**简介**

服务端机器

服务端安装位置

/opt/mhn/

服务组件日志位置

/var/log/mhn/

服务端地址

http://1

Superuser email:

Superuser password:

节点及机器名

10.225 senso

节点蜜罐类型：dionaea。

安装位置：docker

日志位置：/var/dionaea

配置位置：/etc/Dionaea

配置文件中有自己蜜罐的名字。Hpfeed 的地址及端口

进入docker命令：docker exec -it a3f009163c25 /bin/bash

# 0x08 MHN的web界面

MHN的web接口是很简洁明了的，第一次访问web截面时，需要输入账户名和密码，登录成功后会看见一个总结性的页面

1.在最近24小时内有多少攻击着攻击

2.攻击次数排在前五的IP

3.被攻击端口排在前五的端口

4.top 5的攻击签名

Map 页面就是显示的地图，这里一开始点击会显示说 404，需要在配置文件把页面地址更改一下 > vim /opt/mhn/server/config.py

把 > HONEYMAP\_URL = ‘:3000’

改成

HONEYMAP\_URL = ‘[http://ip:3000'](http://ip:3000'/)

ip 即为该服务器 ip

Deploy 页面即保存部署蜜罐的脚本，可以下拉选择不同的蜜罐，也可以自定义脚本。它提供的脚本不一定完全适用，有些情况需要自己更改一下。复制上面的 Deploy Command 到另外的机器上执行，完成后一般就会在 Sensors 显示新安装的蜜罐节点。

Attack 页面记录攻击源，攻击端口，受攻击节点，攻击事件，攻击协议。

Plyloads 页面显示一些攻击行为的 payload，包括 sql 注入，恶意扫描等，它会记录所有 url 访问。只针对http扫描有记录

Rules 页面可以自定义一些触发规则，一般保持默认就好

Sensors 是各个蜜罐节点的情况，成功运行的蜜罐会在这里显示

Charts 页面会显示 ssh 蜜罐收集到的用户名密码等，这里显示的是 cowrie 捕捉到的一些 ssh 尝试登录，以及 top 用户名和密码