Lab - Installing the WebMap-Nmap Dashboard

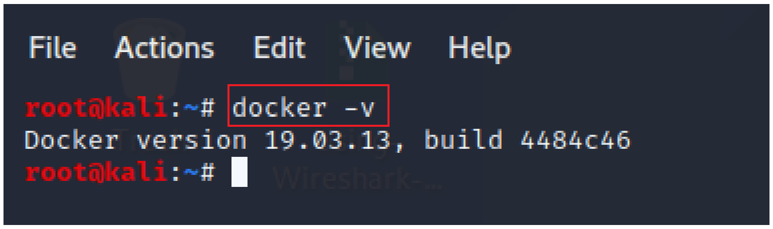
Overview

WebMap is a web dashboard for Nmap scans. For this lab, we will be installing and then using WebMap to generate an XML report of our Nmap scan results, which can be saved as a PDF report.

For this lab, you will need the Docker program installed with your virtual install of Kali Linux.

Check to see if Docker is installed

To see if Docker is installed and to see what version is being used, open a terminal and at the prompt type, **`docker -v`** and press enter.

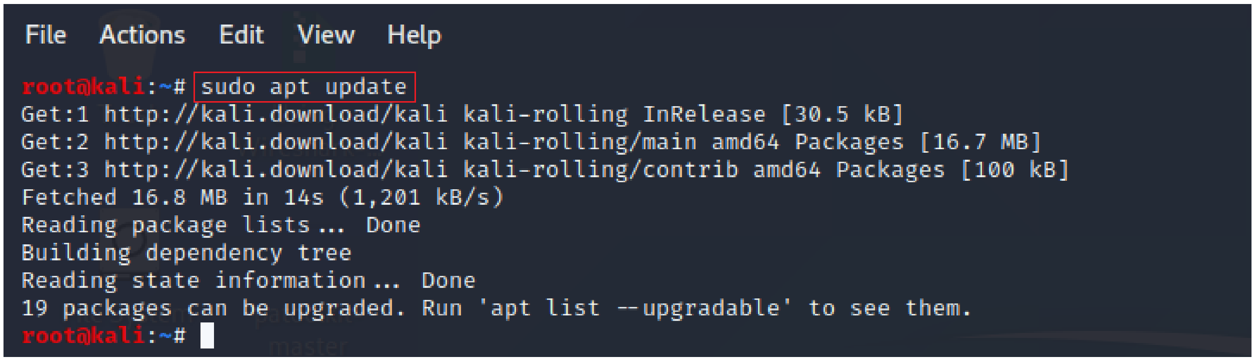


```
root@kali:~# docker -v
Docker version 19.03.13, build 4484c46
root@kali:~# 
```

If docker is present, move on to the section of the lab entitled **Installing WebMap.**

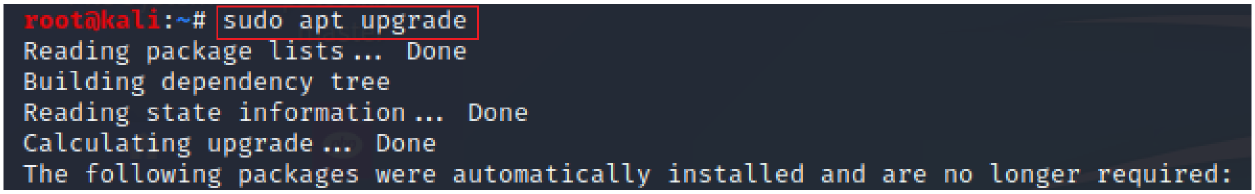
Installing Docker.

As always, check for updates. **`sudo apt update`**



```
root@kali:~# sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [16.7 MB]
Get:3 http://kali.download/kali kali-rolling/contrib amd64 Packages [100 kB]
Fetched 16.8 MB in 14s (1,201 kB/s)
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
19 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@kali:~# 
```

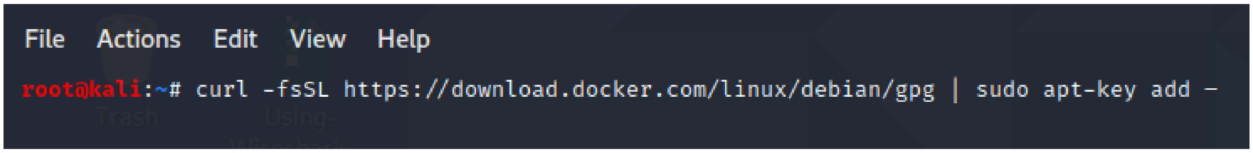
Need to upgrade? **`sudo apt upgrade`**



```
root@kali:~# sudo apt upgrade
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
```

Add the official Docker PGP key:

```
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo
apt-key add -
```

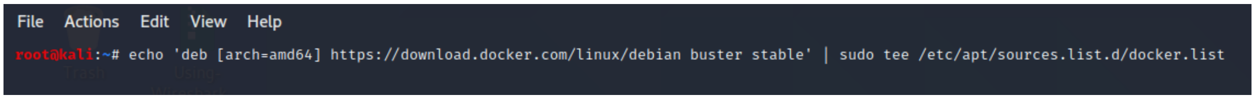


```
root@kali:~# curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -
```

Configure the correct Advanced Package Tool (APT), so we will be able to download, install, and update Docker.

```
echo 'deb [arch=amd64] https://download.docker.com/linux/debian
buster stable' | sudo tee /etc/apt/sources.list.d/docker.list
```

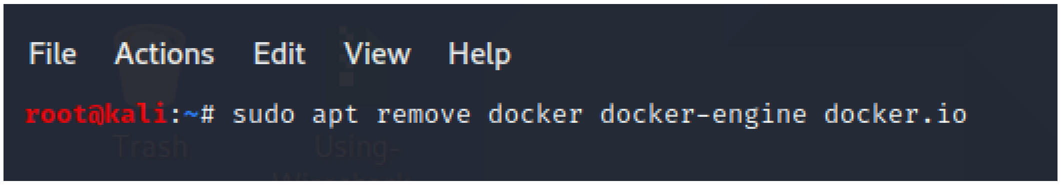
(The **Advanced Package Tool** (APT) is how programs, libraries, documentation, and even the kernel itself are installed and managed on Kali and other Debian-based derivatives.)



```
root@kali:~# echo 'deb [arch=amd64] https://download.docker.com/linux/debian buster stable' | sudo tee /etc/apt/sources.list.d/docker.list
```

In case you have any older or outdated version of Docker installed on your system, we make sure to get rid of it first:

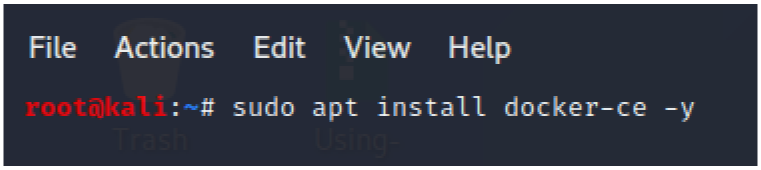
```
sudo apt remove docker docker-engine docker.io
```



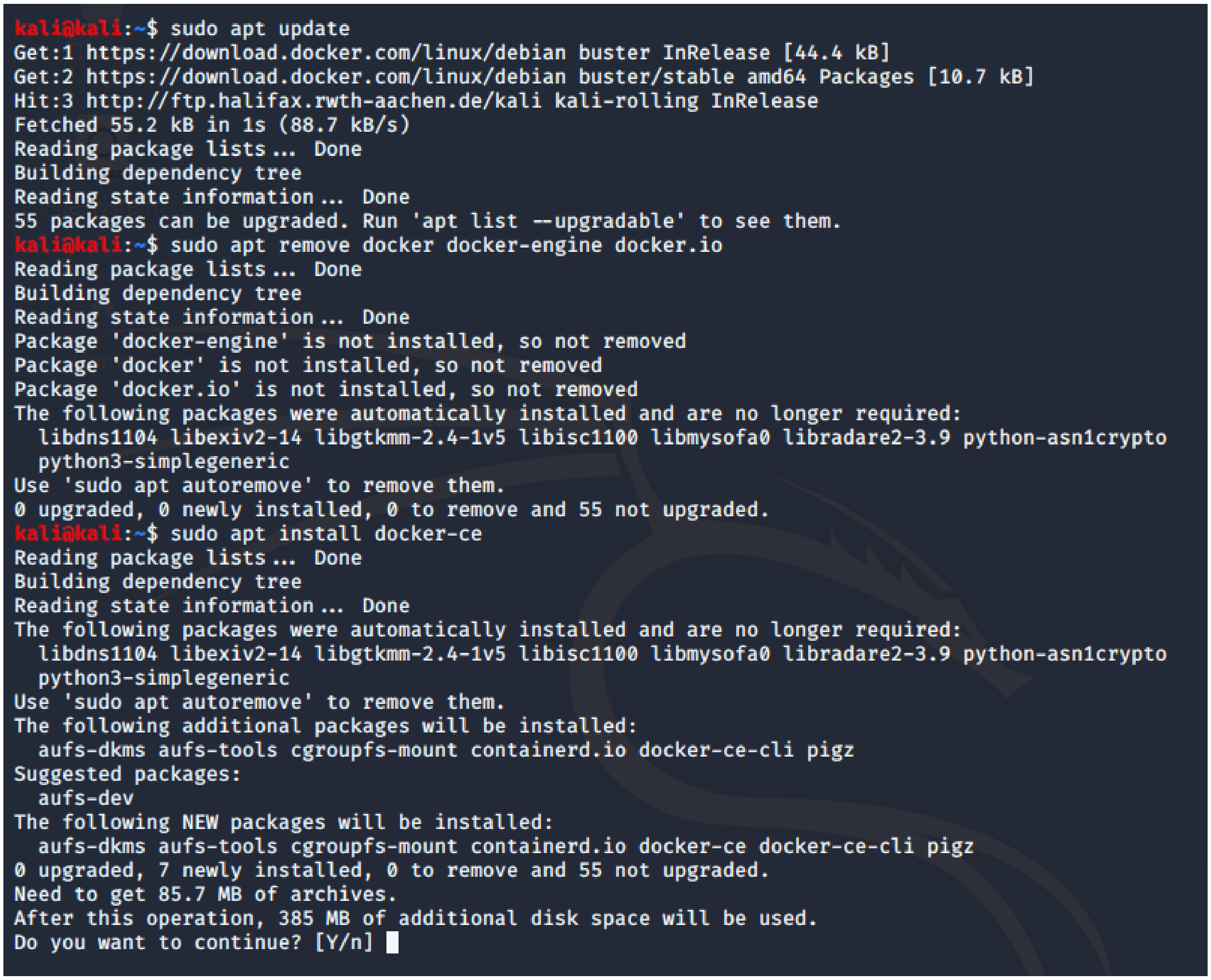
```
root@kali:~# sudo apt remove docker docker-engine docker.io
```

Install Docker

```
sudo apt install docker-ce -y
```



```
root@kali:~# sudo apt install docker-ce -y
```

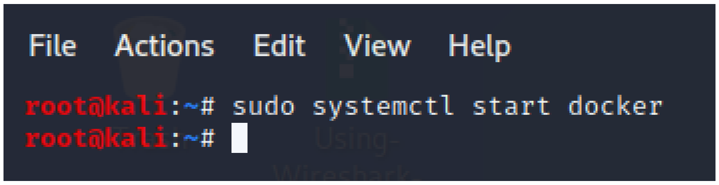


```
kali@kali:~$ sudo apt update
Get:1 https://download.docker.com/linux/debian buster InRelease [44.4 kB]
Get:2 https://download.docker.com/linux/debian buster/stable amd64 Packages [10.7 kB]
Hit:3 http://ftp.halifax.rwth-aachen.de/kali kali-rolling InRelease
Fetched 55.2 kB in 1s (88.7 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
55 packages can be upgraded. Run 'apt list --upgradable' to see them.
kali@kali:~$ sudo apt remove docker docker-engine docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'docker-engine' is not installed, so not removed
Package 'docker' is not installed, so not removed
Package 'docker.io' is not installed, so not removed
The following packages were automatically installed and are no longer required:
  libdns1104 libexiv2-14 libgtkmm-2.4-1v5 libisc1100 libmysofa0 libradare2-3.9 python-asn1crypto
  python3-simplegeneric
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 55 not upgraded.
kali@kali:~$ sudo apt install docker-ce
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdns1104 libexiv2-14 libgtkmm-2.4-1v5 libisc1100 libmysofa0 libradare2-3.9 python-asn1crypto
  python3-simplegeneric
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  aufs-dkms aufs-tools cgroupfs-mount containerd.io docker-ce-cli pigz
Suggested packages:
  aufs-dev
The following NEW packages will be installed:
  aufs-dkms aufs-tools cgroupfs-mount containerd.io docker-ce docker-ce-cli pigz
0 upgraded, 7 newly installed, 0 to remove and 55 not upgraded.
Need to get 85.7 MB of archives.
After this operation, 385 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Start Docker Service

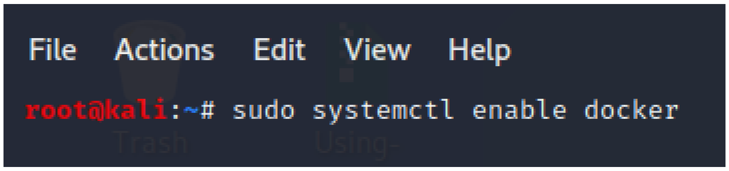
This command starts Docker as you need it.

`sudo systemctl start docker`



```
root@kali:~# sudo systemctl start docker
root@kali:~#
```

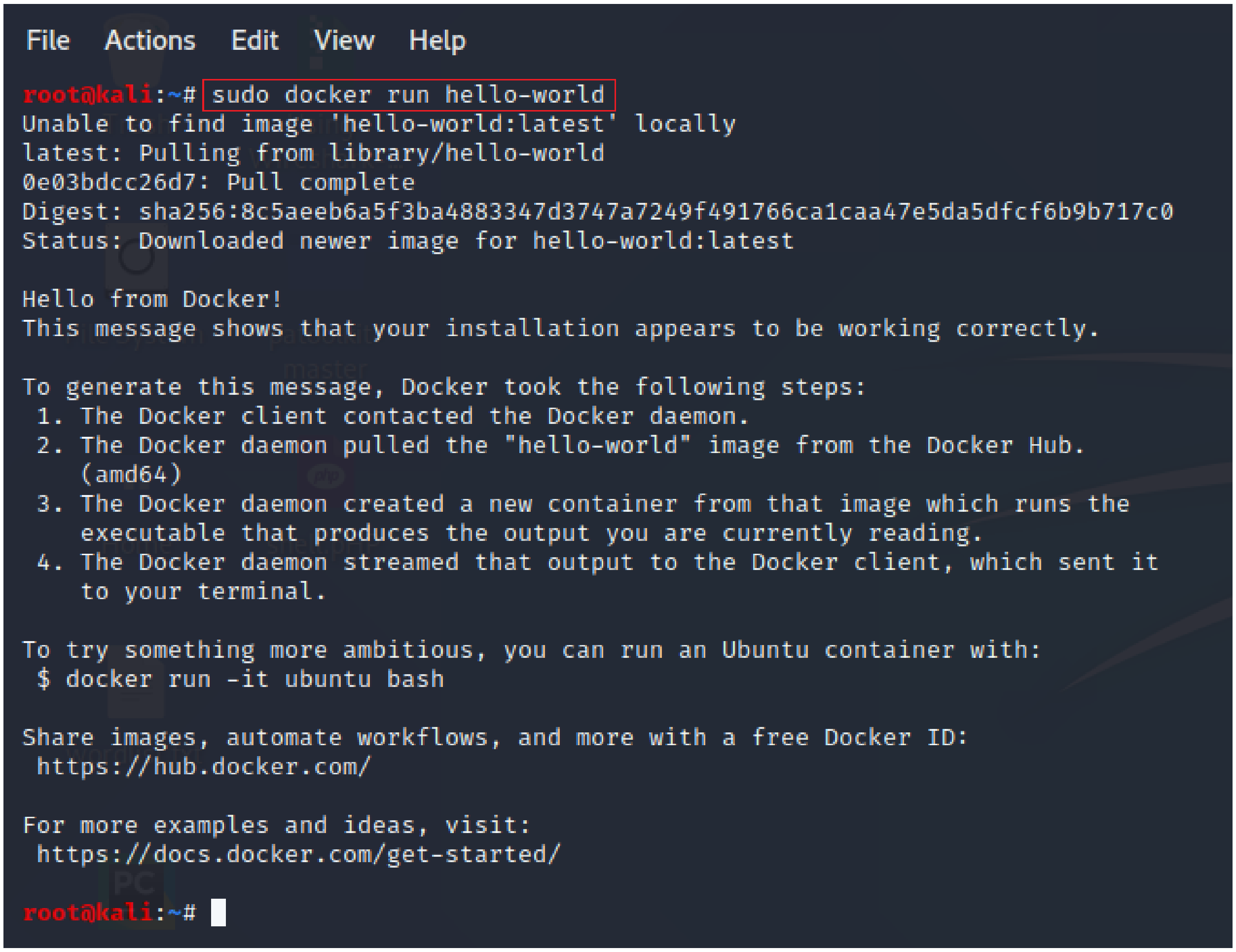
To have Docker start at startup, use, **`sudo systemctl enable docker`**



```
root@kali:~# sudo systemctl enable docker
```

You can check to see if Docker works using the following command.

sudo docker run hello-world



```
root@kali:~# sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
0e03bdcc26d7: Pull complete
Digest: sha256:8c5aeeb6a5f3ba4883347d3747a7249f491766ca1caa47e5da5dfcf6b9b717c0
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/

root@kali:~# 
```

Install WebMap

We first need to make a directory where your Nmap scan can be saved and pulled from. This is the directory WebMap will look in for your Nmap scan results when WebMap starts.

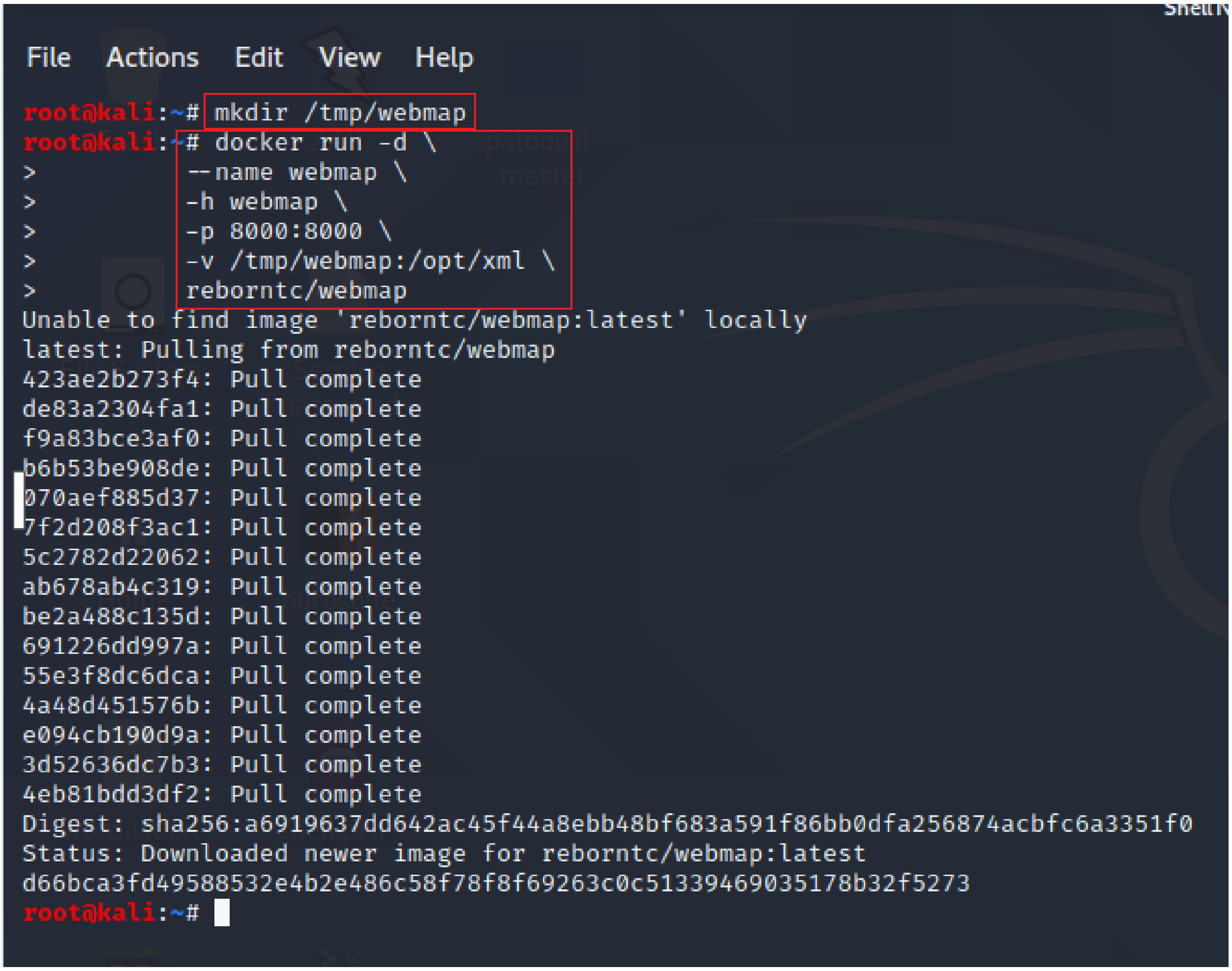
At the prompt, type the following command: **mkdir /tmp/webmap**

We are now ready to install the WebMap docker image using the following commands. These commands can be entered at the prompt all at once or one at a time.

```
docker run -d \
         --name webmap \
         -h webmap \
         -p 8000:8000 \
         -v /tmp/webmap:/opt/xml \
         reborntc/webmap
```

Once you have the last command inserted at the prompt, you can press enter to begin downloading the Docker image for WebMap. You can ignore the error,

`Unable to find image 'reborntc/webmap:latest' locally.`



```
root@kali:~# mkdir /tmp/webmap
root@kali:~# docker run -d \
>         --name webmap \
>         -h webmap \
>         -p 8000:8000 \
>         -v /tmp/webmap:/opt/xml \
>         reborntc/webmap
Unable to find image 'reborntc/webmap:latest' locally
latest: Pulling from reborntc/webmap
423ae2b273f4: Pull complete
de83a2304fa1: Pull complete
f9a83bce3af0: Pull complete
b6b53be908de: Pull complete
070aef885d37: Pull complete
7f2d208f3ac1: Pull complete
5c2782d22062: Pull complete
ab678ab4c319: Pull complete
be2a488c135d: Pull complete
691226dd997a: Pull complete
55e3f8dc6dca: Pull complete
4a48d451576b: Pull complete
e094cb190d9a: Pull complete
3d52636dc7b3: Pull complete
4eb81bdd3df2: Pull complete
Digest: sha256:a6919637dd642ac45f44a8ebb48bf683a591f86bb0dfa256874acbfc6a3351f0
Status: Downloaded newer image for reborntc/webmap:latest
d66bca3fd49588532e4b2e486c58f78f8f69263c0c51339469035178b32f5273
root@kali:~# 
```

Restart your Kali installation. After performing any update, upgrade, or installing any additional program such as Docker, it is always a good idea to restart Kali's before proceeding.

Once your Kali is back up, open a terminal and at the prompt type,

`systemctl start docker`

Press enter.

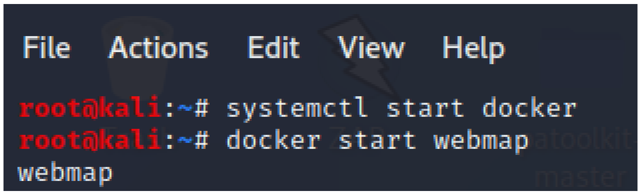
This starts the Docker service.

At the next terminal prompt type,

`docker start webmap`

Press enter.

This starts the WebMap docker image inside the Docker container.



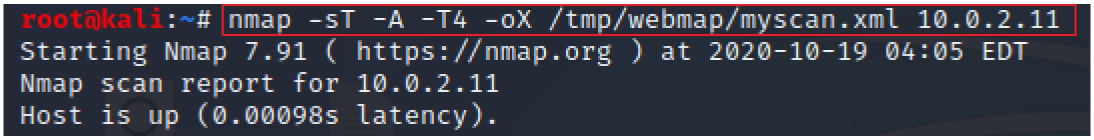
```
root@kali:~# systemctl start docker
root@kali:~# docker start webmap
webmap
```

Start a Nmap scan

For this example, I have started a Nmap scan of my installation of Metesploitable2 using the following command.

`nmap -sT -A -T4 -oX /tmp/webmap/myscan.xml 10.0.2.11`

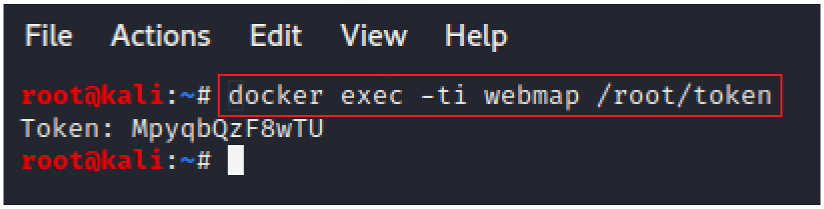
The **`-oX`** switch directs Nmap to output the scan results as an XML file type and to save the results to, **`/tmp/webmap/`** as **`myscan.xml`**



```
root@kali:~# nmap -sT -A -T4 -oX /tmp/webmap/myscan.xml 10.0.2.11
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-19 04:05 EDT
Nmap scan report for 10.0.2.11
Host is up (0.00098s latency).
```

Once our Nmap scan completes are ready to view the results using WebMap, but before we can log in, we will need to generate a logon token using the following command at the Kali terminal.

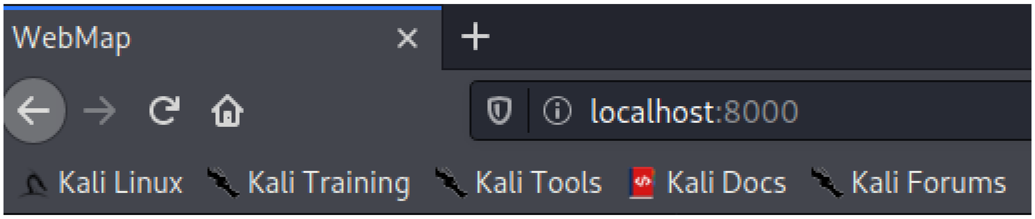
`docker exec -ti webmap /root/token`



```
root@kali:~# docker exec -ti webmap /root/token
Token: MpyqbQzF8wTU
root@kali:~# 
```

Highlight and copy the token.

Open your Kali web browser. In the address bar, type http://localhost:8000



Press enter.

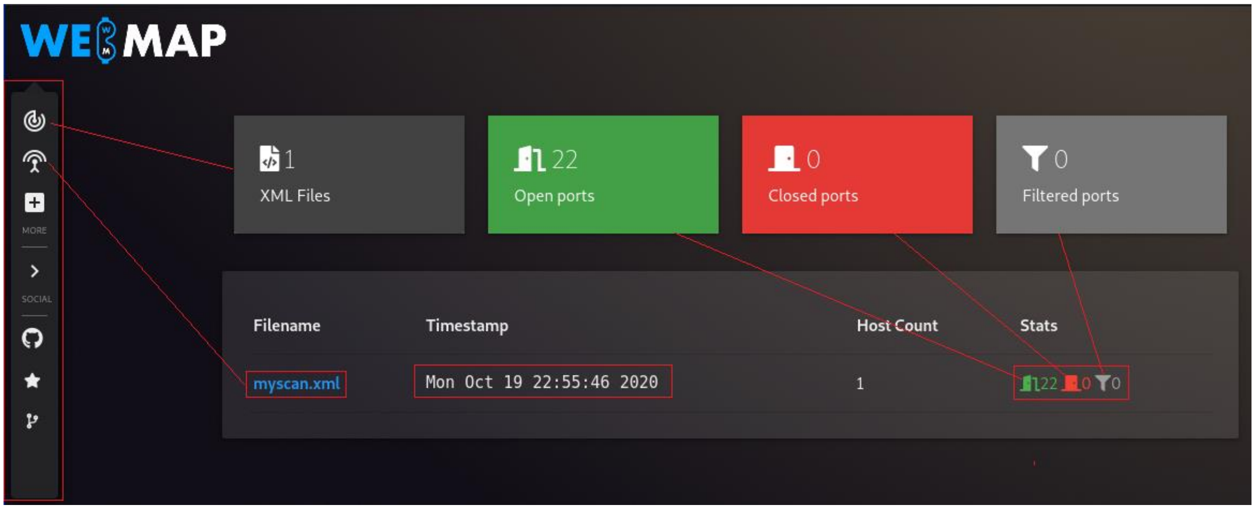
The first time you log in to WebMap, you will be asked for a Token. Copy and paste the token in the token field of the login screen.

When asked if you would like to save the login information, select save.

Navigating WebMap

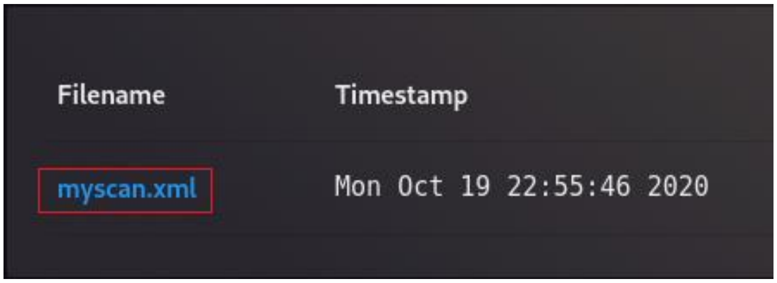
The program is very intuitive, and the main features of the application can be accessed directly from the items on the main page or using the quick launch menu located on the left-hand side of the screen. The first page you are presented with is just a summary of the scan results.

Everything in WebMap is colored coded.



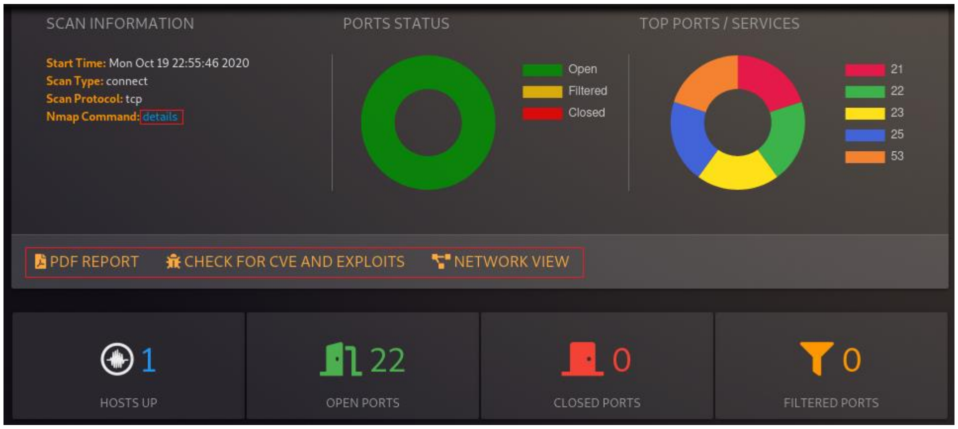
Filename	Timestamp	Host Count	Stats
myscan.xml	Mon Oct 19 22:55:46 2020	1	22 0 0

Find your saved XML file and x2 click it to see the scan results.



Filename	Timestamp
myscan.xml	Mon Oct 19 22:55:46 2020

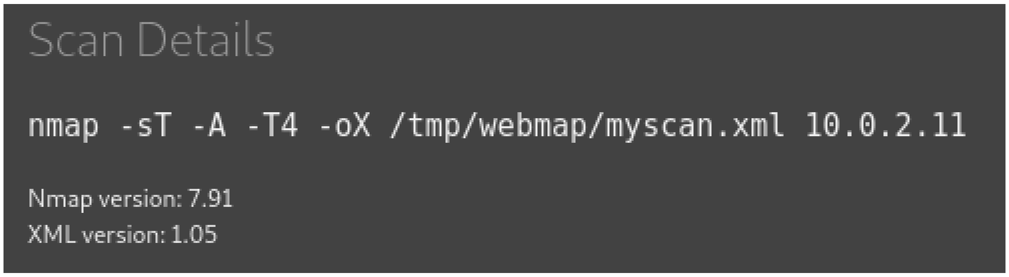
Here you are presented with the same scan results from the first page in more detail along with your advanced options.



SCAN INFORMATION

Start Time: Mon Oct 19 22:55:46 2020
Scan Type: connect
Scan Protocol: tcp
Nmap Command: details

If you click on details under scan information, you are presented with the Nmap command used and some details about your versioning of Nmap.

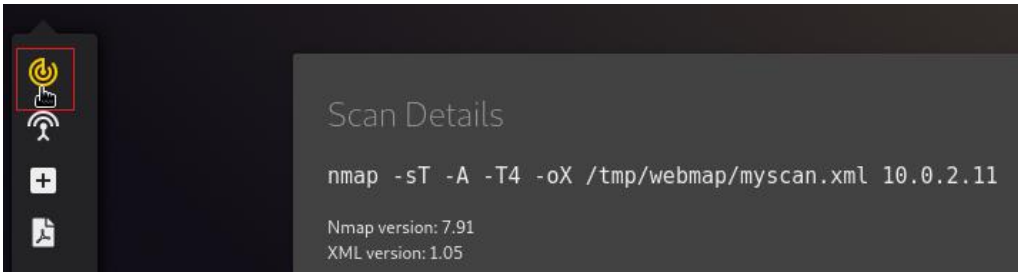


Scan Details

```
nmap -sT -A -T4 -oX /tmp/webmap/myscan.xml 10.0.2.11
```

Nmap version: 7.91
XML version: 1.05

Use your quick launch menu on the left to return to your previous screen.

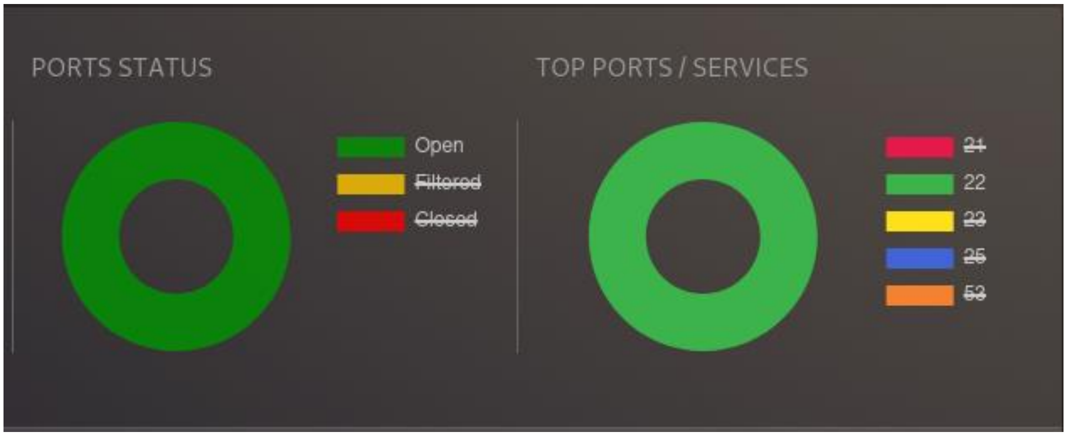


Scan Details

```
nmap -sT -A -T4 -oX /tmp/webmap/myscan.xml 10.0.2.11
```

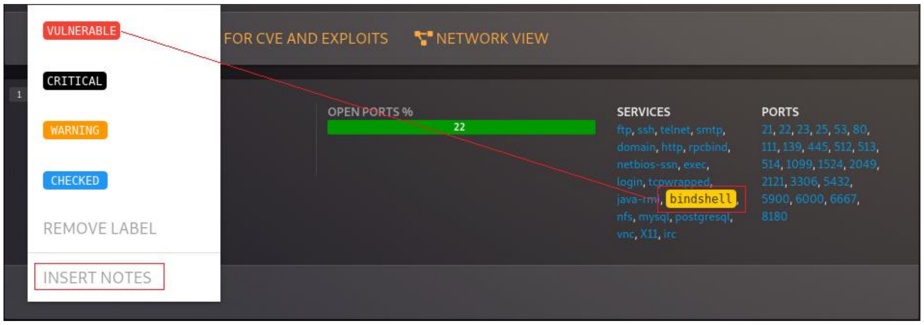
Nmap version: 7.91
XML version: 1.05

You can click on any of the colored status indicators to add ot reduce the amount of detail being shown in the pie chart.



You can scroll down to services to expand your scan results by just clicking on any of the information highlighted in blue text. At the bottom of the services, you will see an Action feature. Any scan result can be labeled by choosing your vulnerable port or service and applying the level of risk from the Action context menu.

Here is where you can add your notes. All this information will be included in your WebMap report.

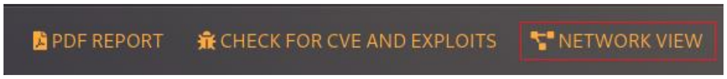


OPEN PORTS % 22

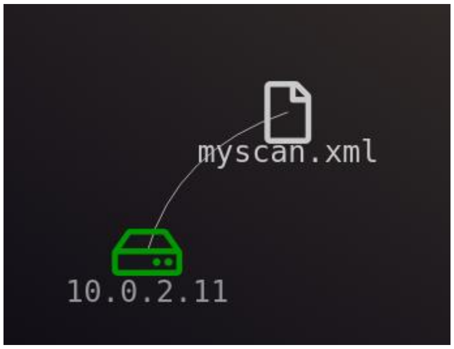
SERVICES
ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, exec, login, tcpwrapped, java-rmi, bindshell, nfs, mysql, postgresql, vnc, X11, irc

PORTS
21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8180

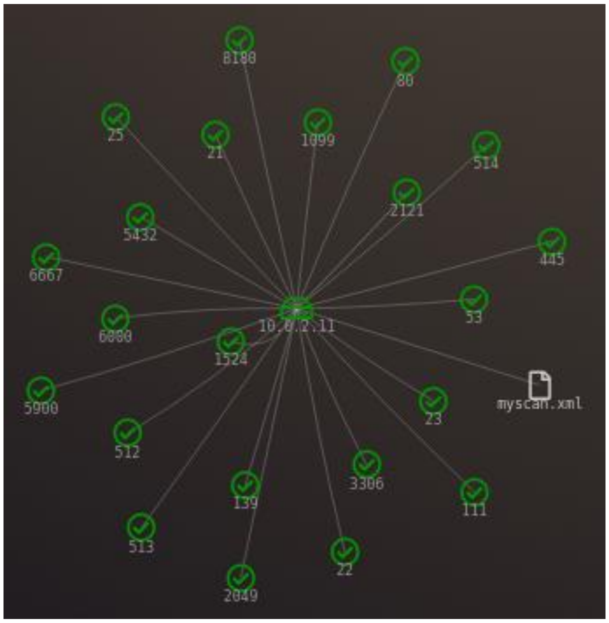
Another feature of WebMap is to generate a network diagram of the target area. Click on Network View.



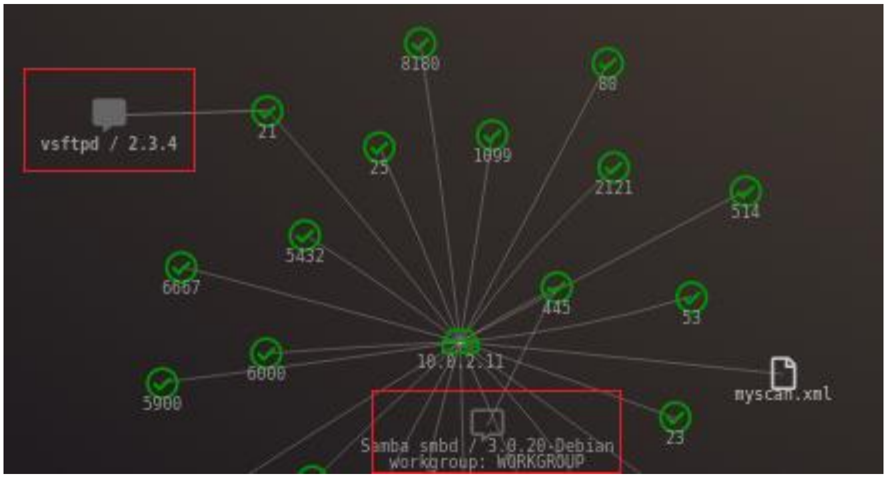
The view is animated, and the objects are moveable. You can zoom in and out using your mouse wheel.



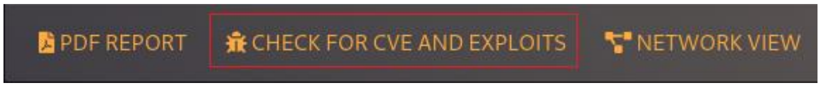
If you click on the scanned device, you will be treated to an exploded view of the machine showing all its vulnerable ports.



If you click on any port in the network view, you will be given information about the service, what application, and version of the application is being hosted.



There is a feature that checks for CVE and exploits, but it uses an API to call on the CVE database and exploits. I can find no information on how to register the API inside of Kali. There is little useful information about the feature and no screenshots of this feature working.



From the author:

CVE & Exploits

Thanks to the amazing API services by circl.lu, WebMap is able to looking for CVE and Exploits for each CPE collected by Nmap. Not all CPE are checked over the circl.lu API, but only when a specific version is specified (for example: `cpe:/a:microsoft:iis:7.5` *and not* `cpe:/o:microsoft:windows`*).*

I guess that since the program is still in beta, this feature will be improved upon later.

The last feature we need to discuss is the PDF report feature. Launching this feature generates a very detailed report of the scan results along with any notes or additional findings you may have added. The report includes the Nmap commands and any NSE scripts used.

Port Scan Report

myscan

If the CVE and exploit lookup feature were included as a part of the report feature, it would have been great to have, but both items can be added to the report using the notes section of the tool.

Summary –

In this lab, we got to see how software emulation using Docker, helps in the installation of programs that Kali might otherwise not allow us to install. Every file or application that WebMap needs to run is downloaded with its Docker image. Docker uses the WebMap image to run the application within its own isolated sandbox, never touching the Kali operating system.

Regardless if you are a pentester, a digital forensic investigator, or a network administrator, generating reports are one of the most challenging aspects of the job. When mixed with the reporting capability of other tools such as NESSUS, WebMap can add much value to your final presentation.