ssh-keygen to create a new SSH key pair.

cat ~/.ssh/id\_rsa.pub to display your id\_rsa.pub key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC4vJxMDKgHxHJsUvg6z00etGv5ON/lZ+NEZp2QKCnARuIz+ozgUhfUzuVn9q4qlom8SK5DumAyS7xqRTdQyj9WvnJk9Op71rI9uAUrOh8gvpVENOfSwLT+WaN7WrFxa6KSgfDYoQcbVe+Bz0bUqeTv+KTuuAdRDtl1ef9SkzeFezwX8dEakJd4zksWV3CCBy0Kr5TMfILEV2KonExWadjCkli30t0IhPuQqgpkmrU/WrWjzGdKIQFzlEqhEKOrgPui10D/Oa1iVDVTKHAKMEpAi6Q9lcKwa6iabS1wr4LrjcTZgZ2dUpPeqhkjlv4cmd6I09/s4i6ermYcM2RHqDtN RedAdmin@Jump-Box-Provisoner

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDO1ZlhltFo54c3xqHVui1Xl1odl9okM0zVw5MIkiEQ3oYxSsFwx7LmBzg/DguinWU2nqssSyA1w7kPqHc28UmPIvaBs/y4Q9I5+oA5oTJ0+Zo21OU5rkAY6wQnatRQ3nCGRl0bAWtPdXMX/4ujHY3ixA4a+dQ2bn/QZXhsM6s8YlTqTVzIBJpM8STp+/rQUB4i2I6LxUK9rMcsUZnjr3wwGf4GFoxIwynQ0lTxsR55Gfo5hZJC5xxMeZytM0n1B0uA3pdHBvZqcSibIzhCXVvE1m2alCvE5qN6xyfxECwiaIxHD8rRMmutQLO+XrT/W5t9FUnPSGmINh5lNNTsa57 root@caade18fd244

curl icanhazip.com find your IP address or googling "What's my IP address?

Cd ./ssh

Ssh [Redadmin@ 20.185.196.133](mailto:Redadmin@52.255.132.125)ansib (username@publicjumpboxip)

Ssh -i ~/.ssh/RedAdmin

Ssh [RedAdmin@10.1.0.4](mailto:RedAdmin@10.1.0.4) to connect to ELK

**Sudo docker ps** to check your ansible container

Sudo docker container list -a  to verify that the container is on.

Cd /etc/hosts

Ctl + shift + \_ In nano

Nano hosts

Ansible webservers -m ping

Sudo docker start elk ( If it isn't, run)

Check for your Ansible container: sudo docker ps

Cd /etc/ansible

Ls

Nano hosts

Nano elk.yml

Ansible-playbook elk.yml

### SSH

Secure Shell sets up an encrypted connection between two machines. Commands given on the first machine are executed on the second machine and output from the second machine is sent back to the first machine.

The result is the ability to control a remote machine using the command line while keeping all your actions private from any would be attacker or snooper.

#### ssh-keygen

The ssh-keygen command creates a private/public key pair that you can use to authenticate your SSH connections. Once created, the public key is copied to the server into the ~/.ssh/known\_hosts file.

# Create an ssh public/private key pair

ssh-keygen

You can create a password for your SSH key if you wish, but this isn't recommended if the SSH key is going to be used for automation purposes.

#### ssh-copy-id

The ssh-copy-id command will copy the public ssh key into the correct location on the remote server.

# copy the public key for 'mykey' to the ~/.ssh/known\_hosts file on a remote machine

ssh-copy-id -i ~/.ssh/mykey user@<host ip>

#### ssh

The ssh command creates an ssh connection to a remote machine. If you do not have an SSH key in place, you will be prompted for a password.

# Connect to the machine with the IP address 10.10.0.4 using the 'admin' user.

ssh admin@10.10.0.4

You can create multiple keys for different purposes and different machines. To specify a particular key, use the -i flag.

# Connect to the machine at 10.10.0.4 using a specific 'mykey' identity

ssh -i mykey.pub admin@10.10.0.4

### Docker

Docker allows you to run Linux containers on any server or local machine. Containers are similar to a virtual machine, except they only run the resources necessary to complete their specific task.

A container typically only runs one task. This could be a web server, or a particular application or any program you choose. They are similar to an app on your phone. A container is completely self sufficient and has everything it needs to run.

#### docker pull

docker pull will copy a container to the server so you can run it.

# download the 'dvwa' container from the 'cyberxsecurity' docker repository

docker pull cyberxsecurity/dvwa

#### docker image ls

docker image ls lists all of the container images that are copied to the server. Each image can be used to create any number of containers.

docker image ls

REPOSITORY TAG IMAGE ID CREATED SIZE

cyberxsecurity/ansible latest 6657e0b22542 11 days ago 303MB

ubuntu 18.04 775349758637 7 weeks ago 64.2MB

#### docker container list -a

docker container list -a will list all of the containers on the system, including containers that are not running.

#### docker run

docker run will create a container from the specified image.

# Run the cyberxsecurity/ansible container

docker run cyberxsecurity/ansible

# Run the container using the image ID 6657e0b22542

docker run 6657e0b22542

#### docker start

docker start container\_name will start a stopped container. This does not create a container from a container image. Instead, it will only start a container that you already have created.

#### docker stop

docker stop will stop a running container. This is similar to shutting down a VM.

# stop the ansible container

docker stop ansible

#### docker exec

docker exec will execute a command directly on a container and return the output of that command to you. This is commonly used to get a bash shell on the container by executing the bash command.

# run the `bash` command on a container named 'my-container'

docker exec -it my-container /bin/bash

Here the -it flags stand for interactive and terminal or interactive terminal all together. The result is that this command returns a bash shell.

#### docker attach

docker attach will give you a shell on the specified container. This works similarly to an SSH connection and can be used instead of the exec command above to get a bash shell on a container.

# connect to the container named ansible

docker attach ansible

#### docker image rm

docker image rm removes an image from the server

# Remove the dvwa container image from the server

docker image rm dvwa

### Ansible

Ansible is a provisioner that can be used to configure any Linux machine. There is significant documentation for how to use Ansible on their website [HERE](https://docs.ansible.com/ansible/latest/user_guide/intro_getting_started.html).

#### ansible all -m ping

Ansible usually needs a file full of commands called a 'playbook' in order to complete it's tasks. However, you can also execute single commands if you wish using the -m flag to specify the module you want to use.

With this command we are using the 'ping' module (-m) on 'all' of the machines listed in the hosts file.

# Ping all of the hosts in the hosts file using the ping module

ansible all -m ping

#### ansible-playbook

The ansible-playbook command will run the contents of a playbook.yml file. The playbook file can be named anything you wish as long as it ends in .yml and it has the correct formatting.

# Run the playbook 'my-playbook.yml'

ansible-playbook my-playbook.yml

#### Ansible playbooks

Playbooks always carry the .yml extension and begin with --- on the first line to signify that it is a YAML file.

The first few lines of the playbook will give global settings for the file and notate what machines the playbook is to use, if you would like to run the commands as root, and what tasks are to be completed.

---

- name: Config Web VM with Docker

hosts: web

become: true

tasks:

In this Definition, we give the playbook a descriptive name, specify that is to run on the machines listed under the web headding in the hosts file, specify that all commands should be run as root, and then start listing the tasks.

* name: can be anything you wish
* hosts: specify what machines are to be used. Here we are using the web hosts.
* become: true means: 'Become the root user for all the following commands'
* tasks: starts the task section where all other commands/tasks will be listed.

#### Ansible apt module

Ansible modules can easily be found by googling 'Ansible module <name-of-thing-you-want-to-do>'

The apt module lets you install applications using the apt-get commands.

# Install nano. force `apt-get` to be used instead of just `apt`

- name: Install nano

apt:

force\_apt\_get: yes

name: nano

state: present

See all of the apt module options [HERE](https://docs.ansible.com/ansible/latest/modules/apt_module.html)

#### Ansible pip module

The pip module allows you to install python packages as if you were using the command pip install

The syntax is just like the apt module.

- name: Install Docker python module

pip:

name: docker

state: present

See all of the pip module options [HERE](https://docs.ansible.com/ansible/latest/modules/pip_module.html)

#### Ansible docker-container

The docker-container module can be used to download and manage Docker containers.

Here we are downloading the container cyberxsecurity/dvwa, staring the container, and forwarding the host port 80 to the container port 80

- name: download and launch a docker web container

docker\_container:

name: dvwa

image: cyberxsecurity/dvwa

state: started

published\_ports: 80:80

RedAdmin@Jump-Box-Provisoner:~$ sudo docker start practical\_lederberg

practical\_lederberg

RedAdmin@Jump-Box-Provisoner:~$ sudo docker attach practical\_lederberg

root@caade18fd244:~# cat ~/.ssh/id\_rsa.pub

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDO1ZlhltFo54c3xqHVui1Xl1odl9okM0zVw5MIkiEQ3oYxSsFwx7LmBzg/DguinWU2nqssSyA1w7kPqHc28UmPIvaBs/y4Q9I5+oA5oTJ0+Zo21OU5rkAY6wQnatRQ3nCGRl0bAWtPdXMX/4ujHY3ixA4a+dQ2bn/QZXhsM6s8YlTqTVzIBJpM8STp+/rQUB4i2I6LxUK9rMcsUZnjr3wwGf4GFoxIwynQ0lTxsR55Gfo5hZJC5xxMeZytM0n1B0uA3pdHBvZqcSibIzhCXVvE1m2alCvE5qN6xyfxECwiaIxHD8rRMmutQLO+XrT/W5t9FUnPSGmINh5lNNTsa57 root@caade18fd244

root@caade18fd244:~# ssh RedAdmin@10.0.0.5

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that a host key has just been changed.

The fingerprint for the ECDSA key sent by the remote host is

SHA256:uJwXU+oHCFyCXsTUT/EL+L5eLUyPDS71gl3KUkqFT1M.

Please contact your system administrator.

Add correct host key in /root/.ssh/known\_hosts to get rid of this message.

Offending ECDSA key in /root/.ssh/known\_hosts:1

remove with:

ssh-keygen -f "/root/.ssh/known\_hosts" -R "10.0.0.5"

ECDSA host key for 10.0.0.5 has changed and you have requested strict checking.

Host key verification failed.

root@caade18fd244:~# ssh-keygen -f "/root/.ssh/known\_hosts" -R "10.0.0.5"

# Host 10.0.0.5 found: line 1

/root/.ssh/known\_hosts updated.

Original contents retained as /root/.ssh/known\_hosts.old

root@caade18fd244:~# ssh RedAdmin@10.0.0.5

The authenticity of host '10.0.0.5 (10.0.0.5)' can't be established.

ECDSA key fingerprint is SHA256:uJwXU+oHCFyCXsTUT/EL+L5eLUyPDS71gl3KUkqFT1M.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.0.0.5' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1043-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Tue Apr 6 18:03:23 UTC 2021

System load: 0.0 Processes: 109

Usage of /: 4.6% of 28.90GB Users logged in: 0

Memory usage: 10% IP address for eth0: 10.0.0.5

Swap usage: 0%

0 packages can be updated.

0 of these updates are security updates.

New release '20.04.2 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr 6 17:18:26 2021 from 10.0.0.4

To run a command as administrator (user "root"), use "sudo <command>".

See "man sudo\_root" for details.

RedAdmin@DVWA-VM1:~$ exit

logout

Connection to 10.0.0.5 closed.

root@caade18fd244:~# ssh-keygen -f "/root/.ssh/known\_hosts" -R "10.0.0.6"

# Host 10.0.0.6 found: line 1

/root/.ssh/known\_hosts updated.

Original contents retained as /root/.ssh/known\_hosts.old

root@caade18fd244:~# ssh-keygen -f "/root/.ssh/known\_hosts" -R "10.0.0.7"

# Host 10.0.0.7 found: line 1

/root/.ssh/known\_hosts updated.

Original contents retained as /root/.ssh/known\_hosts.old

root@caade18fd244:~# ssh-keygen -f "/root/.ssh/known\_hosts" -R "10.1.0.4"

# Host 10.1.0.4 found: line 1

/root/.ssh/known\_hosts updated.

Original contents retained as /root/.ssh/known\_hosts.old

root@caade18fd244:~# ssh RedAdmin@10.0.0.6

The authenticity of host '10.0.0.6 (10.0.0.6)' can't be established.

ECDSA key fingerprint is SHA256:rxvVQ3vpWuJyQYNKJudK06K152dBvThS1A1ZIxvs2AM.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.0.0.6' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1043-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Tue Apr 6 18:04:30 UTC 2021

System load: 0.0 Processes: 109

Usage of /: 4.6% of 28.90GB Users logged in: 0

Memory usage: 10% IP address for eth0: 10.0.0.6

Swap usage: 0%

\* Introducing self-healing high availability clusters in MicroK8s.

Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

https://microk8s.io/high-availability

0 packages can be updated.

0 of these updates are security updates.

New release '20.04.2 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr 6 17:50:43 2021 from 10.0.0.4

To run a command as administrator (user "root"), use "sudo <command>".

See "man sudo\_root" for details.

RedAdmin@DVWA-VM2:~$ exit

logout

Connection to 10.0.0.6 closed.

root@caade18fd244:~# ssh RedAdmin@10.0.0.7

The authenticity of host '10.0.0.7 (10.0.0.7)' can't be established.

ECDSA key fingerprint is SHA256:fHsOhXcnokcwA5zoi7Uz19DAlzNwBlZTia7UZsG1Z4Q.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.0.0.7' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1043-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Tue Apr 6 18:04:39 UTC 2021

System load: 0.0 Processes: 109

Usage of /: 4.6% of 28.90GB Users logged in: 0

Memory usage: 9% IP address for eth0: 10.0.0.7

Swap usage: 0%

0 packages can be updated.

0 of these updates are security updates.

New release '20.04.2 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr 6 17:19:08 2021 from 10.0.0.4

To run a command as administrator (user "root"), use "sudo <command>".

See "man sudo\_root" for details.

RedAdmin@DVWA-VM3:~$ exit

logout

Connection to 10.0.0.7 closed.

root@caade18fd244:~# ssh RedAdmin@10.1.0.4

The authenticity of host '10.1.0.4 (10.1.0.4)' can't be established.

ECDSA key fingerprint is SHA256:F5DQYg1gXvcnAJK84h/K1SECzXO7JE5M7md86pP7WsQ.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.1.0.4' (ECDSA) to the list of known hosts.

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1043-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Tue Apr 6 18:04:54 UTC 2021

System load: 0.08 Processes: 133

Usage of /: 17.9% of 28.90GB Users logged in: 0

Memory usage: 34% IP address for eth0: 10.1.0.4

Swap usage: 0% IP address for docker0: 172.17.0.1

\* Introducing self-healing high availability clusters in MicroK8s.

Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

https://microk8s.io/high-availability

\* Canonical Livepatch is available for installation.

- Reduce system reboots and improve kernel security. Activate at:

https://ubuntu.com/livepatch

10 packages can be updated.

0 of these updates are security updates.

To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr 6 17:51:17 2021 from 10.0.0.4

RedAdmin@ELK-SERVER:~$ exit

logout

Connection to 10.1.0.4 closed.

root@caade18fd244:~# ls /etc/a

adduser.conf alternatives/ ansible/ apt/

root@caade18fd244:~# ls /etc/ansible/

ansible.cfg filebeat-playbook.yml hosts pentest.yml

elk.yml files metricbeat-playbook.yml roles

root@caade18fd244:~# nano /etc/ansible/hosts

root@caade18fd244:~# nano /etc/ansible/ansible.cfg

root@caade18fd244:~# ansible all -m ping

10.0.0.7 | SUCCESS => {

"changed": false,

"ping": "pong"

}

10.0.0.5 | SUCCESS => {

"changed": false,

"ping": "pong"

}

10.0.0.6 | SUCCESS => {

"changed": false,

"ping": "pong"

}

10.1.0.4 | SUCCESS => {

"changed": false,

"ping": "pong"

}

root@caade18fd244:~# nano /etc/ansible/pentest.yml

root@caade18fd244:~# ansible-playbook /etc/ansible/pentest.yml

PLAY [Config Web VM with Docker] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.0.0.6]

ok: [10.0.0.5]

ok: [10.0.0.7]

TASK [docker.io] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.0.0.5]

changed: [10.0.0.7]

changed: [10.0.0.6]

TASK [Install pip3] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.0.0.6]

changed: [10.0.0.5]

changed: [10.0.0.7]

TASK [Install Docker python module] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.0.0.6]

changed: [10.0.0.5]

changed: [10.0.0.7]

TASK [download and launch a docker web container] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.0.0.7]

changed: [10.0.0.5]

changed: [10.0.0.6]

TASK [Enable docker service] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

changed: [10.0.0.6]

changed: [10.0.0.7]

changed: [10.0.0.5]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.0.0.5 : ok=6 changed=5 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

10.0.0.6 : ok=6 changed=5 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

10.0.0.7 : ok=6 changed=5 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

root@caade18fd244:~#

root@caade18fd244:~# ssh RedAdmin@10.0.0.5

Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1043-azure x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

System information as of Tue Apr 6 18:24:17 UTC 2021

System load: 0.58 Processes: 125

Usage of /: 10.6% of 28.90GB Users logged in: 0

Memory usage: 24% IP address for eth0: 10.0.0.5

Swap usage: 0% IP address for docker0: 172.17.0.1

4 packages can be updated.

3 of these updates are security updates.

To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.

Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Apr 6 18:22:54 2021 from 10.0.0.4

RedAdmin@DVWA-VM1:~$ curl localhost/setup.php

<!DOCTYPE html>

<html lang="en-GB">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Setup :: Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</title>

<link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

<link rel="icon" type="\image/ico" href="favicon.ico" />

<script type="text/javascript" src="dvwa/js/dvwaPage.js"></script>

</head>

<body class="home">

<div id="container">

<div id="header">

<img src="dvwa/images/logo.png" alt="Damn Vulnerable Web Application" />

</div>

<div id="main\_menu">

<div id="main\_menu\_padded">

<ul class="menuBlocks"><li class="selected"><a href="setup.php">Setup DVWA</a></li>

<li class=""><a href="instructions.php">Instructions</a></li>

</ul><ul class="menuBlocks"><li class=""><a href="about.php">About</a></li>

</ul>

</div>

</div>

<div id="main\_body">

<div class="body\_padded">

<h1>Database Setup <img src="dvwa/images/spanner.png" /></h1>

<p>Click on the 'Create / Reset Database' button below to create or reset your database.<br />

If you get an error make sure you have the correct user credentials in: <em>/var/www/html/config/config.inc.php</em></p>

<p>If the database already exists, <em>it will be cleared and the data will be reset</em>.<br />

You can also use this to reset the administrator credentials ("<em>admin</em> // <em>password</em>") at any stage.</p>

<hr />

<br />

<h2>Setup Check</h2>

Operating system: <em>\*nix</em><br />

Backend database: <em>MySQL</em><br />

PHP version: <em>7.0.33-0+deb9u10</em><br />

<br />

Web Server SERVER\_NAME: <em>localhost</em><br />

<br />

PHP function display\_errors: <em>Disabled</em><br />

PHP function safe\_mode: <span class="success">Disabled</span><br/ >

PHP function allow\_url\_include: <span class="success">Enabled</span><br/ >

PHP function allow\_url\_fopen: <span class="success">Enabled</span><br />

PHP function magic\_quotes\_gpc: <span class="success">Disabled</span><br />

PHP module gd: <span class="success">Installed</span><br />

PHP module mysql: <span class="success">Installed</span><br />

PHP module pdo\_mysql: <span class="success">Installed</span><br />

<br />

MySQL username: <em>app</em><br />

MySQL password: <em>\*\*\*\*\*\*</em><br />

MySQL database: <em>dvwa</em><br />

MySQL host: <em>127.0.0.1</em><br />

<br />

reCAPTCHA key: <span class="failure">Missing</span><br />

<br />

[User: www-data] Writable folder /var/www/html/hackable/uploads/: <span class="success">Yes</span><br />

[User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: <span class="success">Yes</span><br />

<br />

<br />

[User: www-data] Writable folder /var/www/html/config: <span class="success">Yes</span>

<br />

<i><span class="failure">Status in red</span>, indicate there will be an issue when trying to complete some modules.</i><br />

<br />

If you see disabled on either <i>allow\_url\_fopen</i> or <i>allow\_url\_include</i>, set the following in your php.ini file and restart Apache.<br />

<pre><code>allow\_url\_fopen = On

allow\_url\_include = On</code></pre>

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

<br /><br /><br />

<!-- Create db button -->

<form action="#" method="post">

<input name="create\_db" type="submit" value="Create / Reset Database">

<input type='hidden' name='user\_token' value='44aafbf4d4eefaab07c83384703e88e9' />

</form>

<br />

<hr />

</div>

<br /><br />

</div>

<div class="clear">

</div>

<div id="system\_info">

</div>

<div id="footer">

<p>Damn Vulnerable Web Application (DVWA) v1.10 \*Development\*</p>

<script src='/dvwa/js/add\_event\_listeners.js'></script>

</div>

</div>

</body>

</html>RedAdmin@DVWA-VM1:~$ exit

logout

Connection to 10.0.0.5 closed.

root@caade18fd244:~#