

Install Metasploitable

Metasploitable contains a set of vulnerable Web applications that can be used as software under test for Web application security testing. You can install Metasploitable on your cloud machines.

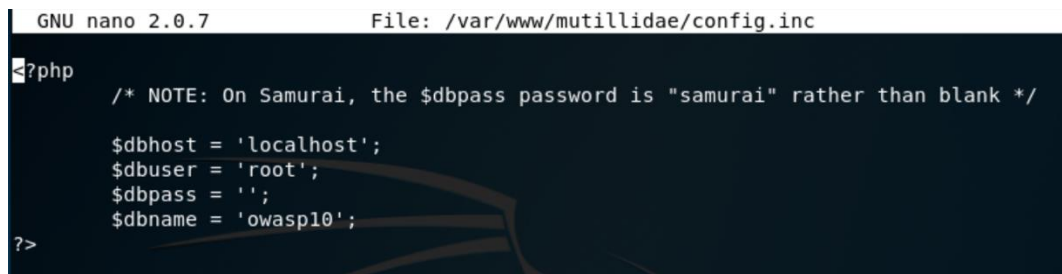
The following steps describe the setup process of Metasploitable 2.0 based on container¹ technology (we will use docker container in this process).

- 1) Create a new Ubuntu 18.04 VM, allow HTTP and HTTPs traffic to your machine. Setup your firewall so that the Web applications inside this VM are accessible from outside.
- 2) SSH to your VM and run the following commands:
- 3) Install docker container

```
sudo apt-get update
sudo apt install docker.io
sudo systemctl start docker
sudo systemctl enable docker
docker --version
```
- 4) Download Metasploitable

```
sudo docker pull tleemcjr/metasploitable2
```
- 5) Create a config with the following content and save your file

```
sudo apt-get install nano
cd ~/
touch config.inc
nano config.inc
```



```
GNU nano 2.0.7      File: /var/www/mutillidae/config.inc
?php
/* NOTE: On Samurai, the $dbpass password is "samurai" rather than blank */

$dbhost = 'localhost';
$dbuser = 'root';
$dbpass = '';
$dbname = 'owasp10';
?>
```

- 6) Now start your docker using the given config file, and exposing port 80 for outside access

¹ Container technology is a method of packaging an application so it can be run with isolated dependencies, and they have fundamentally altered the development of software today due to their compartmentalization of a computer system.

```
sudo docker run -p 80:80 --name metasploitable --rm -it -v ~/config.inc:/var/www/mutillidae/config.inc tleemcjr/metasploitable2:latest sh -c "bash"
```

Start the Web application inside the container:

`/bin/services.sh`

```
jazmine_amannejad@meta2:~$  
jazmine_amannejad@meta2:~$ sudo docker run -p 80:80 --name metasploitable --rm -it -v ~/config.inc:/var/www/mutillidae/config.inc tleemcjr/metasploitable2:latest sh -c "bash"  
root@b3fd00e2800a:/# /bin/services.sh
```

- 7) Now, you should be able to access your Web application online at <http://IP ADDRESS/>
 - Make sure to use HTTP.
- 8) If, you cannot access it, it might be because of your firewall settings or your setup was incorrect. Open another SSH window and type “**curl localhost**”. If this works as the below image, but you cannot access the page in browser, you need to fix your firewall settings.

```
jazmine_amannejad@meta-testinstall:~$ curl localhost  
<html><head><title>Metasploitable2 - Linux</title></head><body>  
<pre>  
  
Metasploitable2  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
</pre>  
<ul>  
<li><a href="/twiki/">TWiki</a></li>  
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>  
<li><a href="/mutillidae/">Mutillidae</a></li>  
<li><a href="/dvwa/">DVWA</a></li>  
<li><a href="/dav/">WebDAV</a></li>  
</ul>  
</body>  
</html>
```

- 9) Metasploitable contains several Web applications: TWiki, phpMyAdmin, Mutillidae, DVWA, WebDAV. Here we will be using DVWA (Damn Vulnerable Web Application).
 - Feel free to use the other ones as your application under test, if you want to have more practice for Security testing.


Username and password for DVWA are **admin**, **password**.

Note 1: Considering that Metasploitable is a vulnerable Web application, you'd better run your VM only when you need it and stop it when you are done.

Note 2: If you turn off your machine, in your next uses, you only need to repeat step 6 (the following two commands):

```
sudo docker run -p 80:80 --name metasploitable --rm -it -v  
~/config.inc:/var/www/mutillidae/config.inc tleemcjr/metasploitable2:latest sh -c "bash"
```

[/bin/services.sh](#)

The logo for Metasploitable, featuring the word "metasploitable" in a stylized, blocky font where each letter is composed of a grid of small squares.

Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

