**网络信息安全**

**实验报告**

学号： 2220193816

姓名： 赤凯

班级： 网络2班

报告日期：2022年6月25

实验四： 综合扫描实验

**【实验目的】**

**尝试搭建和学习蜜罐环境**

**【实验内容】**

**1、搭建HFish 蜜罐系统**

**2、模拟攻击和使用蜜罐**

**【实验环境】**

**ubuntu 18.04 LTS**

**【实验步骤】**

1. **HFISH 介绍**

**HFish 是一款国产开源的现代蜜罐系统，在github拥有3.3K个star。HFish是一款社区型免费蜜罐，侧重企业安全场景，从内网失陷检测、外网威胁感知、威胁情报生产三个场景出发，为用户提供可独立操作且实用的功能，通过安全、敏捷、可靠的中低交互蜜罐增加用户在失陷感知和威胁情报领域的能力。**

**HFish具有超过40种蜜罐环境、提供免费的云蜜网、可高度自定义的蜜饵能力、一键部署、跨平台多架构、国产操作系统和CPU支持、极低的性能要求、邮件/syslog/webhook/企业微信/钉钉/飞书告警等多项特性，帮助用户降低运维成本，提升运营效率。**

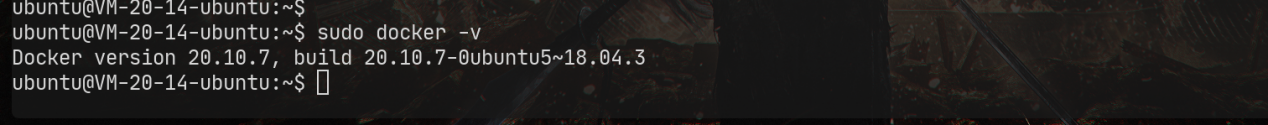
1. **搭建docker 环境**

**在ubuntu 终端输入如下命令:**

**sudo apt install docker**

**sudo apt install docker.io**

**输入命令查看版本:**

****

1. **使用docker 构建 HFish 蜜罐**

**拉取hfish镜像:**

docker run -itd --name hfish \

-v /usr/share/hfish:/usr/share/hfish \

--network host \

--privileged=true \

threatbook/hfish-server:latest

配置自动升级:

docker run -d \

--name watchtower \

--restart unless-stopped \

-v /var/run/docker.sock:/var/run/docker.sock \

--label=com.centurylinklabs.watchtower.enable=false \

--privileged=true \

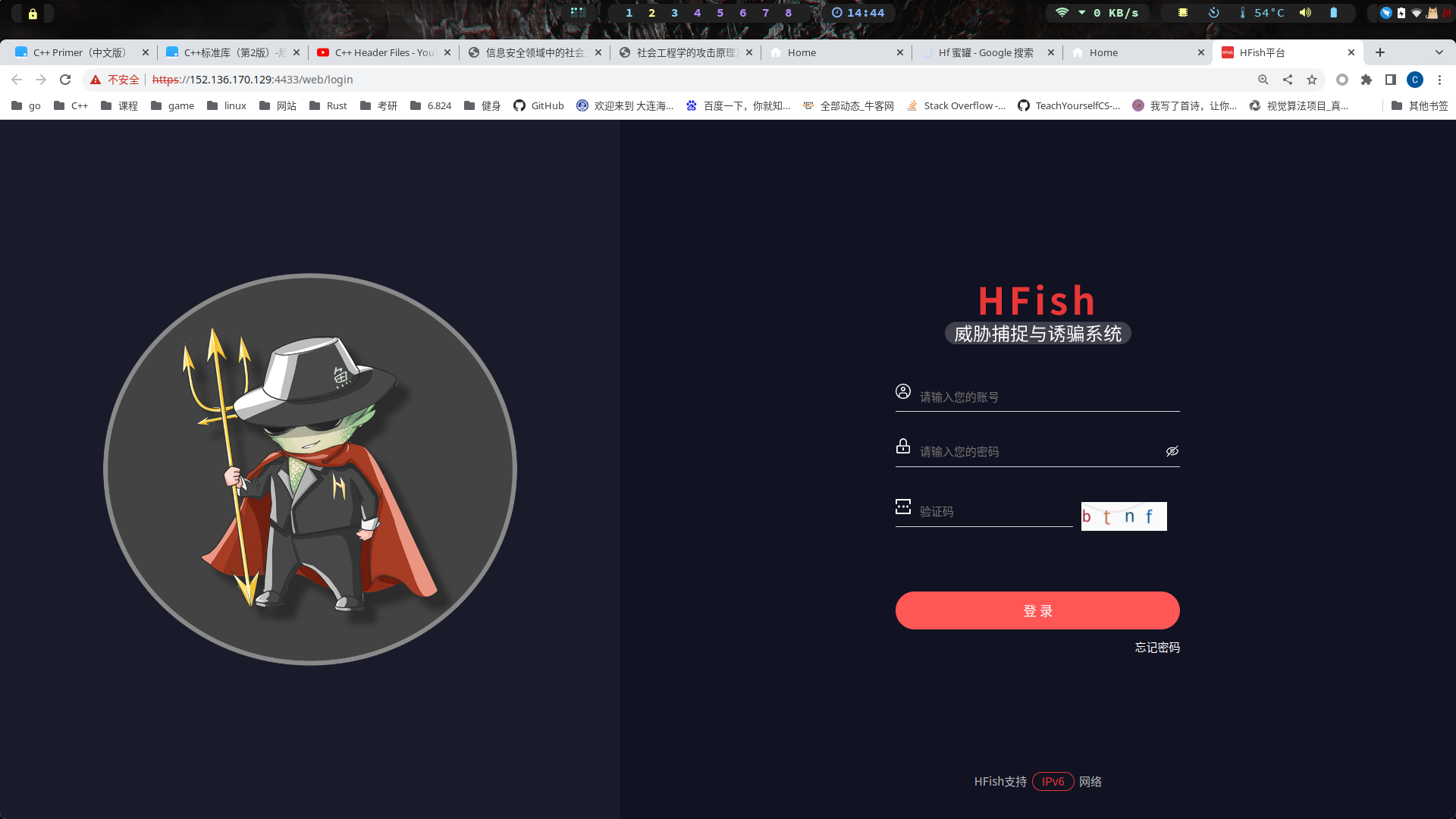
containrrr/watchtower \

--cleanup \

hfish \

--interval 3600

可以通过登陆地址：**[https://ip:4433/web/](https://ip:4433/web/" \t "/home/chikai/Documents\\x/_blank)** 登陆

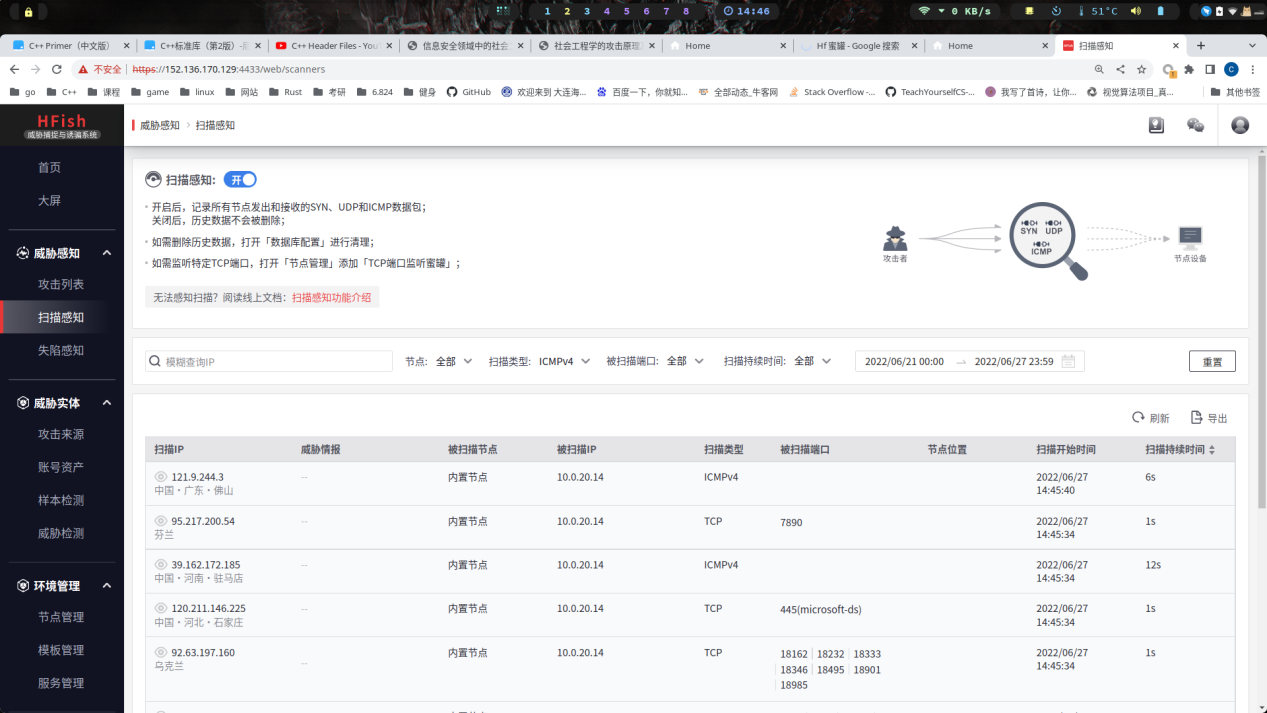
****

1. **模拟攻击**

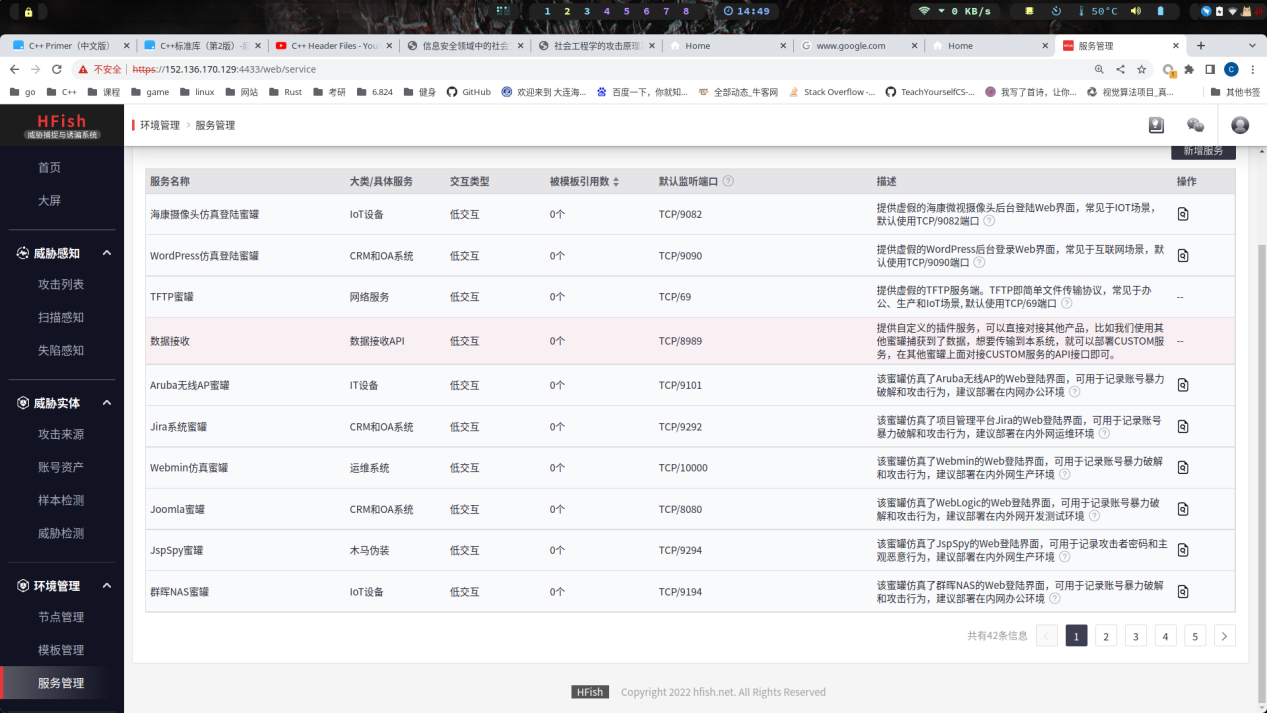
**通过终端向服务器发送ping命令:**

****

**在扫描感知中，可以查询到攻击信息**

****

**此外，我们还可以在系统中使用其他蜜罐模板:**

****

**【结果分析】**

**相比于MNH蜜罐，HFish 更易于搭建。而且HFish更现代化，易于配置。**

**【个人总结&心得体会】**

**通过搭建HFIsh蜜罐环境，我不仅了解了蜜罐的功能和用途，而且进一步学会了蜜罐的详细配置和docker的使用。**