**Detailed Report of Editorial htb**

**Steps 1:** Connect to the VPN

Sudo openvpn labs\_Imdarkseid1.ovpn

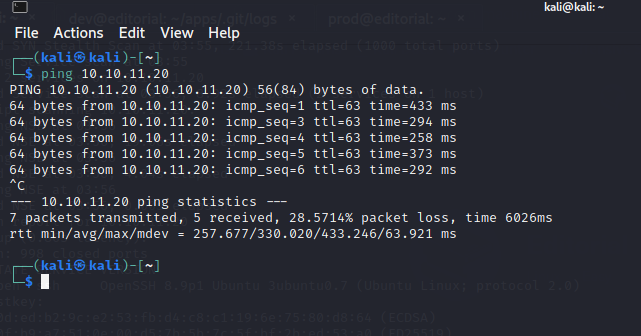
NOTE: you need to download the .ovpn file from Hack The Box itself

Connection will be established with Hack The Box.  
**Step 2:** Join the machine

IP address: 10.10.11.20

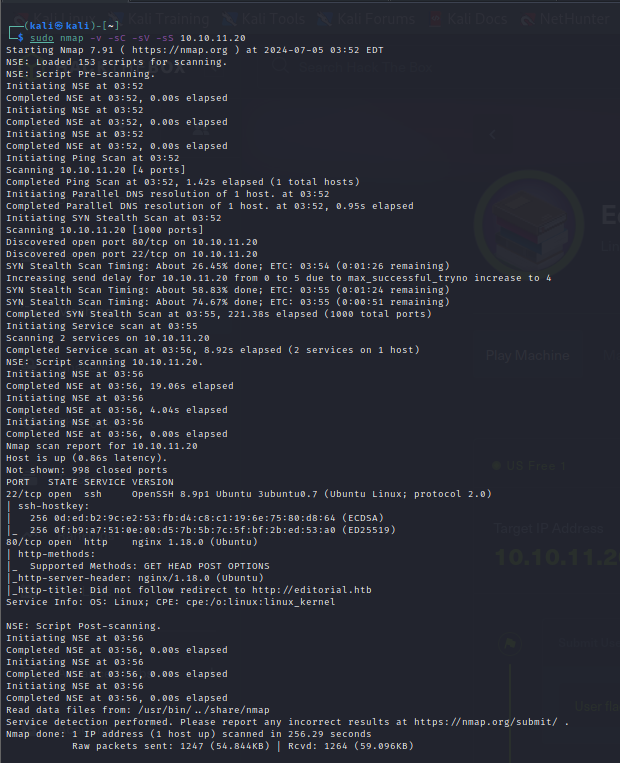
NOTE: IP address may be different

**Step 3:** Ping the IP address for the connect establishment

 Ping 10.10.11.20

**Step 4:** run nmap for active port scanning.

Sudo nmap -V –sC –sV –sS 10.10.11.20



**Step 5:** Add the IP address in our hosts.

Sudo nano /etc/hosts

10.10.11.12 editorial.htb

**Step 5:** Open the IP address in the browser

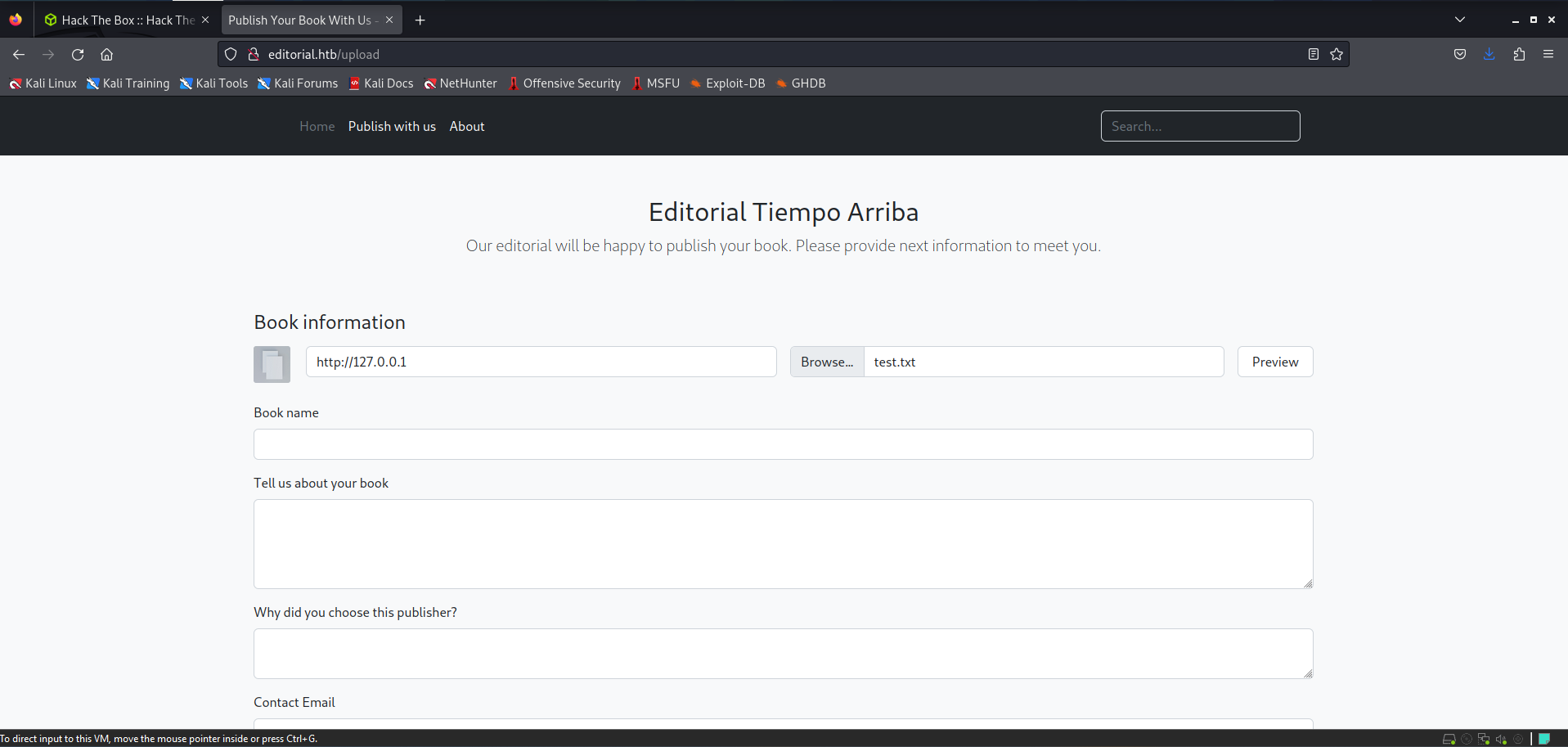
Look for Publish with us link > Click on it

Here, we can try for an upload exploit using Burpsuite tool.

**Step 6:** Create an empty txt file and place it in the desired folder.

Here, I have create test.txt file.   
 And in the place of Cover URL use you manual proxy IP address (127.0.0.1)

To setup manual **proxy address** > go to **firefox** > **setting** > search for **proxy** > **proxy settings** > enter manually the **IP address** and **Port number** which will **127.0.0.1 and 8080** respectively.

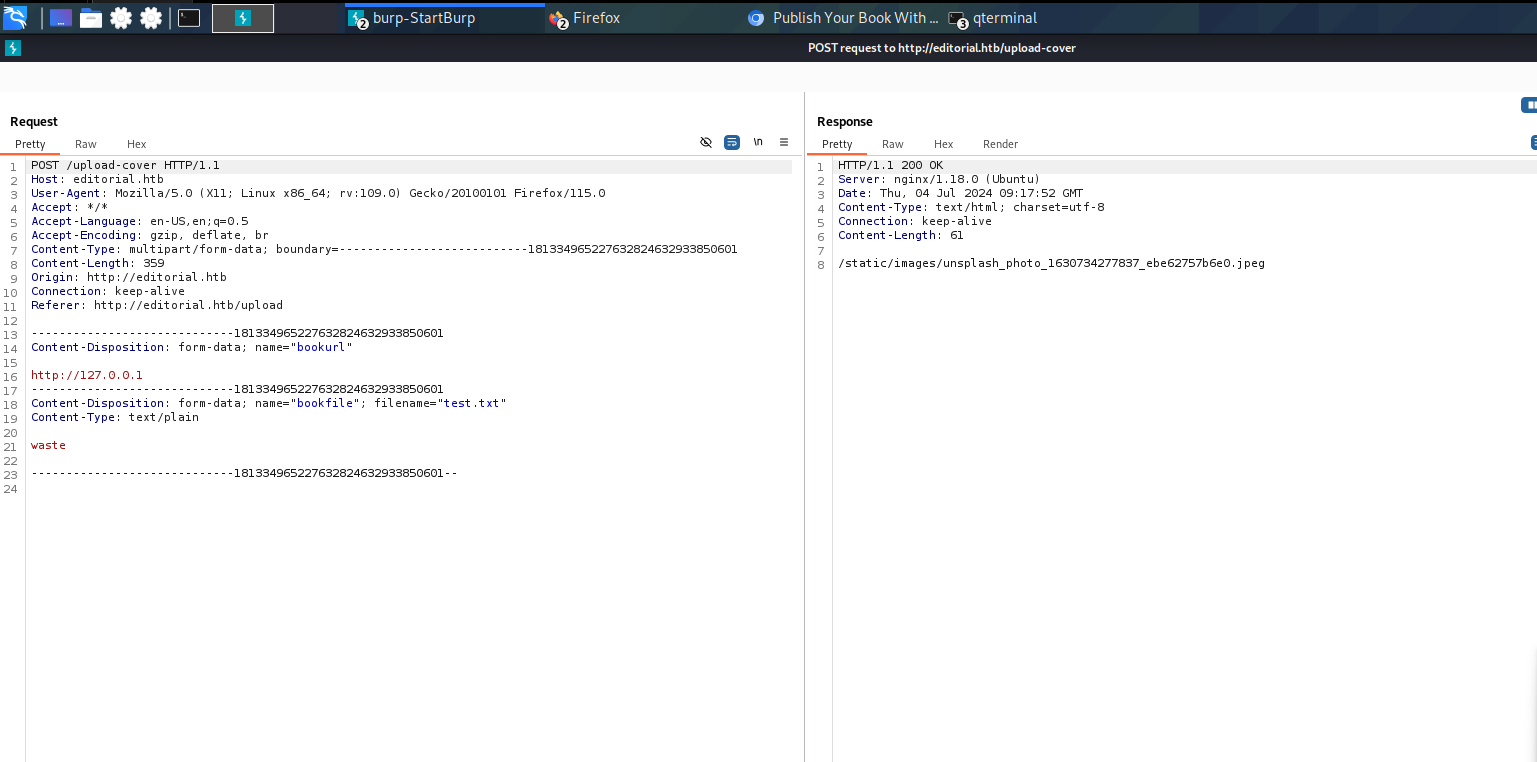


**Step 7:** Then Intercept the Preview request using BurpSuite.

NOTE: First you must install BurpSuite.

To Intercept > Open **BurpSuite** > **Proxy** > Turn **ON** Intercept Mode > Intercept the Preview request by click on Preview Button on browser > Right click on **Request** > **Send to Intruder** > Choose **Positions** > Set the **Attack Type** as **Sniper** > In the Payload Section Set **payload type as Numbers**, **Number Range From as 1 to 7000**, Step as 1. > Hit **Start Attack**.

It will proceed with the attack.



On Number 5000 you will possibly get the response.

**Step 8:** Again Open the Publish with us page and enter the discovered info.

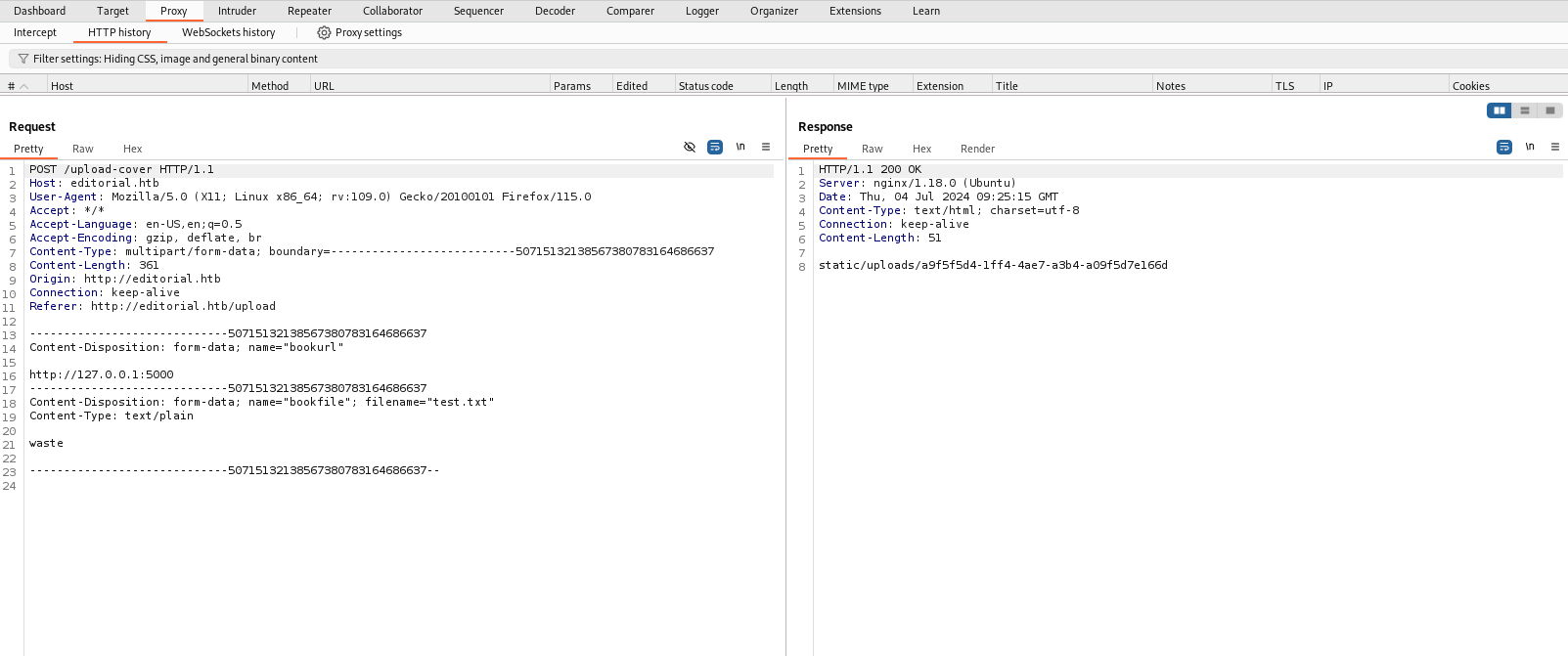
**Cover url**: <http://127.0.0.1:5000>

**Upload:** test.txt

Again Intercept the Preview request using BurpSuite.

In the request section there will **127.0.0.1:5000** and in the response section there will be a static upload file.

Copy the Static upload file for further use.



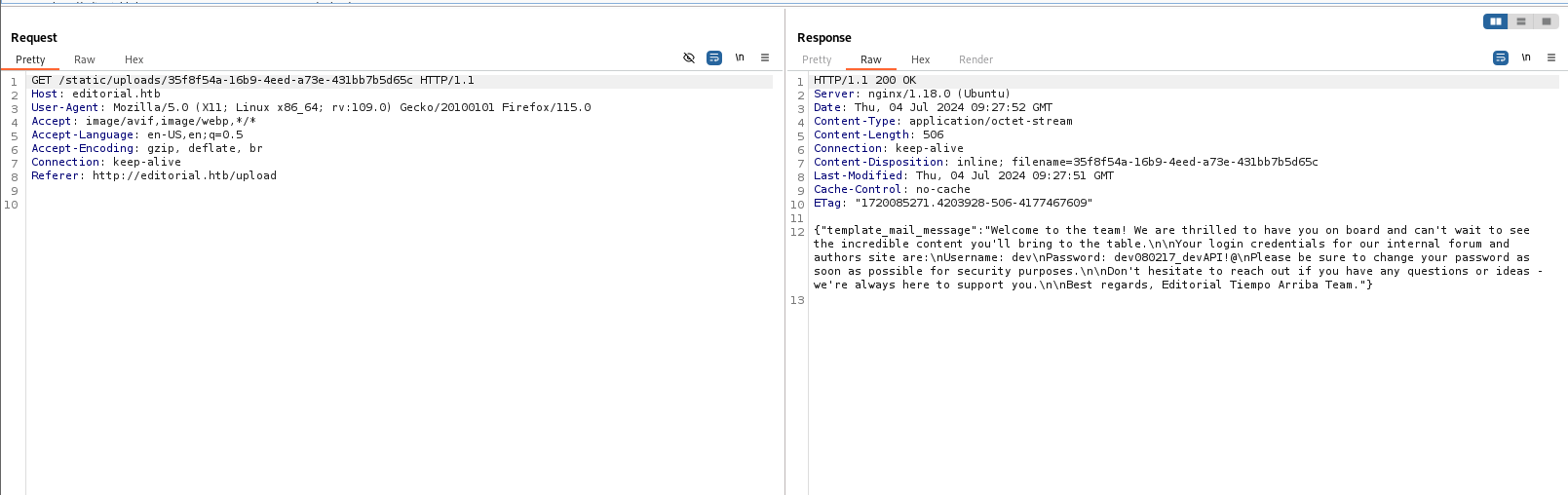
Step 9: Again open the Publish with us page and Intercept the Preview Request.

This time in the place of **Cover URL**: <http://127.0.0.1/static/uploads/api-key>

**NOTE: Remember replace the api-key with yours**.

Once you done with intercepting the response you will the user id and password.

**NOTE: user id and password may differ.**

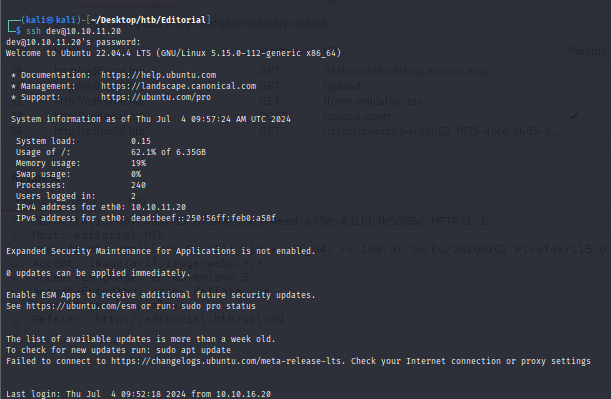
****

**Step 10:** Open you terminal and use the following command for the access of user

**ssh** [**dev@10.10.11.20**](mailto:dev@10.10.11.20)

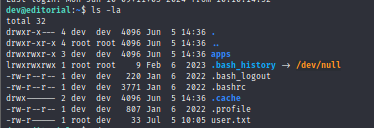
Enter the password

And you will get the access.



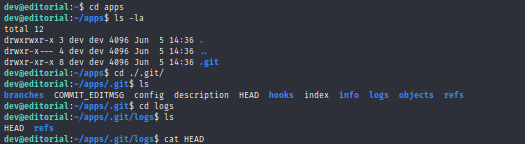
**Step 11:** Soon after getting the access, use the following command.

**ls –la** ( for the list of directory present)



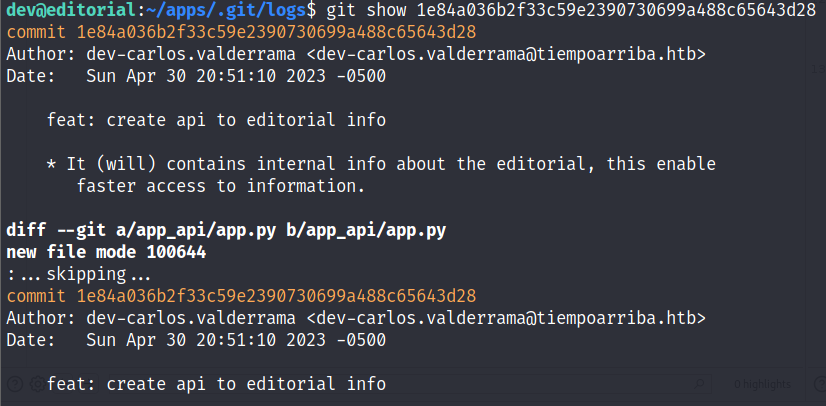
**cat user.txt**

You will the user flag.

**cd apps** ( to access apps directory) > cd ./.git/ > ls > cd logs

**cat HEAD**

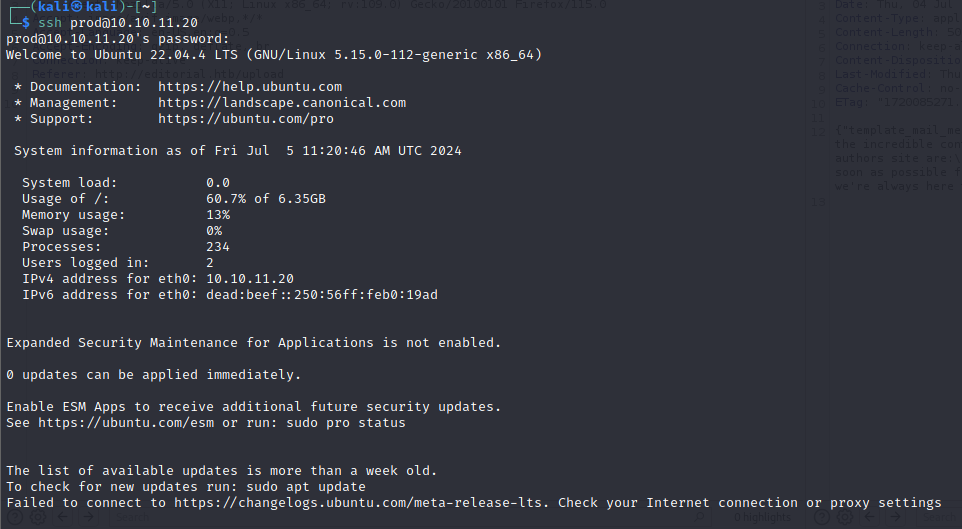
**Copy the API : create api to editorial info**

**git show API (Replace API key with you API)**

At the end you will get the root user ID and password. With **username** as **prod** and password

**Step 12:** Open the root profile with following command.

**ssh** [**prod@10.10.11.20**](mailto:prod@10.10.11.20)



Once logged in inside root user.

Run **ls**

**Root.txt**



You will get the **ROOT FLAG**