838176970  172.67.148.67      192.168.43.11      HTTP      623 HTTP/1.1 404 Not Found
  ```

  再跟踪其HTTP流，发现有以下代码：

  ```html
  <html>
  <head>
  </head>
  <body>
  <script>
              while(true){
                  alert("Flag is here but not here")
              }
          </script>
  <b>Do you know SPF?</b>
  </body>
  </html>
  ```

  以及网址：

  ```
  flag.hgame2021.cf
  ```

  根据代码加粗提示SPF，再根据题目为DNS，可联想到DNS中的SPF记录，打开Kali，在终端输入

  ```
  dig TXT flag.hgame2021.cf
  ```

  查看其SPF记录，得到Flag：

  ```
  hgame{D0main_N4me_5ystem}
  ```