1. **Flag01:**

Mô tả bài tập:

|  |  |  |  |
| --- | --- | --- | --- |
| Môi trường thực hiện | IP address | Net card | Target |
| Máy Kali Linux | 192.168.10.134 | NAT | VM |
|  | | | |
| **Bước 1:** Scan tìm IP máy mục tiêu (netdiscover) | | | |
|  | | | |
| Kết quả Scan địa chỉ mạng ta thấy được địa chỉ IP của máy Target là 192.168.10.137 | | | |
|  | | | |
| **Bước 2:** Tìm port nào đang mở trên máy Target (nmap) ta thấy port 80 đang mở và có chạy dịch vụ web dùng giao thức http:// | | | |
|  | | | |
| **Bước 3:** Scan subdomain của IP http://192.168.10.137 | | | |
|  | | | |
| Truy cập vào link: <http://192.168.10.137/readme> | | | |
|  | | | |
| Truy cập vào link này: https://shorturl.at/LFe4M | | | |
|  | | | |
| Tải 3 file này về máy | | | |
|  | | | |
| Mở flag1.zip thì file này có đặt password | | | |
|  | | | |
| Sử dụng công cụ fcrackzip và wordlist là rockyou.txt để tìm mật khẩu của tập tin flag1.zip.  **Password: pw=madeinvietnam** | | | |
|  | | | |
| Giải nén flag1.zip ra ta thấy có flag1.txt | | | |
|  | | | |
| Mở flag1.txt xem thử ta thấy có 1 chuỗi url encode | | | |
|  | | | |
| Sử dụng công cụ Cyberchef với mode **URL Decode** và chuyển đổi từ số thập phân sang ký tự ta thu được flag là “flag{uitEthicalHacking}”. | | | |
|  | | | |
|  | | | |
|  | | | |

1. **Flag 2:**

|  |
| --- |
| Tập tin flag2 có định dạng là 1 tập tin nén zip |
|  |
| **Khi giải nén yêu cầu nhập password:** |
|  |
| **Dùng công cụ fcrackzip để tìm password: pw = birmingham-city** |
|  |
|  |
| Giải nén ta có được 1 file .txt là: flag2.csv |
|  |
| Sử dụng công cụ Cyberchef với mode URL Decode và chuyển đổi từ số thập phân sang ký tự ta thu được flag là “flag{ehBCU}”. |
|  |
|  |
|  |

1. **Flag 3:** Đối với file steghide.jpg ta sử dụng công cụ steghide để trích xuất dữ liệu được nhúng trong file.

|  |
| --- |
|  |
| **Sau khi trích xuất ta được “secret.png” và mở ra ta được** “flag{taka7}” |
|  |