

Docker for Dummies

This year we will be using a lot of docker machines. They are like virtual machines, however slimed down, therefore using less resources and have smaller file sizes. We recommend running docker on your Kali Linux machine (or Debian based distribution), even though it can run on Windows, it can be temperamental at times. Therefore, this is a guide for Linux only.

Ensure Kali is Updated

```
sudo apt update && sudo apt upgrade
```

Install Docker

```
sudo apt install docker.io docker-compose
```

Grab Docker Image

Next you will need a docker image, we will give you a link to this on the day, as you will need different ones for different challenges, so just replace the link for the appropriate challenge. The below command just downloads a file:

```
wget https://raw.githubusercontent.com/Cov-ComSec/ComSecMaterials/main/Week1-Nmap/docker-compose.yaml
```

NB: Do not change the file name otherwise docker will not work, hence each docker file is best placed in its own folder! **Ensure that the docker file is called docker-compose.yaml**

```
kali@kali:~/Documents$ wget https://raw.githubusercontent.com/Cov-ComSec/ComSecMaterials/main/Week1-Nmap/docker-compose.yaml
--2020-10-19 16:59:00-- https://raw.githubusercontent.com/Cov-ComSec/ComSecMaterials/main/Week1-Nmap/docker-compose.yaml
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.120.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.120.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 802 [text/plain]
Saving to: 'docker-compose.yaml'

docker-compose.yaml                                100%[=====]
2020-10-19 16:59:00 (14.7 MB/s) - 'docker-compose.yaml' saved [802/802]
```

Start the Docker Machine

Navigate to the folder in which you have placed your docker file & type:

```
sudo docker-compose up
```

This may take a minute or two

```
kali@kali:~/Documents$ sudo docker-compose up
WARNING: The Docker Engine you're using is running in swarm mode.

Compose does not use swarm mode to deploy services to multiple nodes in a swarm. All containers will be scheduled on the current node.
To deploy your application across the swarm, use 'docker stack deploy'.

Creating network "documents_external" with the default driver
Creating volume "documents_data-volume" with default driver
Creating documents_ftp_1 ... done
Creating documents_web_1 ... done
Creating documents_ssh_1 ... done
Creating documents_smtp_1 ... done
Attaching to documents_ssh_1, documents_smtp_1, documents_web_1, documents_ftp_1
ftp_1 Starting Pure-FTPd:
ftp_1 pure-ftpd -c 30 -C 10 -l puredb:/etc/pure-ftpd/pureftpd.pdb -j -R -P localhost -p 30000:30059
web_1 AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 192.168.42.4. Set the 'ServerName' directive globally to suppress this message
web_1 AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 192.168.42.4. Set the 'ServerName' directive globally to suppress this message
web_1 [Mon Oct 19 21:05:04.835083 2020] [mpm_prefork:notice] [pid 1] AH00163: Apache/2.4.25 (Debian) PHP/7.2.3-4 configured -- resuming normal operations
web_1 [Mon Oct 19 21:05:04.837042 2020] [core:notice] [pid 1] AH00094: Command line: 'apache2 -D FOREGROUND'
```

NB: do not close this terminal window (otherwise docker will stop) – just open a new terminal window.

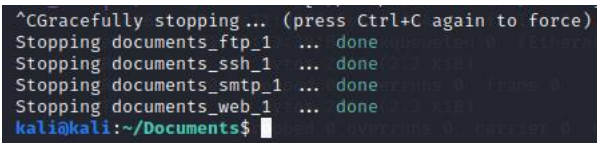
NB: you will get text like in the image above – this is normal, and just the log output, not an error!

The Right IP

Normally docker should assign its self to localhost (127.0.0.1), however this isn't always the case – just have a look at the output from the docker-start command, and it should show you (see the red box in the image below). To be able to attack all services on the back to complicate matters, you will have to change this IP – change the end number to a 1. E.g. 192.168.42.4 -> 192.168.42.1.

Shutting Down Docker

When you have finished & found all the flags (congratulations) go back to the terminal window running docker – press CTRL + C simultaneously. Sometimes this takes a minute or two – wait until you see the blue text below asking you to type your new command.



```
^CGracefully stopping... (press Ctrl+C again to force)
Stopping documents_ftp_1 ... done
Stopping documents_ssh_1 ... done
Stopping documents_smtp_1 ... done
Stopping documents_web_1 ... done
kali@kali:~/Documents$
```

Now you are free to continue onto the next challenge or docker.

Troubleshooting/Common Errors

- **Error** - E: Package 'python3-pip' has no installation candidate
- **Answer** - apt install pip
- **Error** - ERROR: Pool overlaps with other one on this address space
- **Answer** - sudo docker network prune

General advice:

1. Try running the command with sudo – you have the power!
2. Ensure that the docker file is called docker-compose.yaml
3. Restart docker machines - sudo docker-compose restart (must be run in the same folder as the docker-compose file)
4. Run sudo docker-compose kill (must be run in the same folder as the docker-compose file)
5. Try resetting IP addresses - sudo docker network prune
6. Restart VM – surprising what a reboot can do!
7. Google the error or look at the man pages (man docker-compose)!
8. Try singing 'I have got the power' twice in a row & cross your fingers.

After trying all the above & you're still stuck, let us know 😊