一、蜜罐

1. 什么是蜜罐

蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

(1) 开源蜜罐搭建与使用

> 开源的蜜罐非常多，如 hifish 、decoymini 、EHoney等，使用流程与厂商蜜罐产品差距不大。

(2) hifish

A. 基本信息

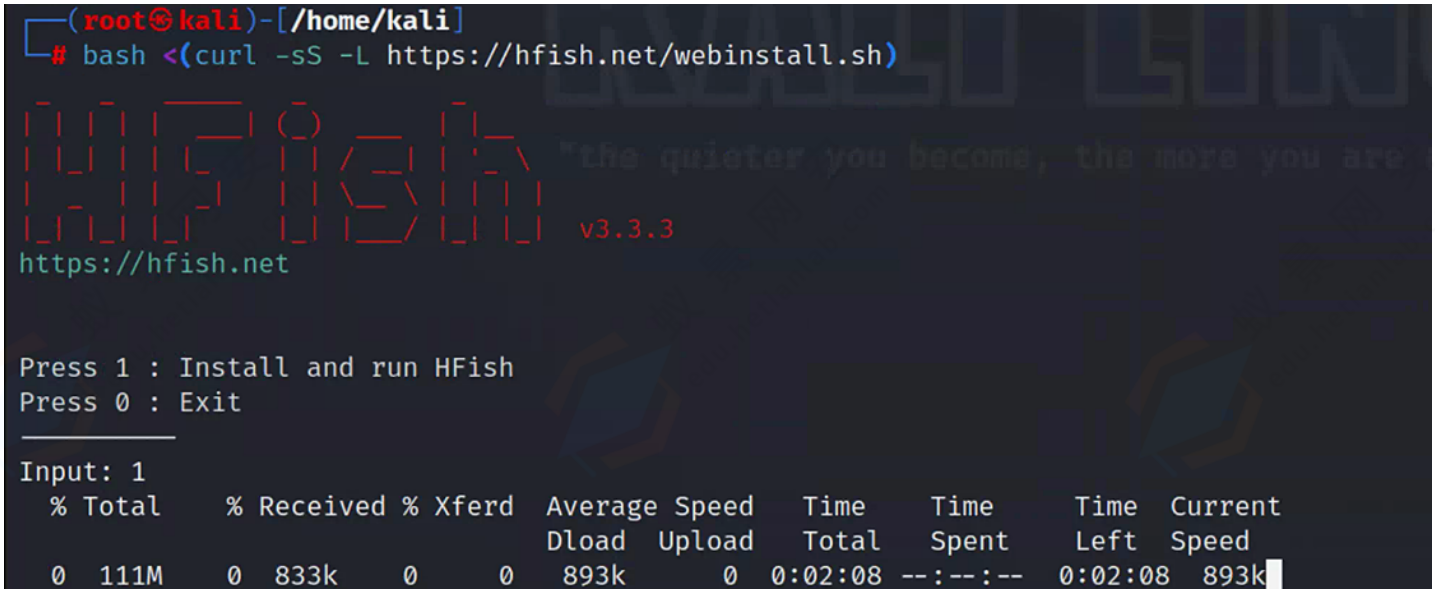
- 官网：https://hfish.net/
- 简介：HFish是一款社区型免费蜜罐，侧重企业安全场景，从内网失陷检测、外网威胁感知、威胁情报生产三个场景出发，为用户提供可独立操作且实用的功能，通过安全、敏捷、可靠的中低交互蜜罐增加用户在失陷感知和威胁情报领域的能力。HFish具有超过40种蜜罐环境、提供免费的云蜜网、可高度自定义的蜜饵能力、一键部署、跨平台多架构、国产操作系统和CPU支持、极低的性能要求、邮件/syslog/webhook/企业微信/钉钉/飞书告警等多项特性，帮助用户降低运维成本，提升运营效率。

B. 安装

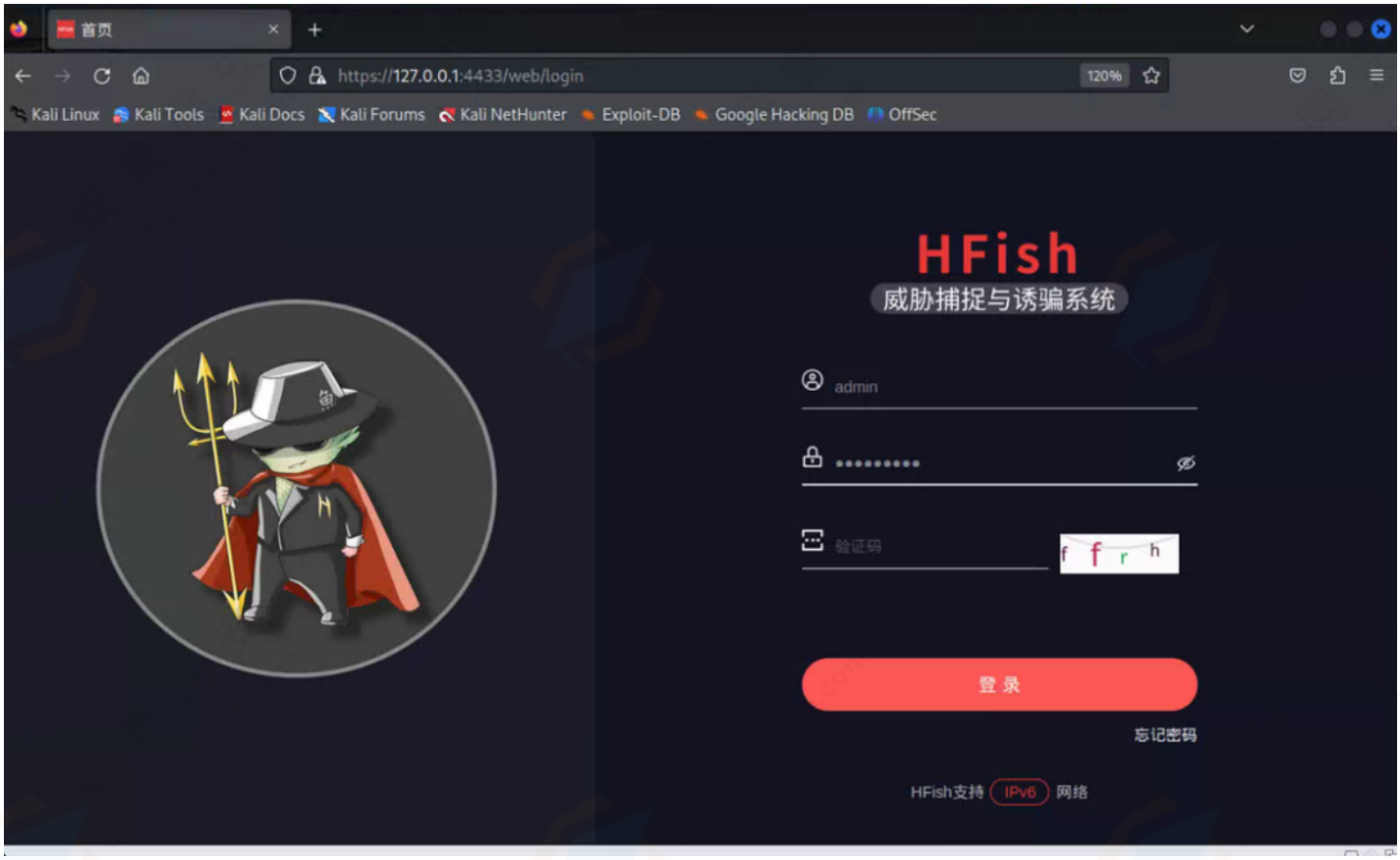
> 这里以Kali Linux作为示例

1. 下载和安装hifish

```
bash <(curl -sS -L https://hfish.net/webinstall.sh)
```



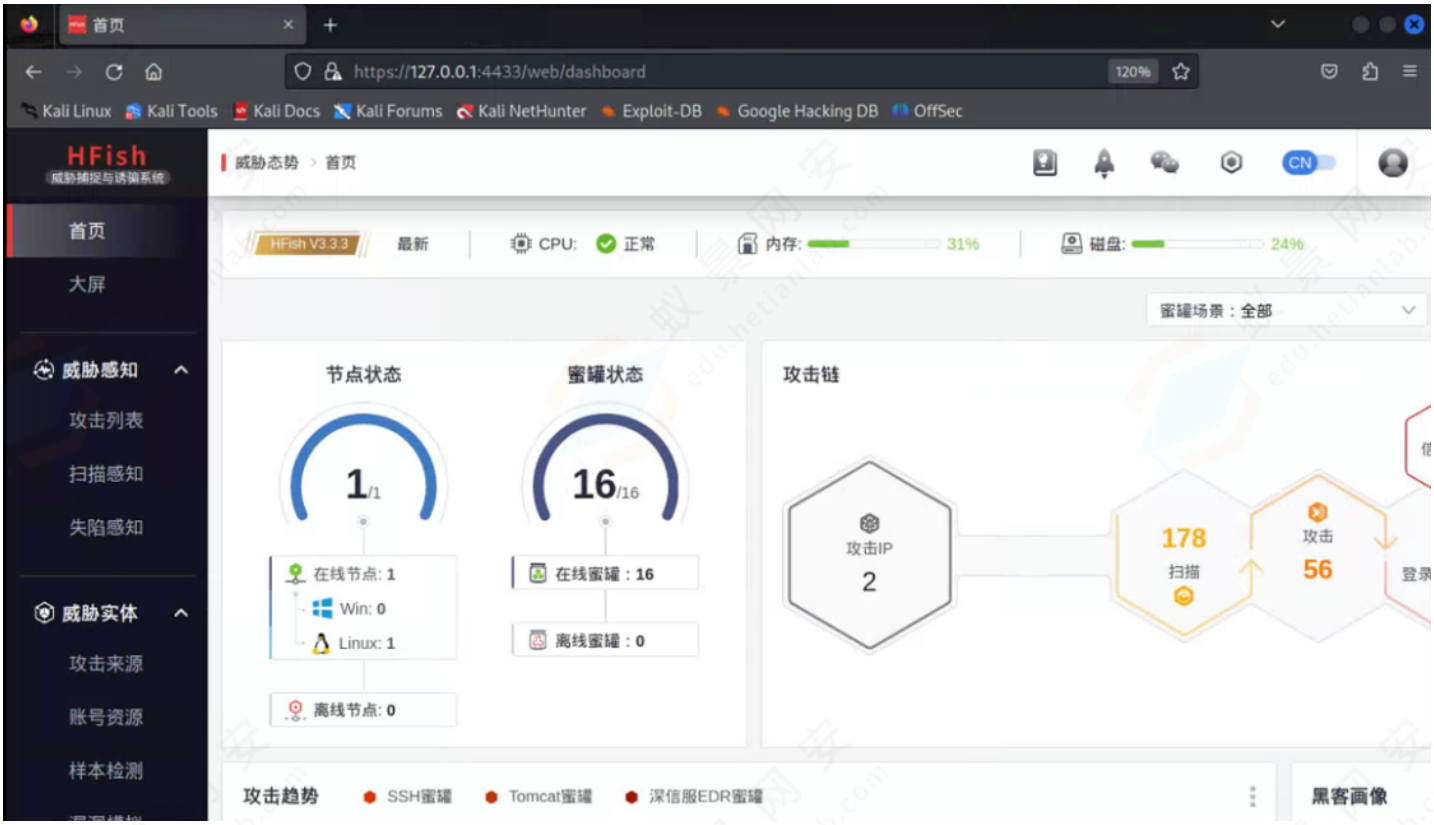
2. 打开https访问 https://127.0.0.1:4433/web 账号：admin 密码：HFish2021



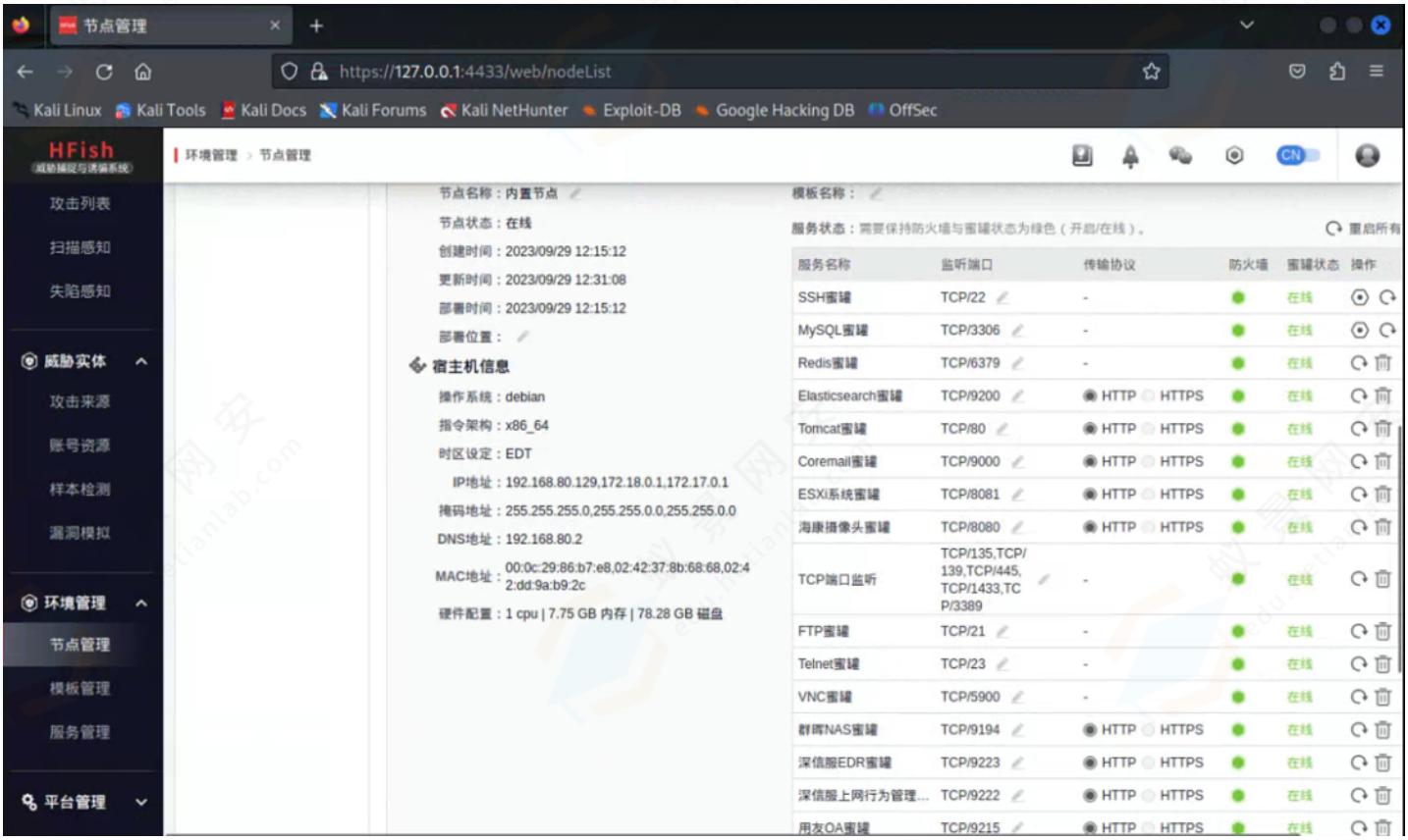
C. 使用

1) 常用功能

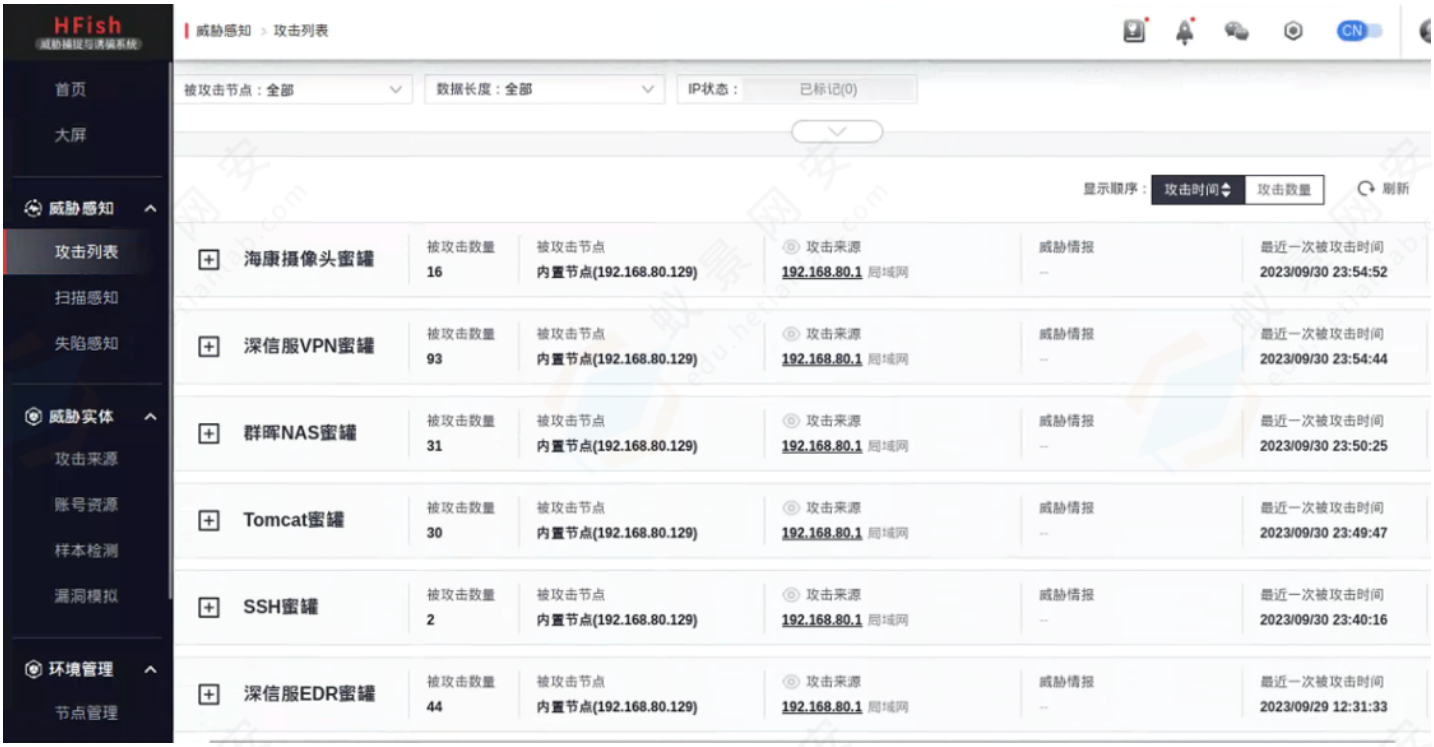
1. 首页


首页
https://127.0.0.1:4433/web/dashboard
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HFish
威胁捕捉与诱骗系统
威胁态势 › 首页
首页
大屏
威胁感知
攻击列表
扫描感知
失陷感知
威胁实体
攻击来源
账号资源
样本检测
HFish V3.3.3
最新
CPU: 正常
内存: 31%
磁盘: 24%
蜜罐场景：全部
节点状态
蜜罐状态
攻击链
1/1
16/16
在线节点: 1
Win: 0
Linux: 1
离线节点: 0
在线蜜罐：16
离线蜜罐：0
攻击IP
2
178
扫描
攻击
56
攻击趋势
SSH蜜罐
Tomcat蜜罐
深信服EDR蜜罐
黑客画像

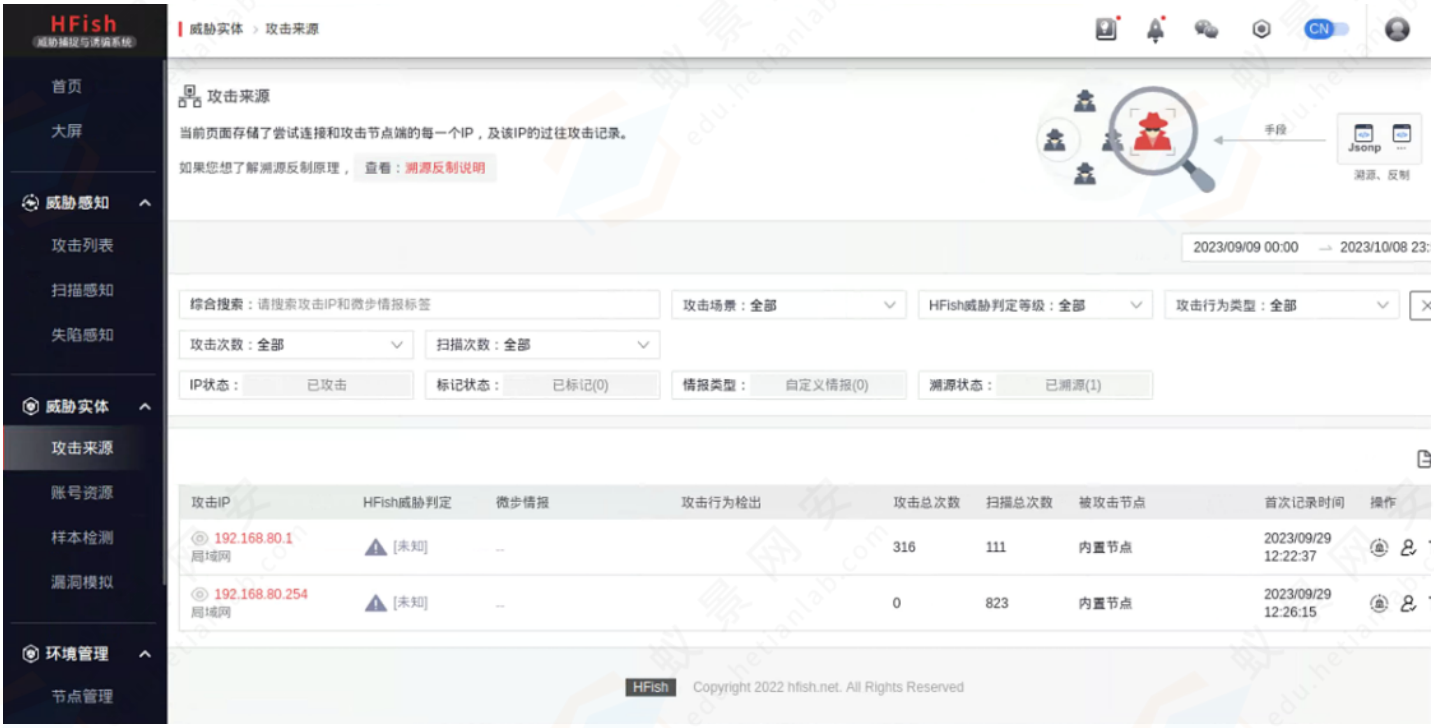
2. 节点管理


节点管理
https://127.0.0.1:4433/web/nodeList
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HFish
环境管理 › 节点管理
攻击列表
扫描感知
失陷感知
威胁实体
攻击来源
账号资源
样本检测
漏洞模拟
环境管理
节点管理
模板管理
服务管理
平台管理
节点名称：内置节点
节点状态：在线
创建时间：2023/09/29 12:15:12
更新时间：2023/09/29 12:31:08
部署时间：2023/09/29 12:15:12
部署位置：
宿主机信息
操作系统：debian
指令架构：x86_64
时区设定：EDT
IP地址：192.168.80.129,172.18.0.1,172.17.0.1
掩码地址：255.255.255.0,255.255.0.0,255.255.0.0
DNS地址：192.168.80.2
MAC地址：00:0c:29:86:b7:e8,02:42:37:8b:68:68,02:42:dd:9a:b9:2c
硬件配置：1 cpu | 7.75 GB 内存 | 78.28 GB 磁盘
模板名称：
服务状态：需要保持防火墙与蜜罐状态为绿色（开启/在线）。
重启所有
服务名称
监听端口
传输协议
防火墙
蜜罐状态
操作
SSH蜜罐 TCP/22
MySQL蜜罐 TCP/3306
Redis蜜罐 TCP/6379
Elasticsearch蜜罐 TCP/9200
Tomcat蜜罐 TCP/80
Coremail蜜罐 TCP/9000
ESXi系统蜜罐 TCP/8081
海康摄像头蜜罐 TCP/8080
TCP端口监听 TCP/135,TCP/139,TCP/445,TCP/1433,TCP/3389
FTP蜜罐 TCP/21
Telnet蜜罐 TCP/23
VNC蜜罐 TCP/5900
群晖NAS蜜罐 TCP/9194
深信服EDR蜜罐 TCP/9223
深信服上网行为管理... TCP/9222
用友OA蜜罐 TCP/9215
HTTP HTTPS
在线

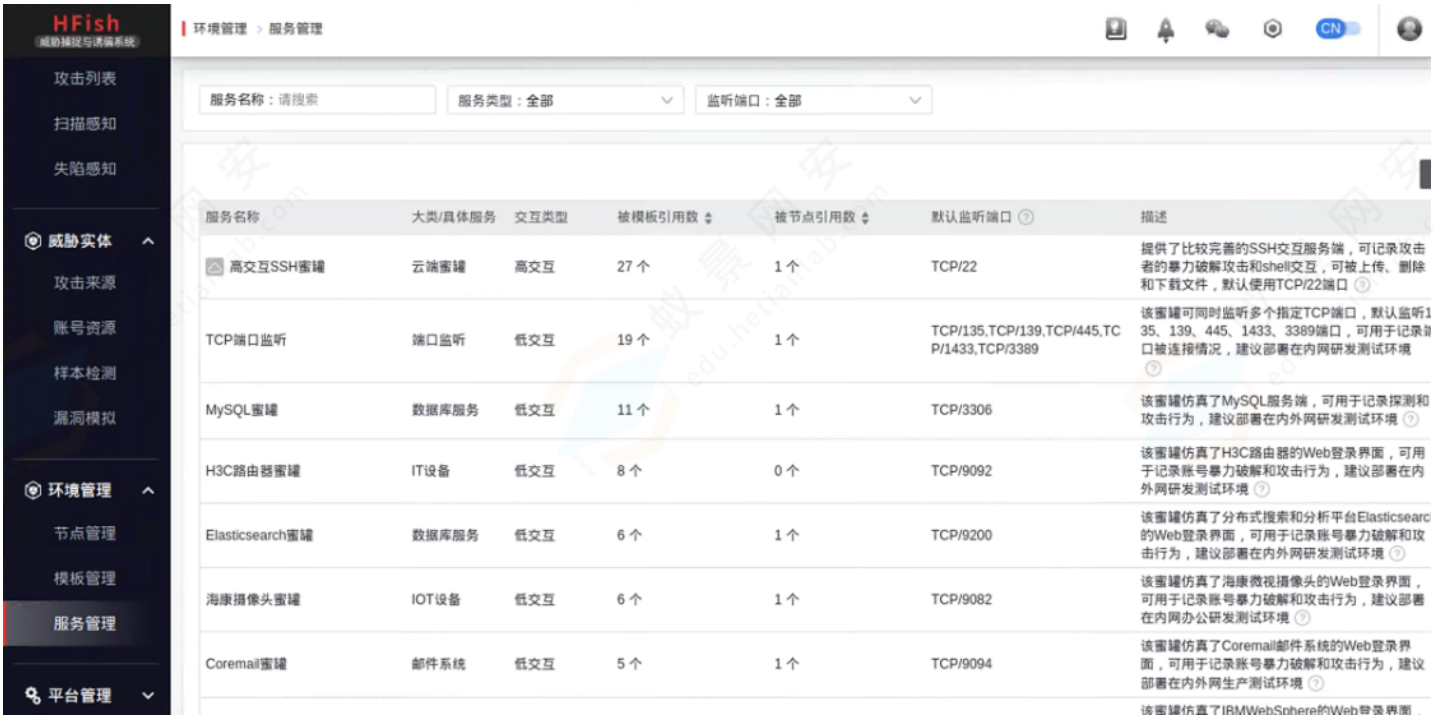
3. 攻击列表


HFish
威胁捕捉与诱骗系统
威胁感知 › 攻击列表
首页
大屏
威胁感知
攻击列表
扫描感知
失陷感知
威胁实体
攻击来源
账号资源
样本检测
漏洞模拟
环境管理
节点管理
被攻击节点：全部
数据长度：全部
IP状态：
已标记(0)
显示顺序：
攻击时间
攻击数量
刷新
海康摄像头蜜罐
被攻击数量 16
被攻击节点 内置节点(192.168.80.129)
攻击来源 192.168.80.1 局域网
威胁情报 --
最近一次被攻击时间 2023/09/30 23:54:52
深信服VPN蜜罐
被攻击数量 93
被攻击节点 内置节点(192.168.80.129)
攻击来源 192.168.80.1 局域网
威胁情报 --
最近一次被攻击时间 2023/09/30 23:54:44
群晖NAS蜜罐
被攻击数量 31
被攻击节点 内置节点(192.168.80.129)
攻击来源 192.168.80.1 局域网
威胁情报 --
最近一次被攻击时间 2023/09/30 23:50:25
Tomcat蜜罐
被攻击数量 30
被攻击节点 内置节点(192.168.80.129)
攻击来源 192.168.80.1 局域网
威胁情报 --
最近一次被攻击时间 2023/09/30 23:49:47
SSH蜜罐
被攻击数量 2
被攻击节点 内置节点(192.168.80.129)
攻击来源 192.168.80.1 局域网
威胁情报 --
最近一次被攻击时间 2023/09/30 23:40:16
深信服EDR蜜罐
被攻击数量 44
被攻击节点 内置节点(192.168.80.129)
攻击来源 192.168.80.1 局域网
威胁情报 --
最近一次被攻击时间 2023/09/29 12:31:33

4. 攻击来源


HFish
威胁捕捉与诱骗系统
威胁实体 › 攻击来源
首页
大屏
威胁感知
攻击列表
扫描感知
失陷感知
威胁实体
攻击来源
账号资源
样本检测
漏洞模拟
环境管理
节点管理
攻击来源
当前页面存储了尝试连接和攻击节点端的每一个IP，及该IP的过往攻击记录。
如果您想了解溯源反制原理，
查看：溯源反制说明
手段
Jsonp
溯源、反制
2023/09/09 00:00
综合搜索：请搜索攻击IP和微步情报标签
攻击场景：全部
HFish威胁判定等级：全部
攻击行为类型：全部
攻击次数：全部
扫描次数：全部
IP状态：
已攻击
标记状态：
已标记(0)
情报类型：
自定义情报(0)
溯源状态：
已溯源(1)
攻击IP
HFish威胁判定
微步情报
攻击行为检出
攻击总次数
扫描总次数
被攻击节点
首次记录时间
操作
192.168.80.1
局域网
[未知]
316
111
内置节点
2023/09/29 12:22:37
192.168.80.254
局域网
[未知]
0
823
内置节点
2023/09/29 12:26:15
HFish
Copyright 2022 hfish.net. All Rights Reserved

5. 服务管理



2) 漏洞模拟

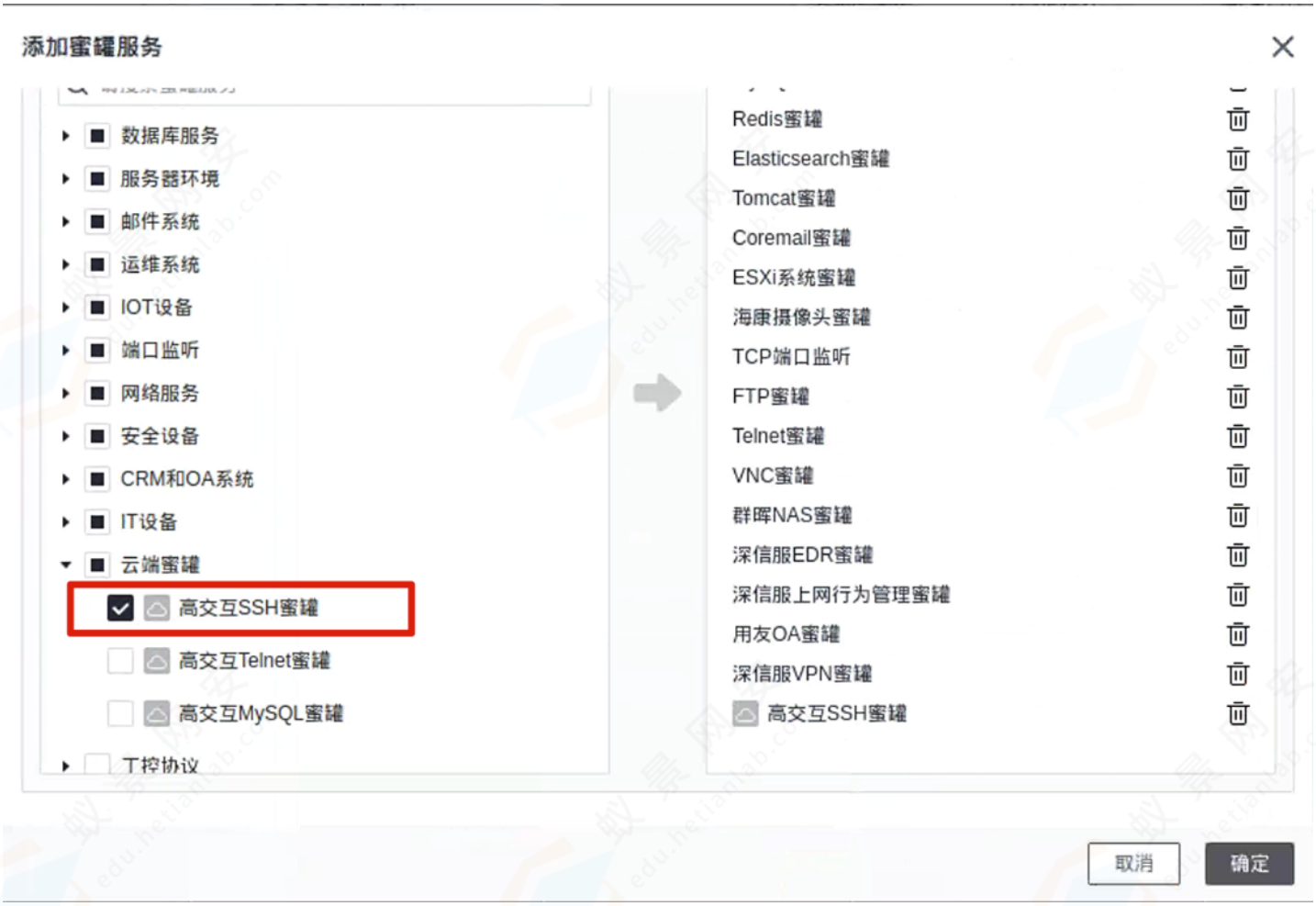
如果请求时参数或请求体被漏洞模拟中预设的指纹匹配到，就会记录其攻击行为
如访问参数中包含 ${jndi:ldap:/ 就会被记录log4j远程命令执行漏洞

请求类型	请求详情(url)	状态	数据长度	攻击行为	攻击详情
GET	/login?a=${jndi:ldap:/	404，请求地址未找到	829(字节)	高危 Log4j远程命令执行3（CVE-2021-442... +1	
GET	/login?a=${jndi:ldap:/	404，请求地址未找到	829(字节)	高危 Log4j远程命令执行3（CVE-2021-442... +1	
GET	/login?a=${jndi:ldap:/	404，请求地址未找到	799(字节)	高危 Log4j远程命令执行2（CVE-2021-442... +1	
GET	/favicon.ico	404，请求地址未找到	745(字节)		

规则名称	规则类型	严重级别	命中记录	最近一次命中时间	创建用户	状态
Log4j远程命令执行3（CVE-2021-44228）	行为检测-内置	[高危]	3	2023/10/08 02:46:09	admin	
Log4j远程命令执行2（CVE-2021-44228）	行为检测-内置	[高危]	3	2023/10/08 02:46:09	admin	
Log4j远程命令执行1（CVE-2021-44228）	行为检测-内置	[高危]	0	--	admin	
疑似 Fastjson 攻击	行为检测-内置	[高危]	0	--	admin	
Java Applet JMX远程代码执行（CVE-2013-0422）	行为检测-内置	[高危]	0	--	admin	

3) 高交互蜜罐

高交互ssh蜜罐用户及密码：root/123456
高交互蜜罐故名思议，如高交互ssh蜜罐，可以登录、执行命令、上传文件，功能很多，不易让黑客察觉，能够充分记录攻击者行为。如果是普通的ssh蜜罐，只会一直登陆错误，仅能记录黑客的攻击ip和爆破ssh时使用的用户及密码字典。
hifish的高交互ssh蜜罐，是hifish自已运营的云端蜜罐



D. 关闭

结束hfish和hfish-server的进程

```
root@HFish~# ps ax | grep ./hfish | grep -v grep
8435 ?        Sl    97:59 ./hfish
8436 ?        Sl    97:59 ./hfish-server

root@HFish:~# kill -9 8435
root@HFish:~# kill -9 8436
```