**Lab - Installing the WebMap-Nmap Dashboard**

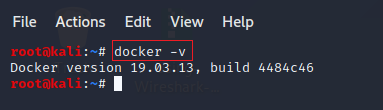
**Overview**

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**

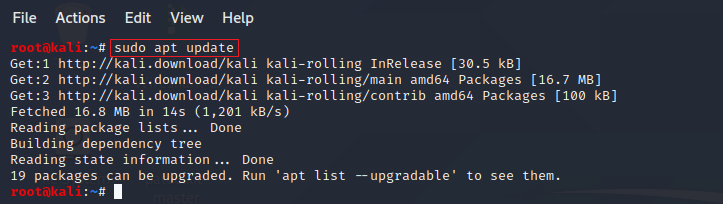
To see if Docker is installed and to see what version is being used, open a terminal and at the prompt type, **docker -v** and press enter.



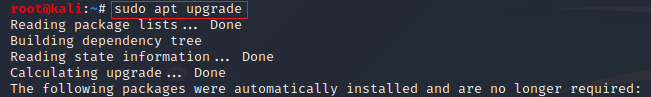
If docker is present, move on to the section of the lab entitled **Installing WebMap.**

**Installing Docker.**

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

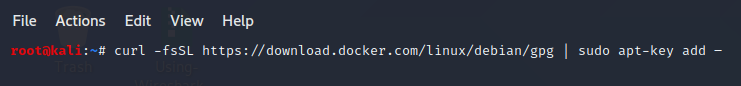


Need to upgrade? **sudo apt upgrade**

****

Add the official Docker PGP key:

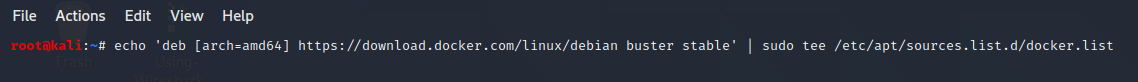
**curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add –**



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

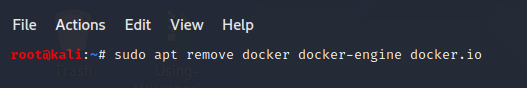
**echo 'deb [arch=amd64] https://download.docker.com/linux/debian buster stable' | sudo tee /etc/apt/sources.list.d/docker.list**

(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.)



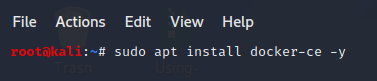
In case you have any older or outdated version of Docker installed on your system, we make sure to get rid of it first:

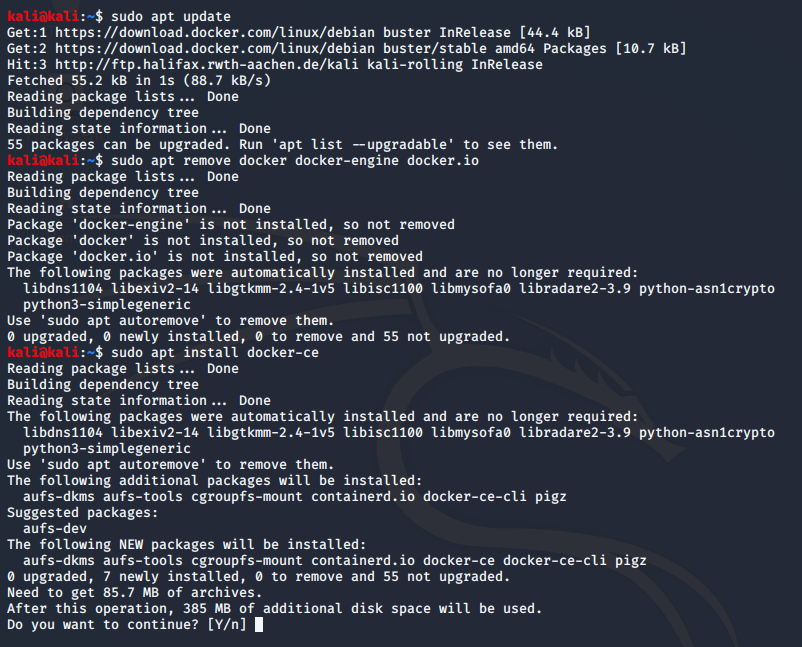
**sudo apt remove docker docker-engine docker.io**

****

**Install Docker**

**sudo apt install docker-ce -y**

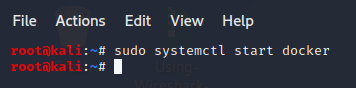
****



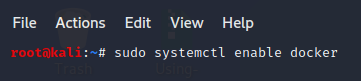
**Start Docker Service**

This command starts Docker as you need it.

**sudo systemctl start docker**

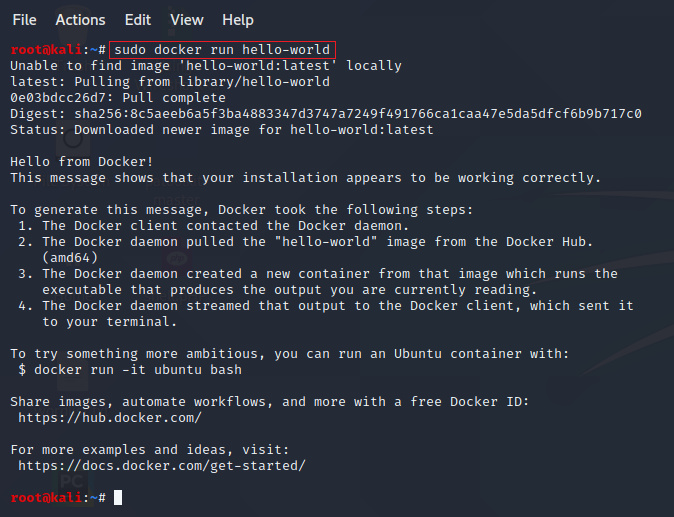
****

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

****

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

**sudo docker run hello-world**



**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 \**

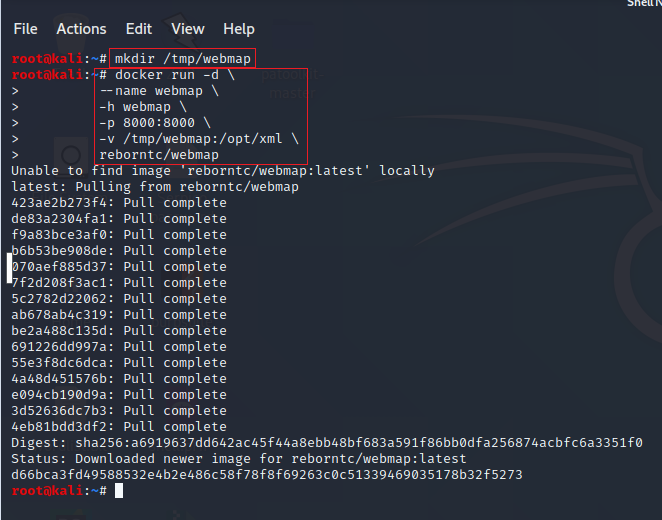
**-p 8000:8000 \**

**-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.**



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.

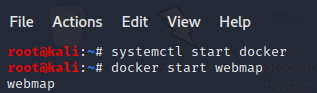
This starts the Docker service.

At the next terminal prompt type,

**docker start webmap**

Press enter.

This starts the WebMap docker image inside the Docker container.

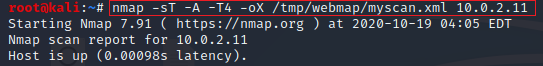


**Start a Nmap scan**

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

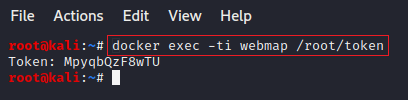
**nmap -sT -A -T4 -oX /tmp/webmap/myscan.xml 10.0.2.11**

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**



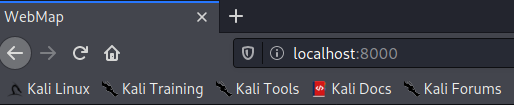
Once our Nmap scan completes are ready to view the results using WebMap, but before we can log in, we will need to generate a logon token using the following command at the Kali terminal.

**docker exec -ti webmap /root/token**

****

Highlight and copy the token.

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



Press enter.

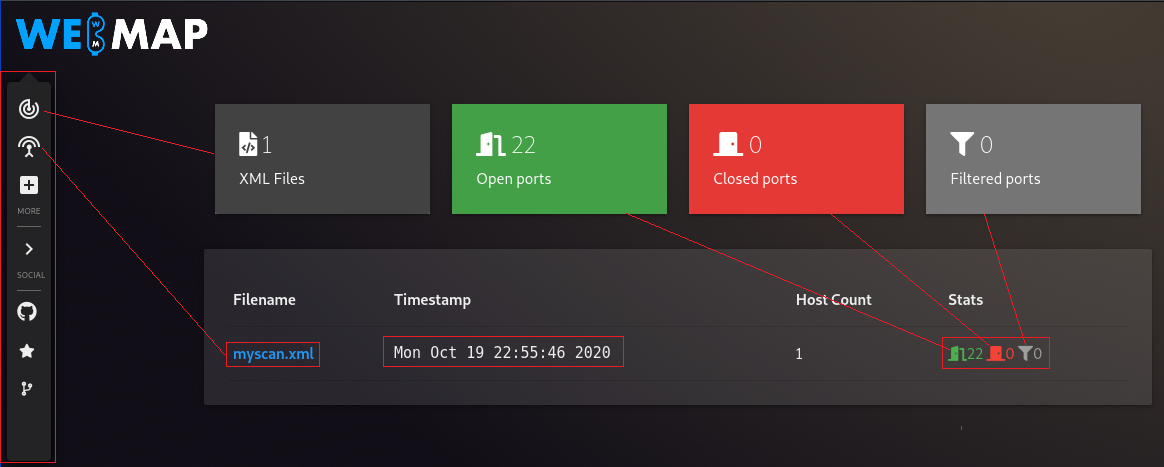
The first time you log in to WebMap, you will be asked for a Token. Copy and paste the token in the token field of the login screen.

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

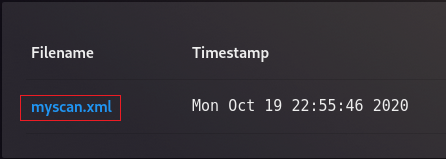
**Navigating WebMap**

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.

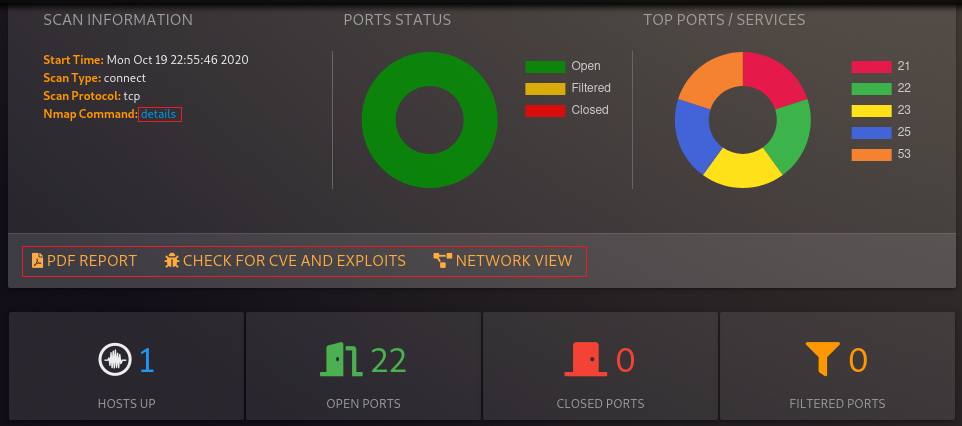
Everything in WebMap is colored coded.



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



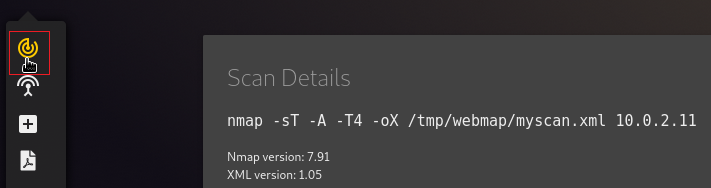
Here you are presented with the same scan results from the first page in more detail along with your advanced options.



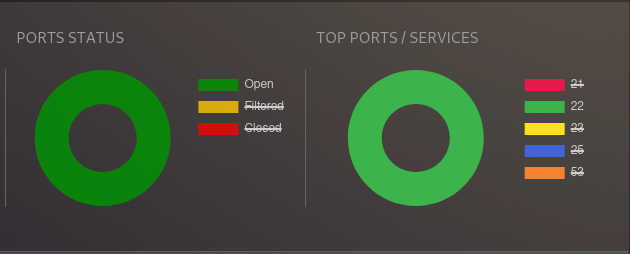
If you click on details under scan information, you are presented with the Nmap command used and some details about your versioning of Nmap.



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

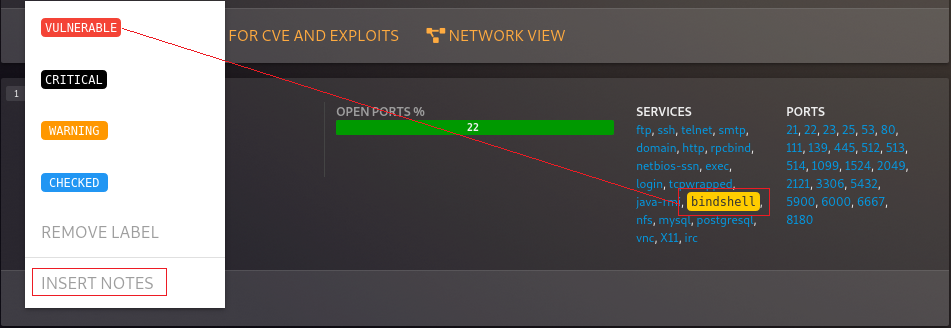


You can click on any of the colored status indicators to add ot reduce the amount of detail being shown in the pie chart.



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.

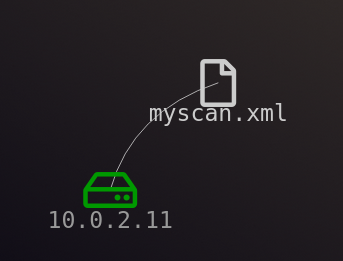
Here is where you can add your notes. All this information will be included in your WebMap report.



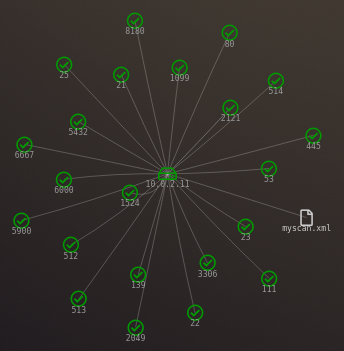
Another feature of WebMap is to generate a network diagram of the target area. Click on Network View.



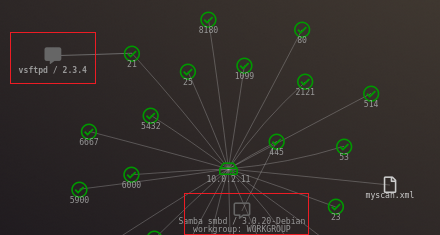
The view is animated, and the objects are moveable. You can zoom in and out using your mouse wheel.



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.



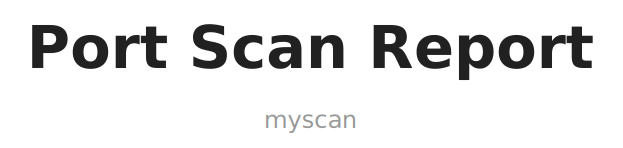
From the author:

**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.



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.