Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: Cơ chế hoạt động của mã độc

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Simple botnet

GV: Nghi Hoàng Khoa

Ngày báo cáo: 10/4/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Bùi Kim Ngân	20520648	20520648@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Yêu cầu 1	100%	Ngân
2	Yêu cầu 2	100%	Ngân
3	Yêu cầu 3	100%	Ngân
4	Yêu cầu 4	100%	Ngân

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

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

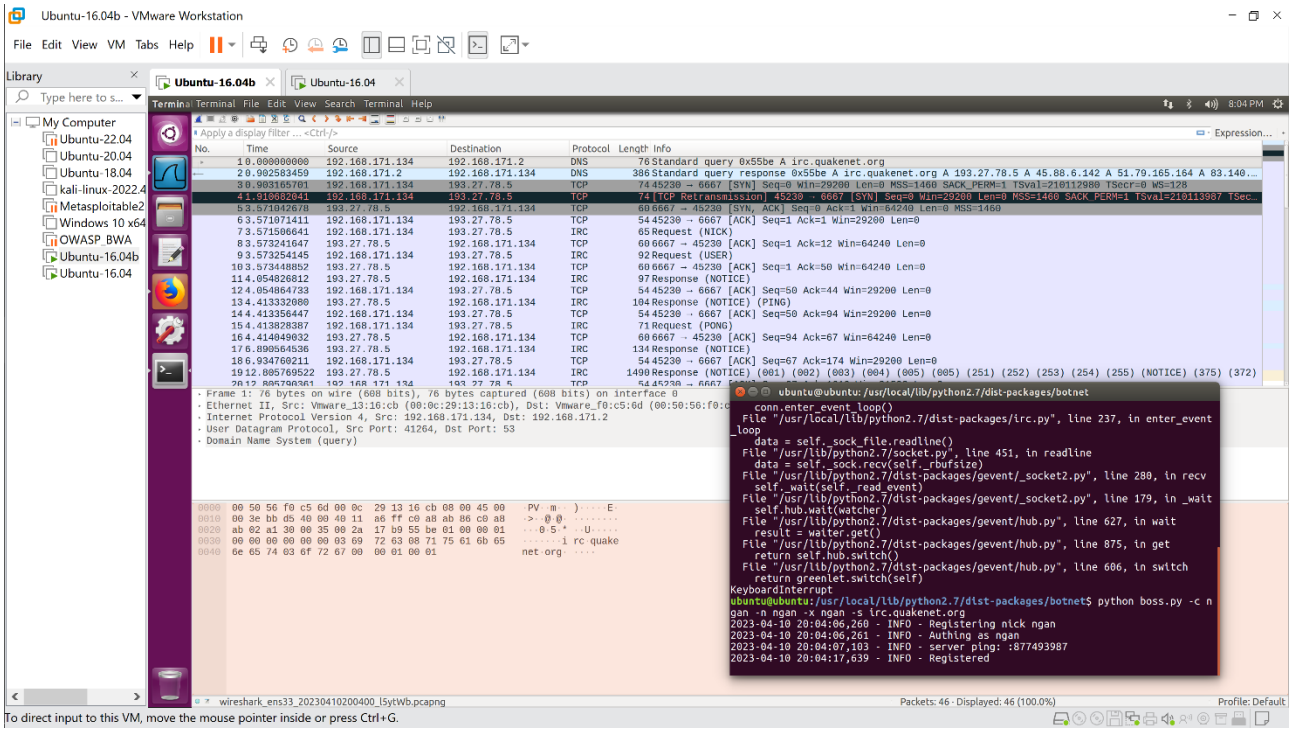
1. Yêu cầu 1: Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.

Tại máy ubuntu 16.04 làm boss, khởi động Wireshark tiến hành bắt gói tin, chạy các dòng lệnh dưới

cd /usr/local/lib/python2.7/dist-packages/botnet

python boss.py -c ngan -n ngan -x ngan -s irc.quakenet.org

Quá trình kết nối của botmaster với irc.quakenet.org theo các gói tin wireshark bắt được như hình dưới

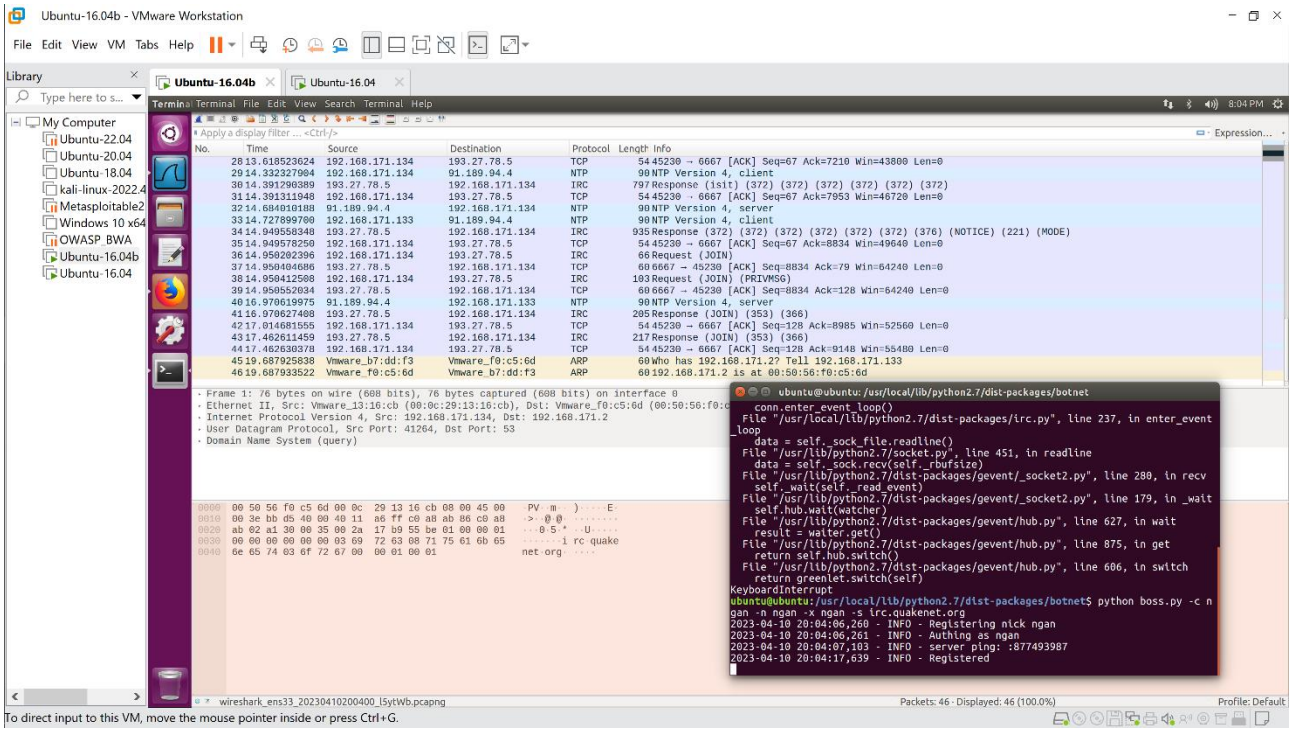


Đầu tiên, gói DNS sẽ được gửi để phân giải tên miền irc.quakenet.org thành IP.

Sau đó thực hiện bắt tay 3 bước TCP, các gói SYN, SYN ACK, ACK lần lượt được gửi qua lại

Các gói request NICK, USER được gửi đi từ máy 192.168.171.134 qua protocol IRC để tiến hành đăng ký lên server

Kế đó, các gói PING PONG được gửi qua lại để kiểm tra kết nối



Khi đăng ký thành công, thấy rằng có các request JOIN, để boss kết nối đến server và mở channel

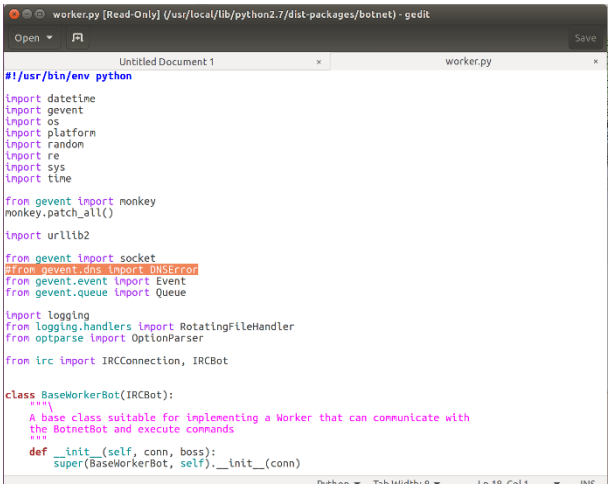
2. **Yêu cầu 2: Từ kết quả wireshark thu thập được. Hãy phân tích quá trình gì đang diễn ra.**
3. **Yêu cầu 4: Tiếp tục những gì đang thực hiện tại C.1, bạn hãy mở rộng mạng Botnet với 2 bots.**

Tại máy ubuntu 16.04 làm worker, khởi động wireshark và thực hiện các câu lệnh sau.

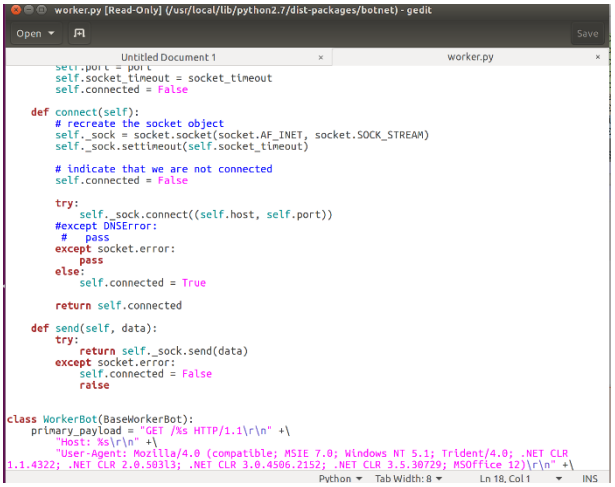
cd /usr/local/lib/python2.7/dist-packages/botnet

gedit worker.py

Tại đây ta cần chỉnh sửa lại đoạn worker.py



Thêm # vào trước DNSError

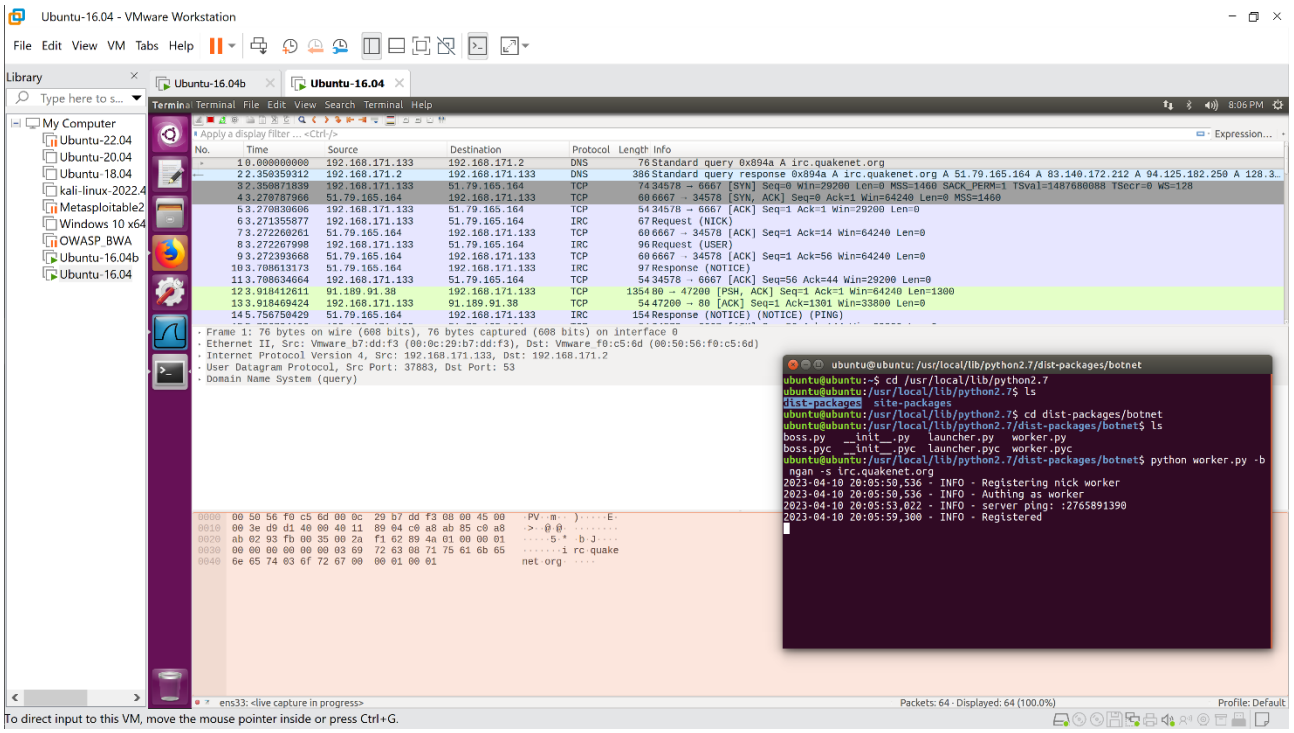


Thêm # vào except DNSError và dòng pass ngay dưới

Chạy worker 1

python worker.py -b ngan -s irc.quakenet.org

Kết quả bắt gói tin như hình dưới

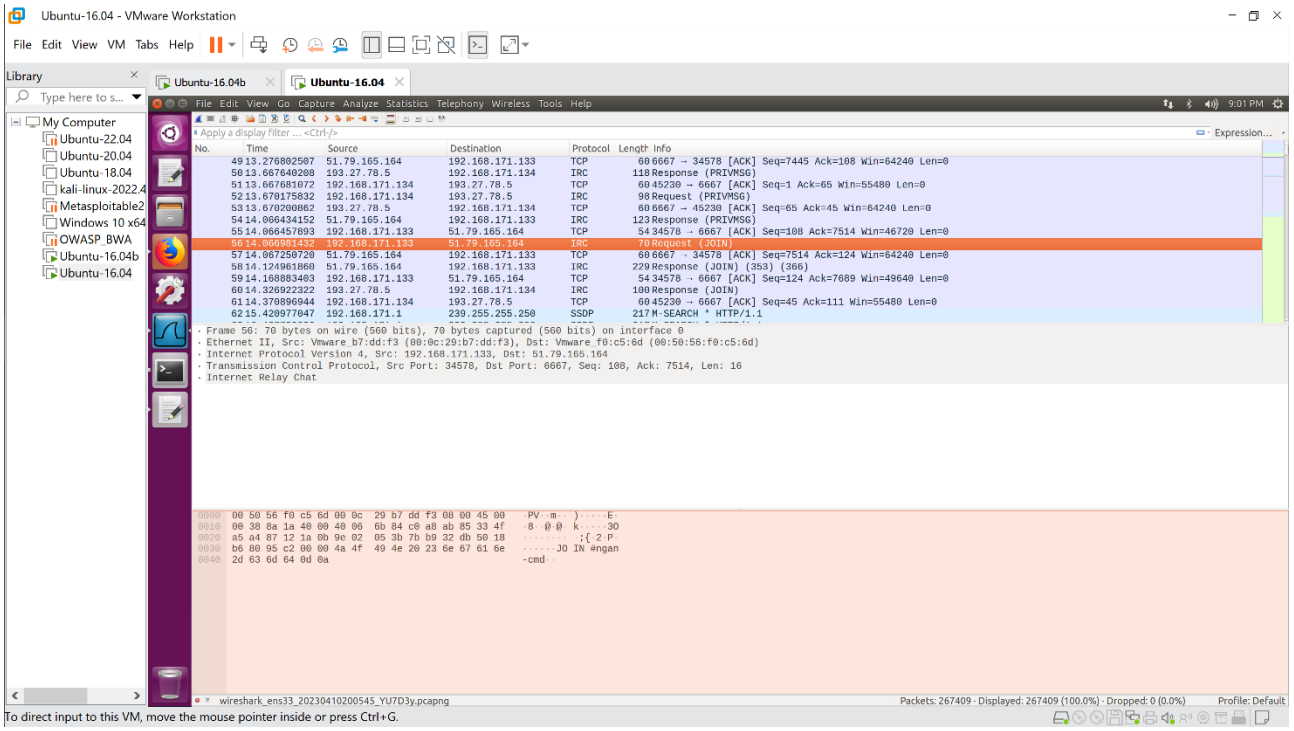


Tương tự boss, Gói tin DNS để phân giải tên miền irc.quakenet.org được gửi đầu tiên

Sau đó, gửi các gói TCP thực hiện quá trình bắt tay 3 bước

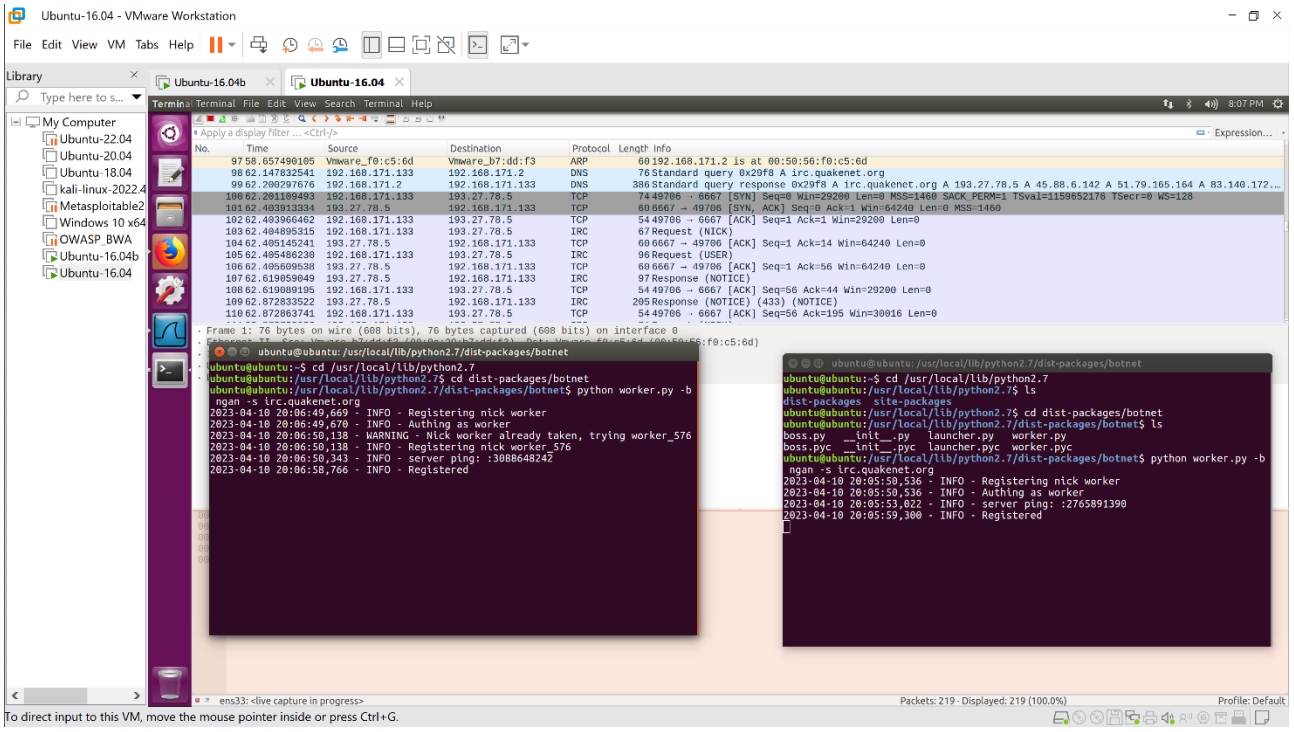
Các gói request NICK, USER được gửi đi từ máy 192.168.171.134 qua protocol IRC để tiến hành đăng ký

Kế đó, các gói PING PONG được gửi qua lại để kiểm tra kết nối



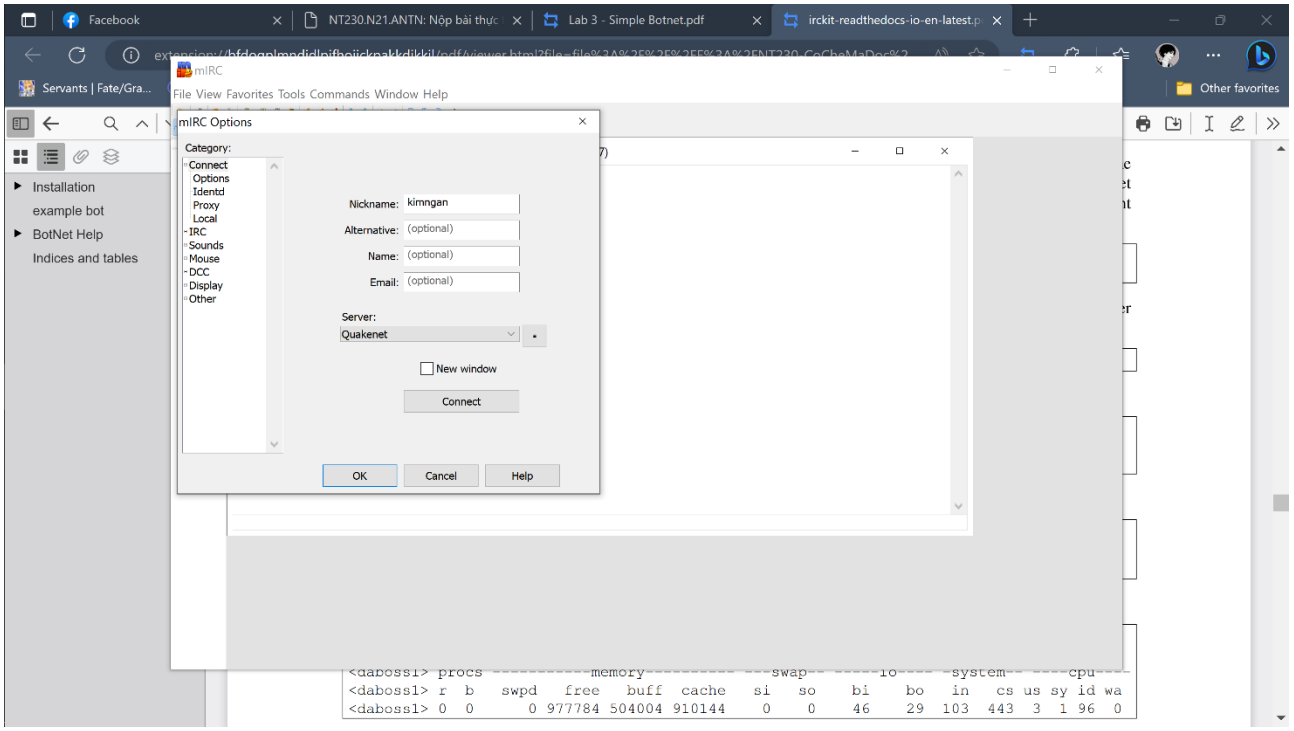
Request JOIN để worker tham gia vào channel của boss

Tạo worker thứ 2 bằng cách tạo terminal khác. Các bước tương tự như trên. Do nick worker đã được dùng nên worker mới này có nick là worker_576

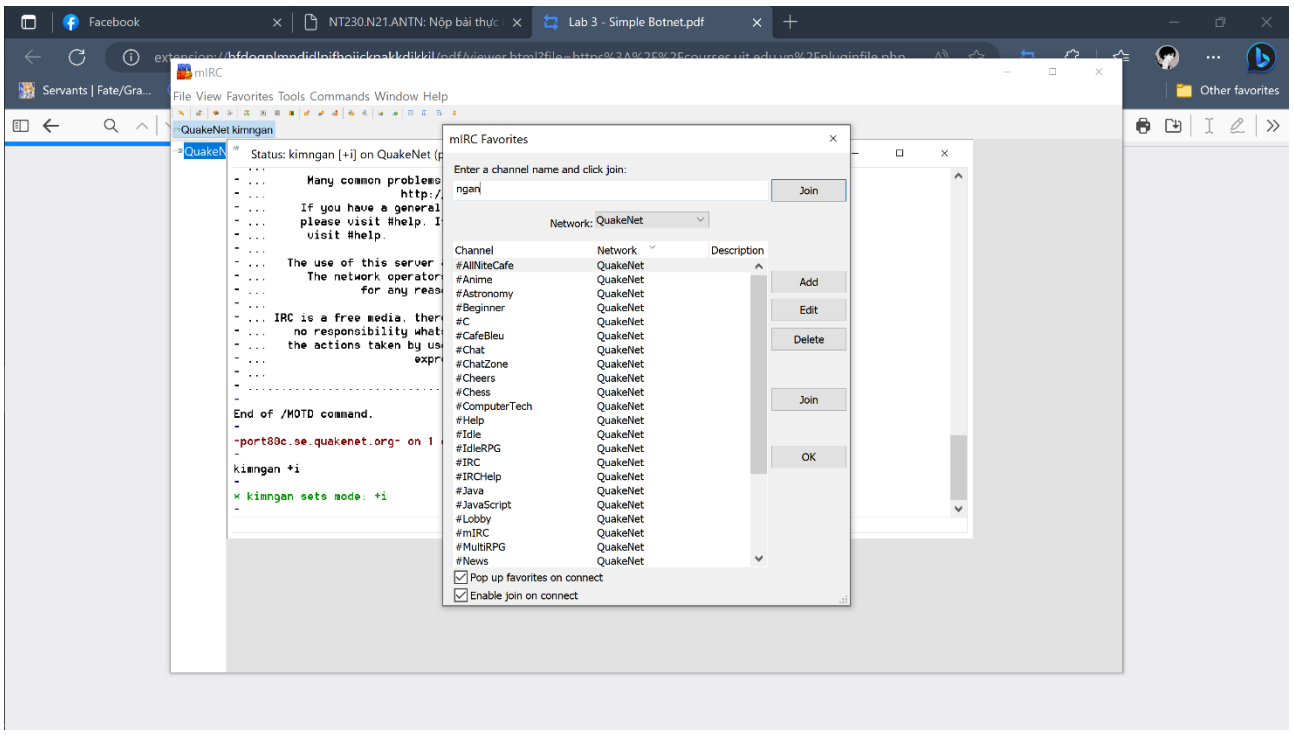


4. Kịch bản 03: Báo cáo kết quả chạy command IRC client.

Cài đặt mIRC lên máy window. Chọn server Quakenet (server mà boss kết nối tạo channel), đăng ký nickname, Connect.



Viết tên channel đã chọn, Join



!auth [password] để xác thực với boss

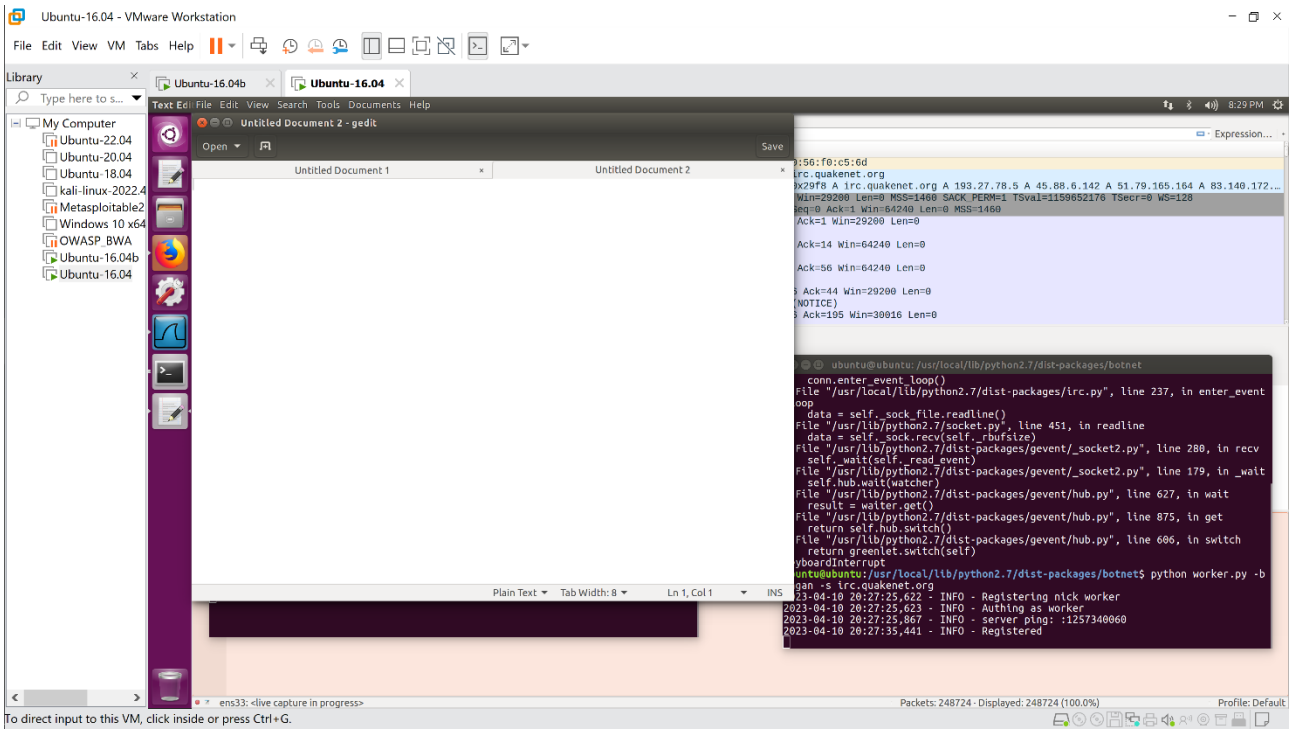
!status thấy rằng có 2 worker đang hoạt động

```
* Now talking in #ngan
<kimngan> !status
<kimngan> !auth ngan
<@ngan> Success
<kimngan> !status
<@ngan> 2 workers available
<@ngan> 0 tasks have been scheduled
```

Tạo task chạy gedit (text editor) cho worker

```
<kimngan> !execute run gedit
<@ngan> Scheduled task: "run gedit" with id 1 [2 workers]
<kimngan> !print
<@ngan> [worker_883:{ubuntu}] - run gedit
<@ngan> [worker:{ubuntu}] - run gedit
```

Kiểm tra lại máy ubuntu worker, text editor đã được bật



Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT