群友靶机-Ahiz

信息搜集

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 03:49 EDT
Nmap scan report for bogon (192.168.1.106)
Host is up (0.00011s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:85:9E:D7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

web探测

提示密码分成了好多串，猜测是需要扫一下目录

猜测welcome为用户名称，可以尝试进行ssh登陆

扫目录

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.1.106 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -r  -x php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.106
[+] Method:                  GET
[+] Threads:                 10
```

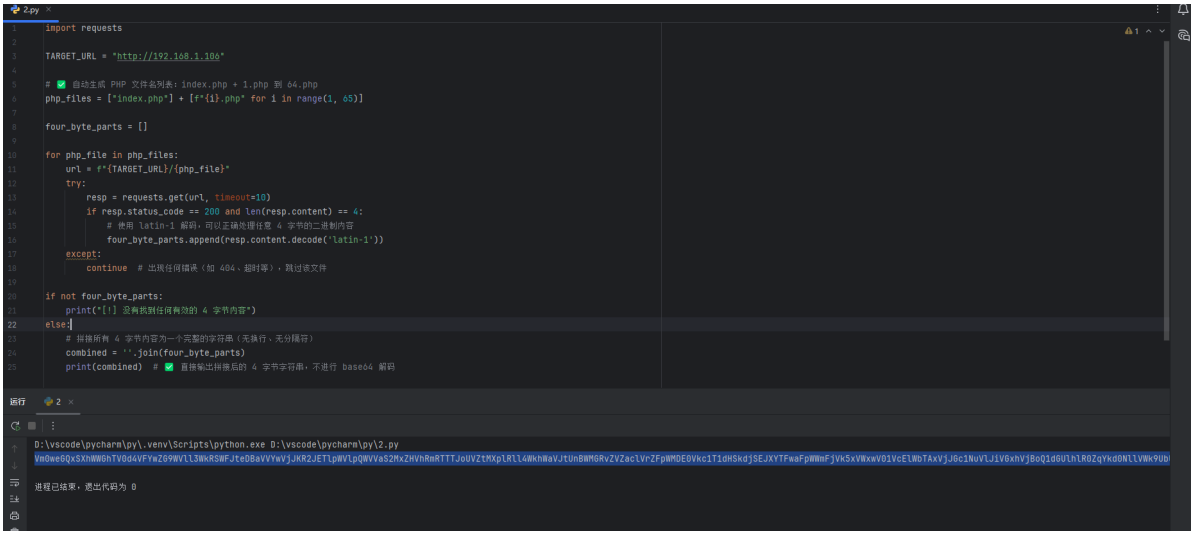
```
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/12.php               (Status: 200) [Size: 4]
/10.php               (Status: 200) [Size: 4]
/11.php               (Status: 200) [Size: 4]
/1.php                (Status: 200) [Size: 4]
/3.php                (Status: 200) [Size: 4]
/13.php               (Status: 200) [Size: 4]
/4.php                (Status: 200) [Size: 4]
/14.php               (Status: 200) [Size: 4]
/16.php               (Status: 200) [Size: 4]
/2.php                (Status: 200) [Size: 4]
/18.php               (Status: 200) [Size: 4]
/20.php               (Status: 200) [Size: 4]
/5.php                (Status: 200) [Size: 4]
/21.php               (Status: 200) [Size: 4]
/22.php               (Status: 200) [Size: 4]
/6.php                (Status: 200) [Size: 4]
/19.php               (Status: 200) [Size: 4]
/24.php               (Status: 200) [Size: 4]
/23.php               (Status: 200) [Size: 4]
/15.php               (Status: 200) [Size: 4]
/27.php               (Status: 200) [Size: 4]
/26.php               (Status: 200) [Size: 4]
/17.php               (Status: 200) [Size: 4]
/9.php                (Status: 200) [Size: 4]
/30.php               (Status: 200) [Size: 4]
/28.php               (Status: 200) [Size: 4]
/29.php               (Status: 200) [Size: 4]
/7.php                (Status: 200) [Size: 4]
/25.php               (Status: 200) [Size: 4]
/8.php                (Status: 200) [Size: 4]
/31.php               (Status: 200) [Size: 4]
/32.php               (Status: 200) [Size: 4]
/36.php               (Status: 200) [Size: 4]
/40.php               (Status: 200) [Size: 4]
/33.php               (Status: 200) [Size: 4]
/35.php               (Status: 200) [Size: 4]
/37.php               (Status: 200) [Size: 4]
/39.php               (Status: 200) [Size: 4]
/34.php               (Status: 200) [Size: 4]
/42.php               (Status: 200) [Size: 4]
/41.php               (Status: 200) [Size: 4]
/48.php               (Status: 200) [Size: 4]
/50.php               (Status: 200) [Size: 4]
/38.php               (Status: 200) [Size: 4]
/47.php               (Status: 200) [Size: 4]
/43.php               (Status: 200) [Size: 4]
/45.php               (Status: 200) [Size: 4]
/44.php               (Status: 200) [Size: 4]
```

```
/51.php               (Status: 200) [Size: 4]
/46.php               (Status: 200) [Size: 4]
/49.php               (Status: 200) [Size: 4]
/55.php               (Status: 200) [Size: 4]
/59.php               (Status: 200) [Size: 4]
/60.php               (Status: 200) [Size: 4]
/54.php               (Status: 200) [Size: 4]
/53.php               (Status: 200) [Size: 4]
/57.php               (Status: 200) [Size: 4]
/61.php               (Status: 200) [Size: 4]
/52.php               (Status: 200) [Size: 4]
/63.php               (Status: 200) [Size: 4]
/56.php               (Status: 200) [Size: 4]
/64.php               (Status: 200) [Size: 4]
/58.php               (Status: 200) [Size: 4]
/62.php               (Status: 200) [Size: 4]
```

这里可以看到有很多个php文件，并且size是 4 bytes，并且一个一个打开后是4个字符串，猜测是需要把这些php文件内字符串输出了

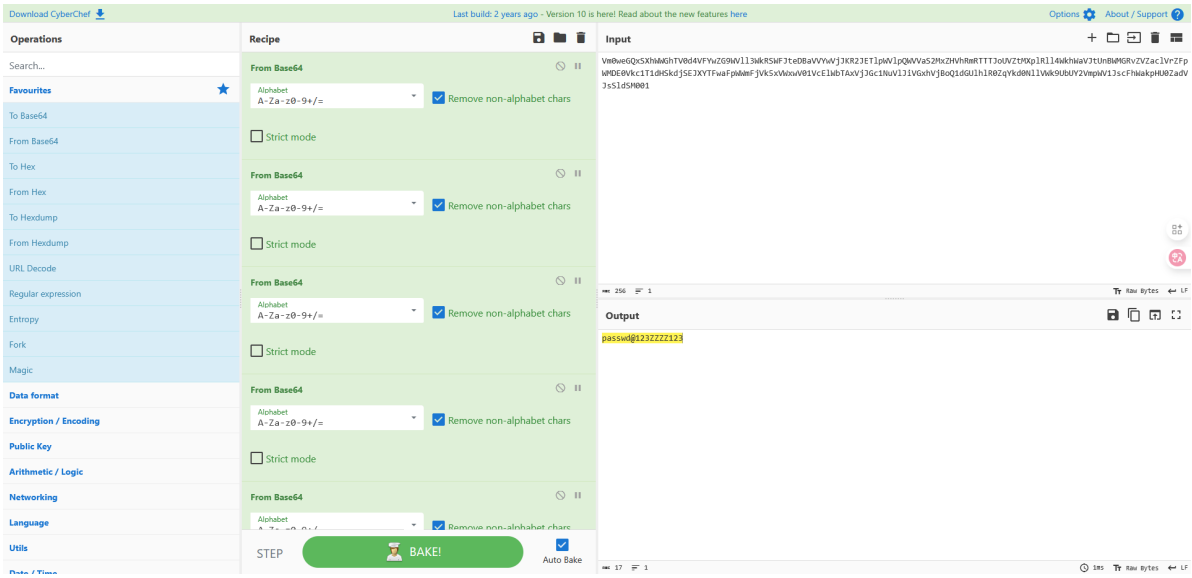
那么写一个脚本对靶机ip内的php文件进行请求，并且将请求到的内容合并输出

```
import requests

TARGET_URL = "http://192.168.1.106"

# ☑ 自动生成 PHP 文件名列表：index.php + 1.php 到 64.php
php_files = ["index.php"] + [f"{i}.php" for i in range(1, 65)]

four_byte_parts = []

for php_file in php_files:
    url = f"{TARGET_URL}/{php_file}"
    try:
        resp = requests.get(url, timeout=10)
        if resp.status_code == 200 and len(resp.content) == 4:
            # 使用 latin-1 解码，可以正确处理任意 4 字节的二进制内容
            four_byte_parts.append(resp.content.decode('latin-1'))
    except:
        continue  # 出现任何错误（如 404、超时等），跳过该文件

if not four_byte_parts:
    print("[!] 没有找到任何有效的 4 字节内容")
else:
    # 拼接所有 4 字节内容为一个完整的字符串（无换行、无分隔符）
    combined = ''.join(four_byte_parts)
    print(combined)  # ☑ 直接输出拼接后的 4 字节字符串，不进行 base64 解码
```



得到了一长串的字符串，用厨子进行解码

多层base64加密



得到了密码passwd@123ZZZZ123

拿去登陆

ssh登陆

```
┌──(root㉿kali)-[/home/kali]
└─# ssh welcome@192.168.1.106
welcome@192.168.1.106's password:
Linux Ahiz 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Sep  7 03:06:11 2025 from 192.168.1.101
welcome@Ahiz:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

在welcome用户的家目录下看见了一个程序**1**

```
welcome@Ahiz:~$ file 1
1: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked,
interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0,
BuildID[sha1]=81544629ae0a32249a48b0bc5134fb7b1455adea, stripped
```

是一个 64 位的 Linux 可执行程序,尝试运行一下

```
welcome@Ahiz:~$ ./1
Usage: ./1 <string>大于密码长度
welcome@Ahiz:~$ ./1 123123123
❌ Input too short, try again.
```

输入什么东西都提示输入的内容太短，尝试使用命令，使其可以生成一个足够长的字符串，并且将字符串作为程序的输入参数，绕过长度检测

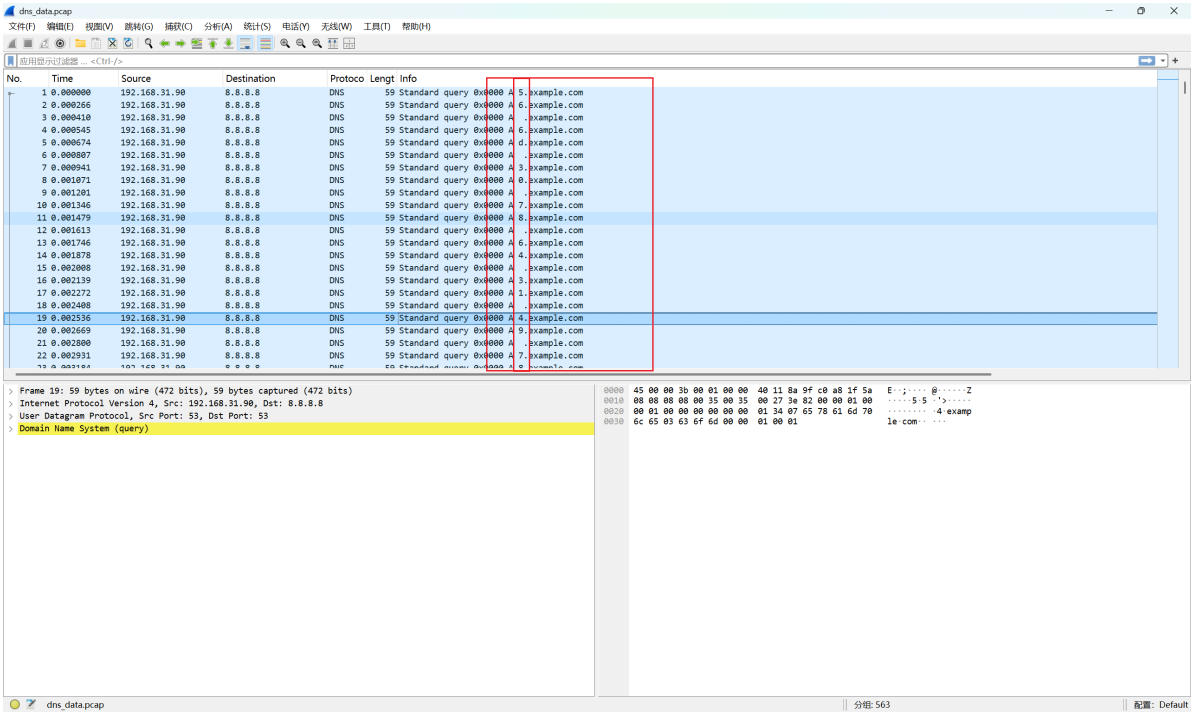
```
welcome@Ahiz:~$ ./1 "$(yes A | head -n 1000 | tr -d '\n')"
☑ Good job! Here is your flag:
user_FLAG{this_is_a_safe_demo_flag}
```

提取

看一下有没有提权的东西

```
welcome@Ahiz:~$ sudo find / -type f -exec getcap {} 2>/dev/null \;
welcome@Ahiz:~$ sudo -l
-bash: /usr/bin/sudo: Permission denied
welcome@Ahiz:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
welcome@Ahiz:~$ sudo find / -type f -exec getcap {} 2>/dev/null \;
```

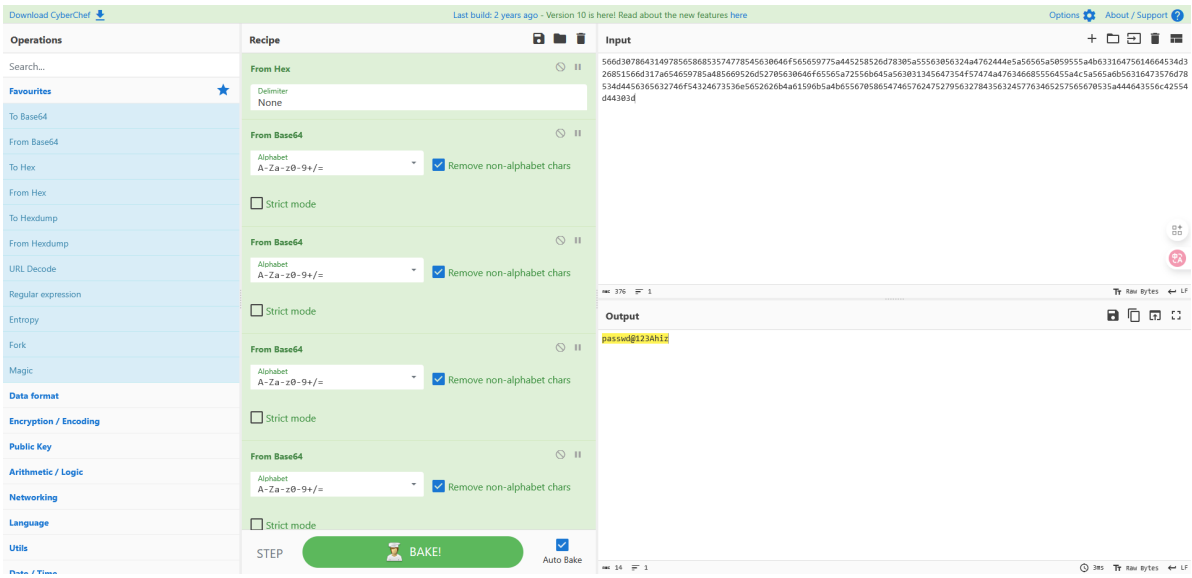
并没有找到提权的方案，并且在/opt下找到了一个dns_data.pacp的流量包，拿到本地用wireshark看一下



可以看到除了`.example.com`之前的内容不同，其他内容大差不差，并且子域名都是十六进制的字符串，那么就尝试提取`.example.com`之前的十六进制内容

```
┌──(kali㉿kali)-[~/aaa]
└─$ tshark -r dns_data.pcap -Y "dns.qry.type==1" -T fields -e dns.qry.name | awk -F. '$1~/^[0-9a-zA-Z]/{printf $1}'
566d3078643149785658685357477854563064 6f565659775a445258526d78305a55563056324a4762444e5a56565a5059555a4b6331647561466453 4d326851566d317a654659785a485669526d52705630646f65565a72556b645a5630313456474 7354f57474a476346685556455a4c5a565a6b56316473576d78534d4456365632746f54324673536e5652626b4a61596b5a4b6556705865474657627 5279563278435632457763465257565670535a444643556c42554d44303d
```

解码发现是一层hex，剩下的都是base64



猜测是root密码，进行切换

```
welcome@Ahiz:~$ su
Password:
root@Ahiz:/home/welcome# id
uid=0(root) gid=0(root) groups=0(root)
```

flag

```
welcome@Ahiz:~$ ./1 "$(yes A | head -n 1000 | tr -d '\n')"
☑ Good job! Here is your flag:
user_FLAG{this_is_a_safe_demo_flag}
root@Ahiz:~# cat root.txt
flag{root}
```