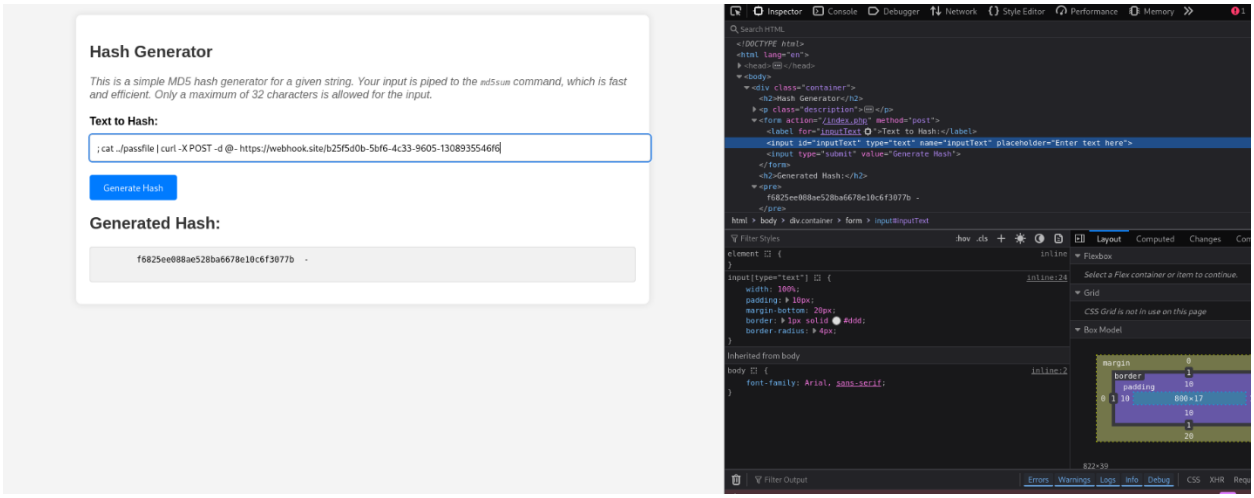
Imager

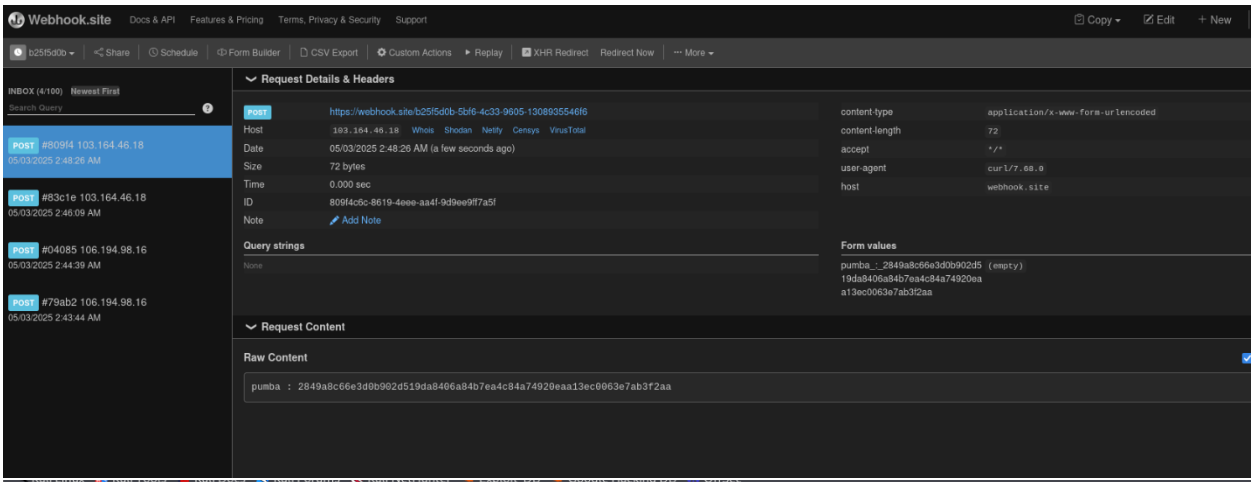
1. Nmap

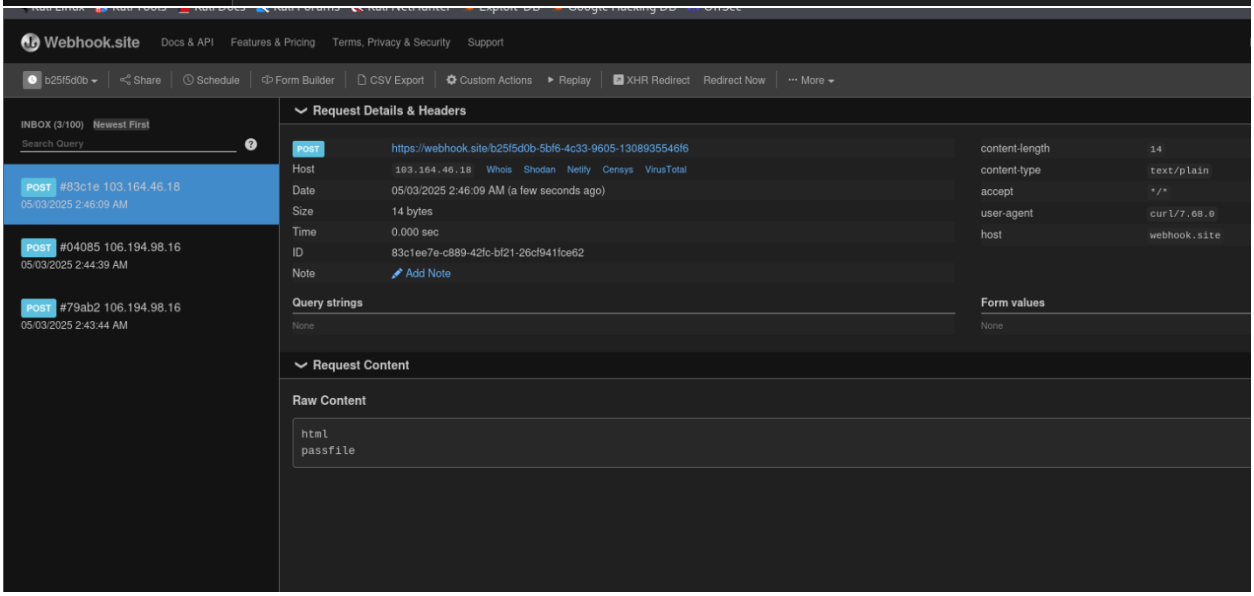
```
┌──(kali㉿kali)-[~/imagery]
└─$ cat imagery.txt
# Nmap 7.95 scan initiated Fri May  2 22:00:07 2025 as: /usr/lib/nmap/nmap --privileged -sC -sV -oN imagery.txt 192.168.154.134
Nmap scan report for 192.168.154.134
Host is up (0.00059s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 8c:82:a5:a9:05:4c:c6:e4:31:c3:cb:94:8c:72:34:08 (RSA)
|   256 60:8d:92:3d:16:3d:5e:71:0b:9a:fb:7d:a3:ca:75:02 (ECDSA)
|_  256 33:4a:b0:1f:dd:74:56:09:f7:80:b1:49:c4:cd:58:71 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Hash Generator
MAC Address: 00:0C:29:DD:BB:C8 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri May  2 22:00:14 2025 -- 1 IP address (1 host up) scanned in 7.27 seconds
```

2. RCE (trying and testing, how md5 is being generated and how input is parsed)







3. Used crack station to get text from hash of content in passfile

4. Got ssh password for user pumba

5. Ran `sudo -l`

6. Got to know about nopasswd on /usr/bin/ls and env_keep+=LD_PRELOAD which is a common privesc vector

7. Created custom shell.c script

8. Ran sudo ls with LD_PRELOAD with our custom shell module

9. Got root access