SNA Lab 2

1.1

Docker version: 18.09.7, build 2d0083

1.2

I used three images in the assignment (database is required for a WEB Documentation service) :

1)postgres:9.6-alpine - database

2)hackmdio/hackmd:1.2.0 - WEB Documentation service.

3)rastasheep/ubuntu-sshd - Open SSH

Their dockerfiles are:

1)
https://github.com/docker-library/postgres/blob/c552b2bcd8dd5ef822463343b461fe0e31445b9d/9.6/alpine/Dockerfile

2)
https://hub.docker.com/r/hackmdio/hackmd/dockerfile

3)
https://hub.docker.com/r/rastasheep/ubuntu-sshd/dockerfile

A way to build everything up (docker-compose is there too):

Link to github: https://github.com/BananaAndBread/SNA/tree/master/Lab2

Python script to set up services (assumed docker is already installed on a host) - run_script.py

Example: `python3 script.py path/database/folder/to/mount path/config/folder/to/mount`

Python script to disable authentication by password and send keys to ssh server- ssh_script.py

Example:

```
mkdir admin
ssh-keygen -t rsa -b 4096 -C "your_email@example.com" -f ./admin/key_example
python3 ssh_script.py
```

Example of a docker-compose created by run_script.py - docker-compose.example.yml

1.3 Outputs of inspection (pic. 1):

```
banana_and_bread@yourMummy:~/SNA/Lab2$ docker network inspect lab2_internet
[
    {
        "Name": "lab2_internet",
        "Id": "67c2e9b1c6b302d30a490d8179e22fdd474769c500ecbed4448e92ab8dc58d09",
        "Created": "2019-09-02T20:28:22.300193196+03:00",
        "Scope": "local",
        "Driver": "bridge",
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": null,
            "Config": [
                {
                    "Subnet": "172.24.1.0/27"
                }
            ]
        },
        "Internal": false,
        "Attachable": false,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {
            "10d00412664a906b0d9899a148cbeaf71ee8924dff54e71e5c3d37638dd6ab22": {
                "Name": "lab2_ssh_1",
                "EndpointID": "38b932fab35272e4a7e4dd099e9e15834e2e9c5ece0034a35e9f8a9
8a6915c4",
                "MacAddress": "02:42:ac:18:01:02",
                "IPv4Address": "172.24.1.2/27",
                "IPv6Address": ""
            }
        },
        "Options": {},
        "Labels": {}
    }
]
```

1.3 Outputs of inspection (pic. 2):

```
banana_and_bread@yourMummy:~/SNA/Lab2$ docker network inspect lab2_no-internet
[
    {
        "Name": "lab2_no-internet",
        "Id": "391e4d07d2578e1dac49055fbd32b6734e8c252ab9cea7db3ba2bdd61effe94a",
        "Created": "2019-09-02T20:28:22.249108128+03:00",
        "Scope": "local",
        "Driver": "bridge",
        "EnableIPv6": false,
        "IPAM": {
            "Driver": "default",
            "Options": null,
            "Config": [
                {
                    "Subnet": "172.24.0.0/27"
                }
            ]
        },
        "Internal": true,
        "Attachable": false,
        "Ingress": false,
        "ConfigFrom": {
            "Network": ""
        },
        "ConfigOnly": false,
        "Containers": {
            "10d00412664a906b0d9899a148cbeaf71ee8924dff54e71e5c3d37638dd6ab22": {
                "Name": "lab2_ssh_1",
                "EndpointID": "d004609a270e404b5ff2f8aa51d6f3389b0c033714a5e0e38c8b0e95
29135332",
                "MacAddress": "02:42:ac:18:00:03",
                "IPv4Address": "172.24.0.3/27",
                "IPv6Address": ""
            },
            "951169632d2d9c494ea3ec03b3add4300e6a8a71c8d1012c278abc7029b78ba0": {
                "Name": "lab2_database_1",
                "EndpointID": "e9d164607583a9bff94c33787b08ff8dec3940f1573827b50304c380
890e2c0e",
                "MacAddress": "02:42:ac:18:00:02",
                "IPv4Address": "172.24.0.2/27",
                "IPv6Address": ""
            },
            "d8e73cbb982368bbd7efcbe97477b8b6ca04cde1db026b721b1e2b045be261d2": {
                "Name": "lab2_app_1",
                "EndpointID": "5ea175b7a73cf2978ae1ec333b929b4d0e889aa9a4270909f6170999
ed4bd83c",
                "MacAddress": "02:42:ac:18:00:04",
                "IPv4Address": "172.24.0.4/27",
                "IPv6Address": ""
            }
        },
        "Options": {},
        "Labels": {}
    }
]
```

1.3 Routing table:

```
root@10d00412664a:/# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.24.1.1      0.0.0.0         UG    0      0        0 eth0
172.24.0.0      0.0.0.0         255.255.255.224 U     0      0        0 eth1
172.24.1.0      0.0.0.0         255.255.255.224 U     0      0        0 eth0
root@10d00412664a:/#
```

2.1 Running containers:

```
banana_and_bread@yourMummy:~/SNA/Lab2$ docker ps
CONTAINER ID        IMAGE                    COMMAND                  CREATED
   STATUS              PORTS                    NAMES
219a24161117        hackmdio/hackmd:1.2.0    "/usr/local/bin/dock…"   9 minutes ago
   Up 9 minutes                                 lab2_app_1
9f43fd0b1137        postgres:9.6-alpine      "docker-entrypoint.s…"   9 minutes ago
   Up 9 minutes                                 lab2_database_1
b9203f07ad5f        rastasheep/ubuntu-sshd   "/usr/sbin/sshd -D"      9 minutes ago
   Up 9 minutes        0.0.0.0:1234->22/tcp     lab2_ssh_1
```

2.2 Folders on the host (Containers' folders are mounted to them):

```
banana_and_bread@yourMummy:~/SNA/Lab2/config$ ls
moduli       ssh_host_ecdsa_key      ssh_host_ed25519_key.pub  ssh_import_id
ssh_config   ssh_host_ecdsa_key.pub  ssh_host_rsa_key
sshd_config  ssh_host_ed25519_key    ssh_host_rsa_key.pub
```

```
root@yourMummy:/home/banana_and_bread/SNA/Lab2/database# ls
base          pg_hba.conf    pg_replslot   pg_subtrans  postgresql.auto.conf
global        pg_ident.conf  pg_serial     pg_tblspc    postgresql.conf
pg_clog       pg_logical     pg_snapshots  pg_twophase  postmaster.opts
pg_commit_ts  pg_multixact   pg_stat       PG_VERSION   postmaster.pid
pg_dynshmem   pg_notify      pg_stat_tmp   pg_xlog
```

2.2 Container with app does not have any access to the internet, however has access to ssh container:

```
banana_and_bread@yourMummy:~/SNA/Lab2$ docker exec -it lab2_app_1 ping google.com
^Cbanana_and_bread@yourMummy:~/SNA/Lab2$ docker exec -it lab2_app_1 bash
root@219a24161117:/hackmd# ping google.com
^C
root@219a24161117:/hackmd# ping ssh
PING ssh (172.24.0.3) 56(84) bytes of data.
64 bytes from lab2_ssh_1.lab2_no-internet (172.24.0.3): icmp_seq=1 ttl=64 time=0.185 ms
64 bytes from lab2_ssh_1.lab2_no-internet (172.24.0.3): icmp_seq=2 ttl=64 time=0.152 ms
64 bytes from lab2_ssh_1.lab2_no-internet (172.24.0.3): icmp_seq=3 ttl=64 time=0.086 ms
64 bytes from lab2_ssh_1.lab2_no-internet (172.24.0.3): icmp_seq=4 ttl=64 time=0.081 ms
^C
--- ssh ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.081/0.126/0.185/0.044 ms
root@219a24161117:/hackmd#
```

2.2 SSH container has internet access :

```
banana_and_bread@yourMummy:~/SNA/Lab2$ docker exec -it lab2_ssh_1 bash
root@b9203f07ad5f:/# ping google.com
bash: ping: command not found
root@b9203f07ad5f:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic InRelease [242 kB]
Get:3 http://security.ubuntu.com/ubuntu bionic-security/universe Sources [200 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:5 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [4173
 B]
```

3. Local tunnel:

3. 1. Using command:

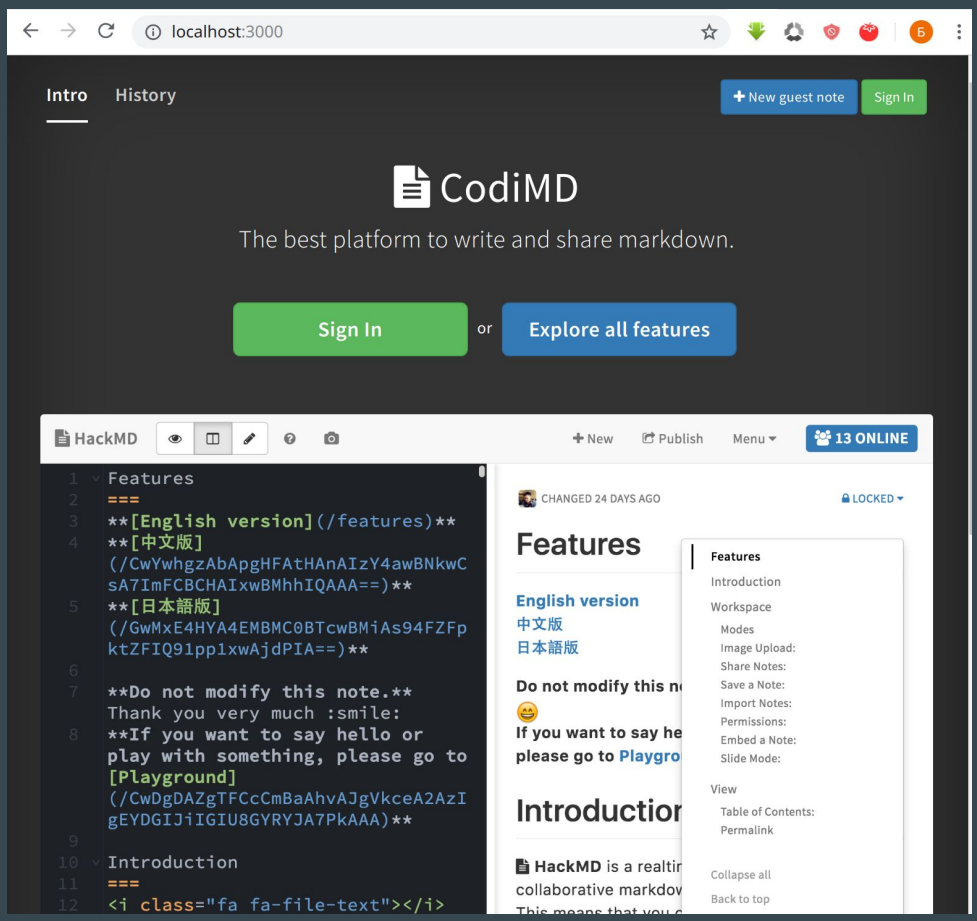
```
ssh -L 3000:app:3000 root@ssh_ip -i path/to/key
```

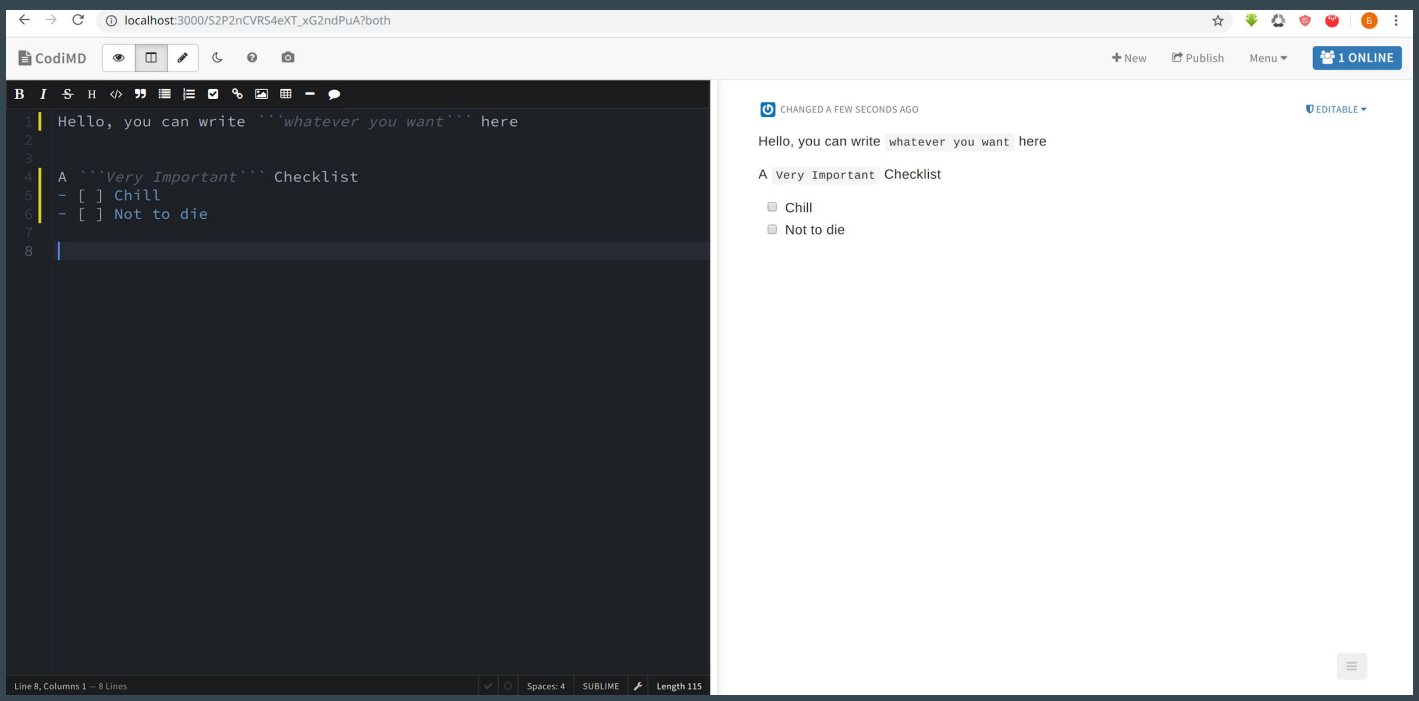
```
banana_and_bread@yourMummy:~/SNA/Lab1$ ssh -L 3000:app:3000 root@172.24.1.2 -p 22 -i admin/key
The authenticity of host '172.24.1.2 (172.24.1.2)' can't be established.
ECDSA key fingerprint is SHA256:YtTfuoRRR5qStSVA5UuznGamA/dvf+djbIT6Y48IYD0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.24.1.2' (ECDSA) to the list of known hosts.
Last login: Mon Sep  2 19:16:33 2019 from 172.24.1.1
root@dfb283b5e04b:~#
```

Netstat:

```
root@dfb283b5e04b:~# netstat -tplna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Pro
gram name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1/sshd

tcp        0      0 127.0.0.11:44113        0.0.0.0:*               LISTEN      -

tcp        0      0 172.24.1.2:22           172.24.1.1:35256        ESTABLISHED 6/sshd:
 root@pts/0
tcp        0      0 172.24.1.2:22           172.24.1.1:38244        ESTABLISHED 124/ssh
d: root@pts/
tcp        0      0 172.24.0.3:34858        172.24.0.4:3000         TIME_WAIT   -

tcp6       0      0 :::22                   :::*                    LISTEN      1/sshd

root@dfb283b5e04b:~#
```

3.2 Even more screenshots for the ~~god of screenshots~~ the report.





4.1 Map the entire network

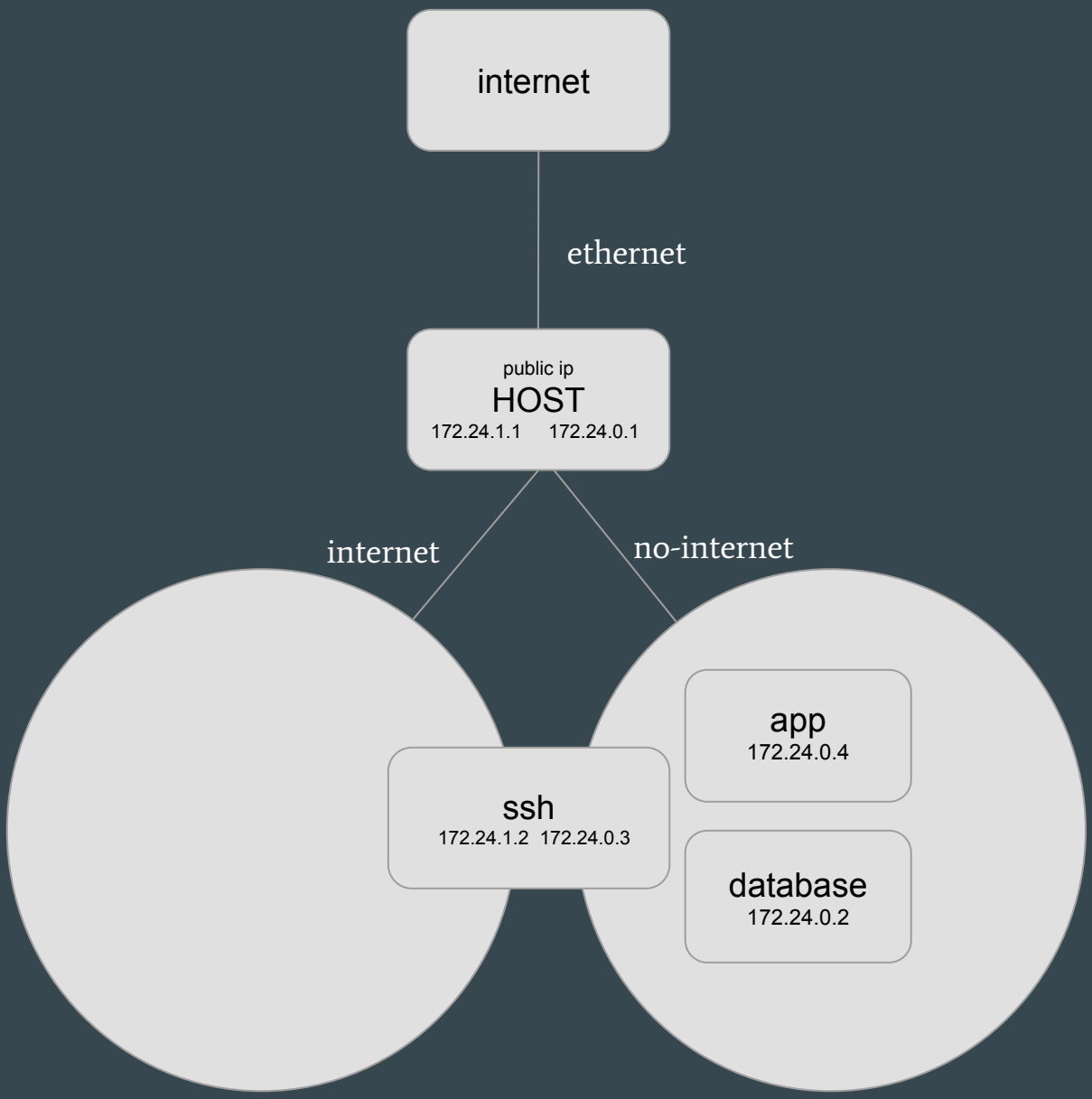
Network with internet:

```
Nmap done: 32 IP addresses (2 hosts up) scanned in 4.54 seconds
root@dfb283b5e04b:~# nmap 172.24.1.0/27

Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-02 20:29 UTC
Nmap scan report for 172.24.1.1
Host is up (0.000087s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
1234/tcp open  hotline
MAC Address: 02:42:EF:95:11:8A (Unknown)

Nmap scan report for dfb283b5e04b (172.24.1.2)
Host is up (0.000036s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 32 IP addresses (2 hosts up) scanned in 4.28 seconds
```

Network without internet:

```
root@dfb283b5e04b:~# nmap 172.24.0.3/27

Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-02 20:21 UTC
Nmap scan report for 172.24.0.1
Host is up (0.00018s latency).
Not shown: 999 closed ports
PORT     STATE    SERVICE
1234/tcp filtered hotline
MAC Address: 02:42:F6:2E:D3:E7 (Unknown)

Nmap scan report for lab2_database_1.lab2_no-internet (172.24.0.2)
Host is up (0.00022s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
5432/tcp open  postgresql
MAC Address: 02:42:AC:18:00:02 (Unknown)

Nmap scan report for lab2_app_1.lab2_no-internet (172.24.0.4)
Host is up (0.00018s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3000/tcp open  ppp
MAC Address: 02:42:AC:18:00:04 (Unknown)

Nmap scan report for dfb283b5e04b (172.24.0.3)
Host is up (0.000025s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 32 IP addresses (4 hosts up) scanned in 114.28 seconds
```

4.1 Diagram


internet
ethernet
public ip
HOST
172.24.1.1 172.24.0.1
internet
no-internet
app
172.24.0.4
ssh
172.24.1.2 172.24.0.3
database
172.24.0.2