valhalla Documentation

Release 0.1

valhalla

November 17, 2016

Contents

This project aims to provide a simple and easy way to do penetration testing with the OWASP pentester guide.

CHAPTER 1

The execution idea

In the penetration testing world there are alot of tools, which Valhalla assembles into different Docker containers. This keeps them separated from your local system, providing a good and simple way to version and execute them via a nice looking web GUI.

Internally the process is simple. A Docker container holds each tool that we need, and around the container is a small Rest API. This lets the user execute commands and get the results in the following way:

```
>>> from valhalla.dockerutils import OwtfContainer
>>> from valhalla.middleman.handler import send_for_execution
>>> oc = OwtfContainer('valhalla/containers/testcontainer')  # Point to the container
>>> oc.build_image()  # Build Docker image
>>> oc.build_container()  # Build continer from image
>>> oc.is_valid  # Check if valid
True
>>> oc.start()  # Start the container
>>> send_for_execution(oc, {'command': 'ping -c 1 scanme.nmap.org'})  # Execute command
```

Contents:

1.1 containerutils

1.1.1 OwtfContainer

The OwtfContainer is the main object in this application and has one single constructor argument, being an Owtf Valhalla Docker image location.

When a new OwtfContainer class is instantiated, the class constructor will call *_validate_config_image_and_container()*. This will then check that everything is OK with all the needed files in place, if the image has been built, if the container is running and so on.

1.2 middleman

CHAPTER 2

Indices and tables

- genindex
- modindex
- search