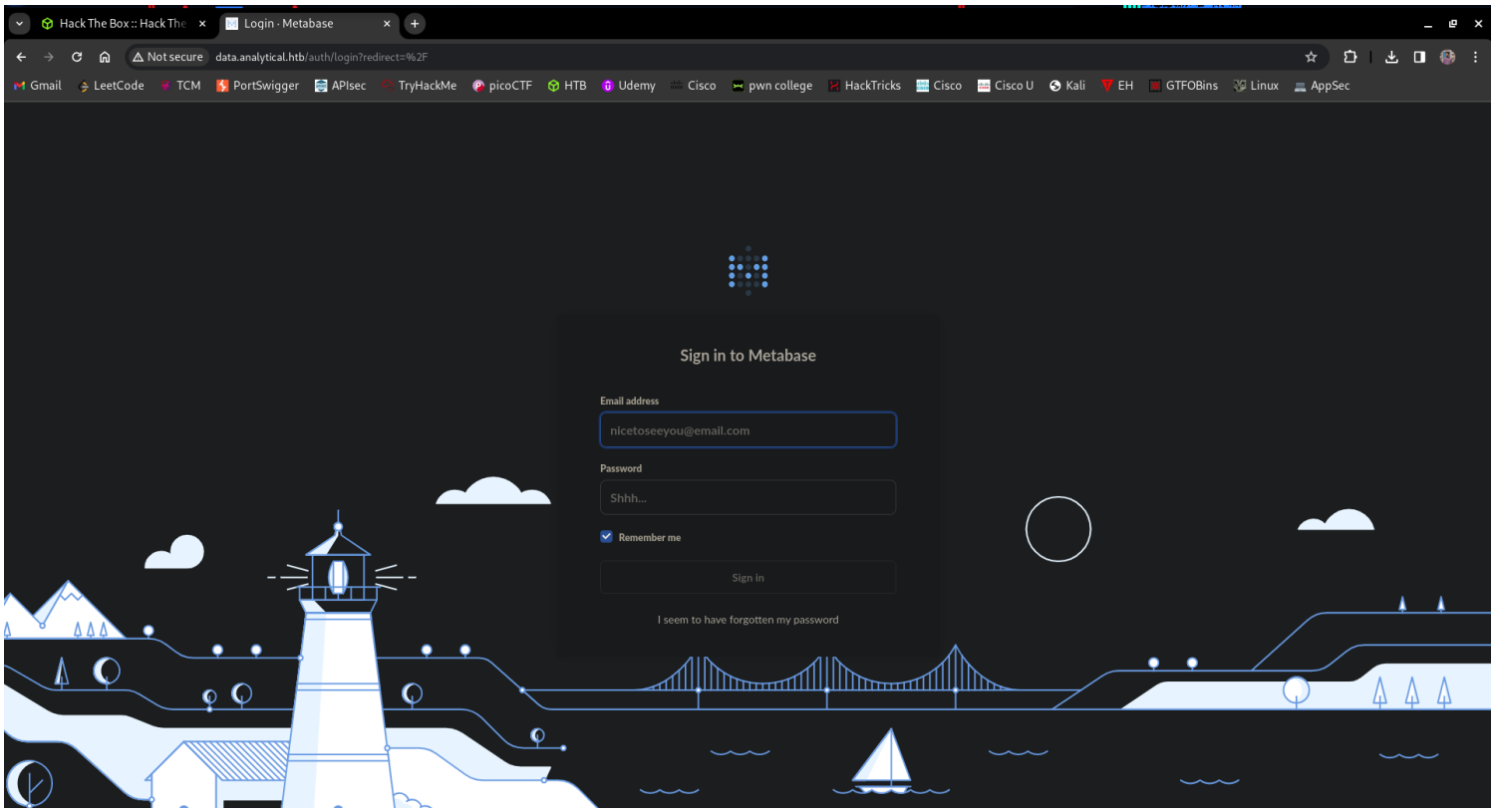
Analytics

Scanning and Enumeration

```
┌──(moghees㉿kali)-[~/Desktop/CTF/HTB/analytics]
└─$ cat nmap.scan
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-11 02:10 PKT
Nmap scan report for analytical.htb (10.10.11.233)
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Analytical
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 52.45 seconds
```

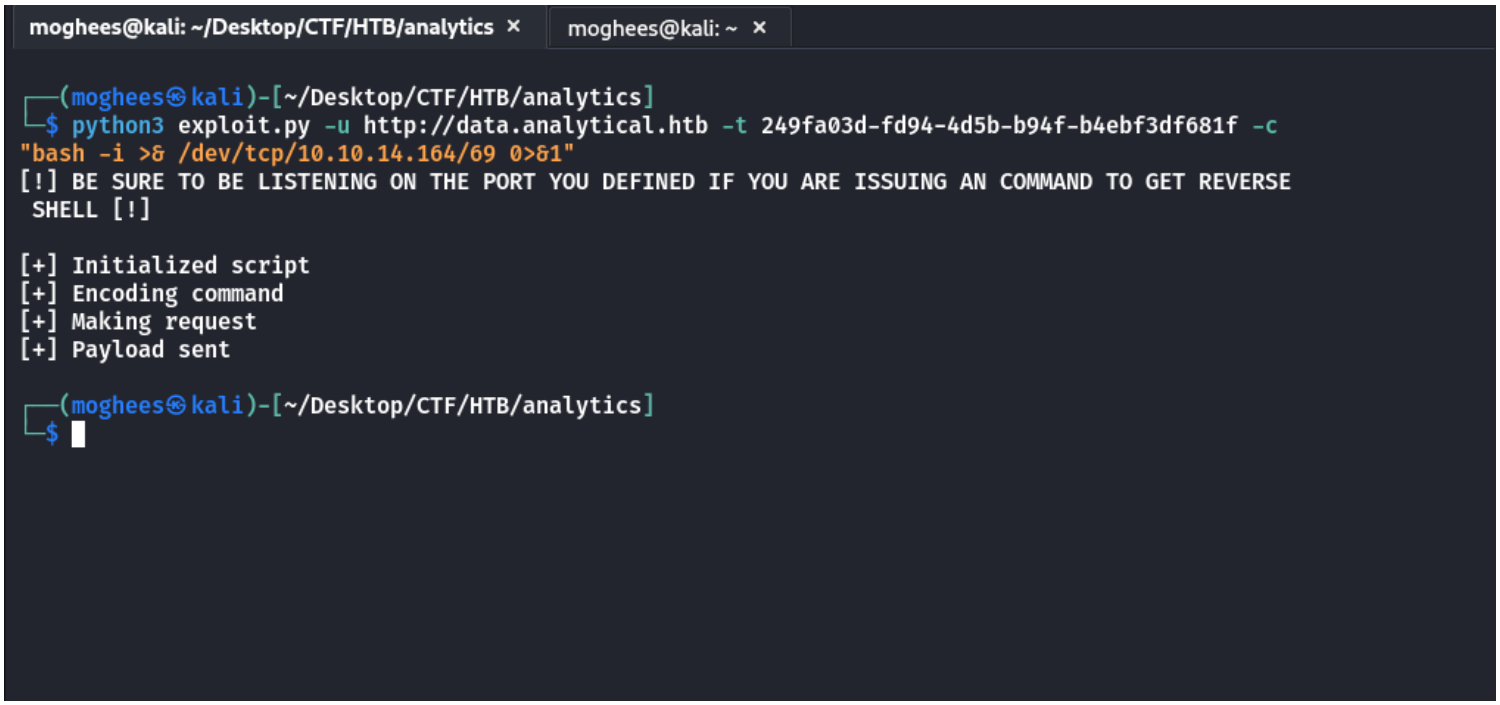


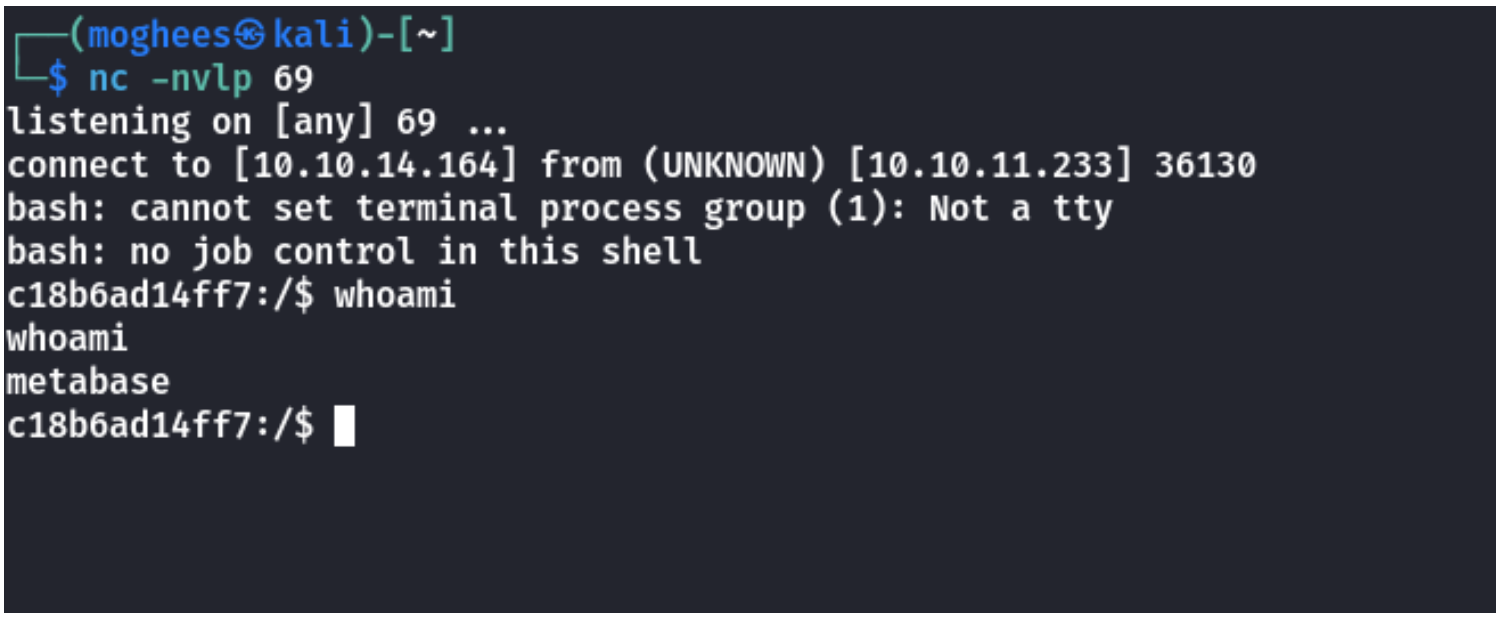
This website is using "**Metabase**". So, look for exploits.

Exploitation

https://github.com/m3m0o/metabase-pre-auth-rce-poc/tree/main

The script needs the **target URL**, the **setup token** and a **command** that will be executed. The setup token can be obtained through the `/api/session/properties` endpoint. Copy the value of the `setup-token` key.



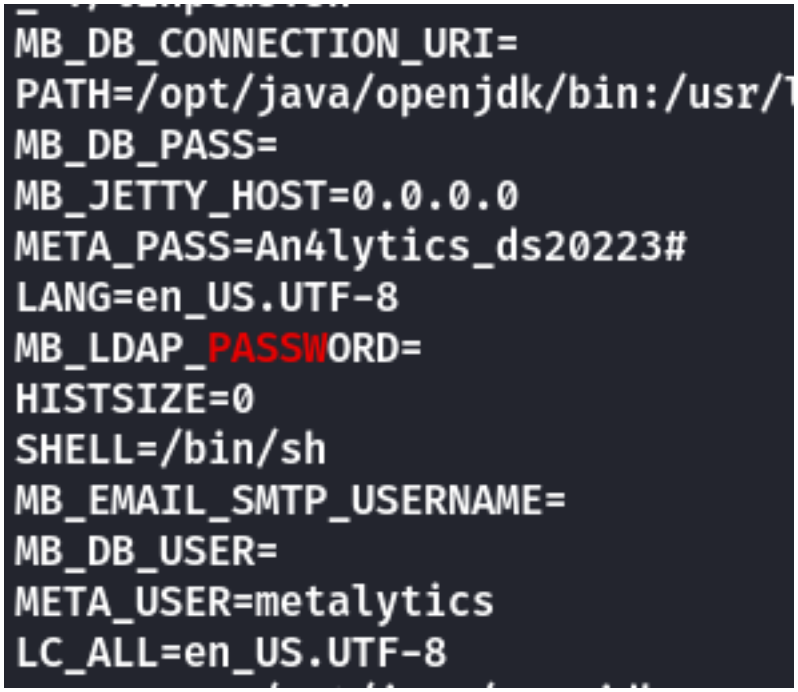


Gained Foothold.

user flag

THERE WAS NO USER FLAG IN **/home/metabase**

- Ran **linpeas.sh**



found username and password.

Username : metalytics
Password : An4lytics_ds20223#

```
┌──(moghees㉿kali)-[~]
└─$ ssh metalytics@10.10.11.233
The authenticity of host '10.10.11.233 (10.10.11.233)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.233' (ED25519) to the list of known hosts.
metalytics@10.10.11.233's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-25-generic x86_64)

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

  System information as of Fri Nov 10 10:03:54 PM UTC 2023

  System load:              0.03271484375
  Usage of /:               97.0% of 7.78GB
  Memory usage:             32%
  Swap usage:               0%
  Processes:                478
  Users logged in:          1
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.10.11.233
  IPv6 address for eth0:    dead:beef::250:56ff:feb9:766c

  ⇒ / is using 97.0% of 7.78GB
  ⇒ There are 294 zombie processes.


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

Got foothold.

```
metalytics@analytics:~$ cat user.txt
a285e5468b4078e036721065365b601a
metalytics@analytics:~$
```

priv esc

Dont know how. There were exploits in machine and I used one sadly.