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: 04/10/2023*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.N21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Kịch bản 01/Câu hỏi 01 | 100% |  |
| 2 | Kịch bản 02 | 100% |  |
| 3 | Kịch bản 03 | 100% |  |
| 4 | Kịch bản 04 | 100% |  |
|  |  |  |  |

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

BÁO CÁO CHI TIẾT

## Kịch bản 01

Đầu tiên ở máy 1 ta thực hiện chạy lệnh boss bằng lệnh:

python boss.py -c kiet -n kiet -x kiet

A screenshot of a computer

Description automatically generated

Đồng thời ta thực hiện việc bắt gói tin

A screenshot of a computer

Description automatically generated

Phân tích gói tin thì ta thấy được:

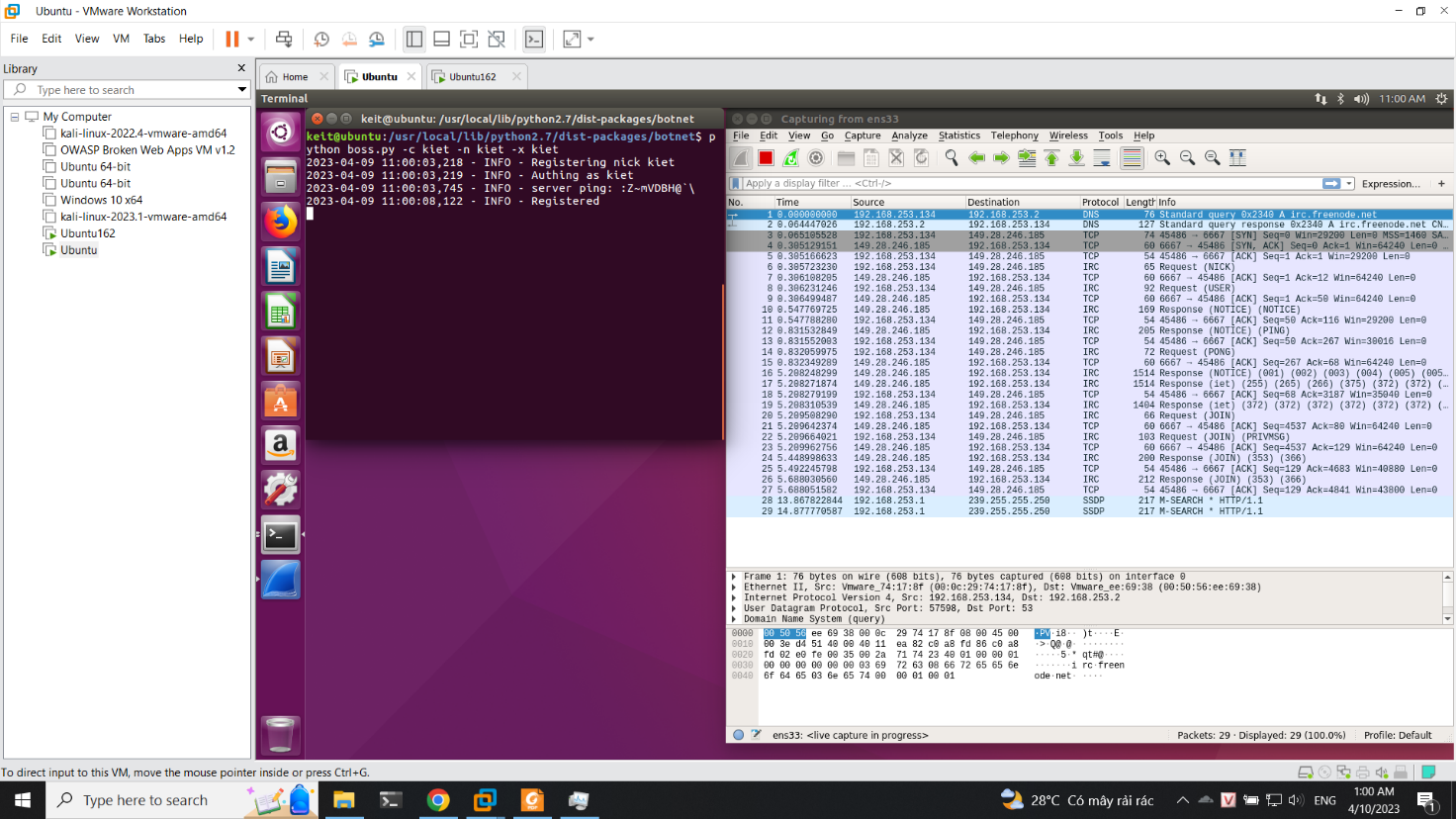
Gói 1 2 là thực hiện việc phân giải tên miền

Gói 3 4 5 là quá trình bắt tay ba bước

Gói 6 đến 19 là thực hiện quá trình kết nối đến server là gửi các request tạo các thông tin được nhập ở console

Gói 20 đến 27 là thực hiện việc join boss vào server và tạo channel như người dùng đã nhập ở console

Fullscreen:



## Kịch bản 2

Trên máy 2, thực hiện chỉnh sửa code:

Tạo một bản copy của worker.py đặt tên là myworker.py

Tắt các dòng lệnh:

#from gevent import DNSError

#Except DNSError:

#pass

Sau đó thực hiện chạy bằng lệnh python myworker.py -b kiet

Text

Description automatically generated

Đồng thời thực hiện bắt gói tin

Text

Description automatically generated

Phân tích gói tin ta thấy được

Gói 1 2 là thực hiện việc phân giải tên miền

Gói 3 4 5 là quá trình bắt tay ba bước

Gói 6 đến 25 là quá trình thực hiện quá trình kết nối đến channel

Ở đây ta thấy được sẽ có những gói join như boss vì không thực hiện việc tạo channel mà join vào channel đã có

Fullscreen

Text

Description automatically generated

## Kịch bản 3

Ở máy window ta thực hiện cài mIRC và thực hiện một số lệnh cơ bản như hình

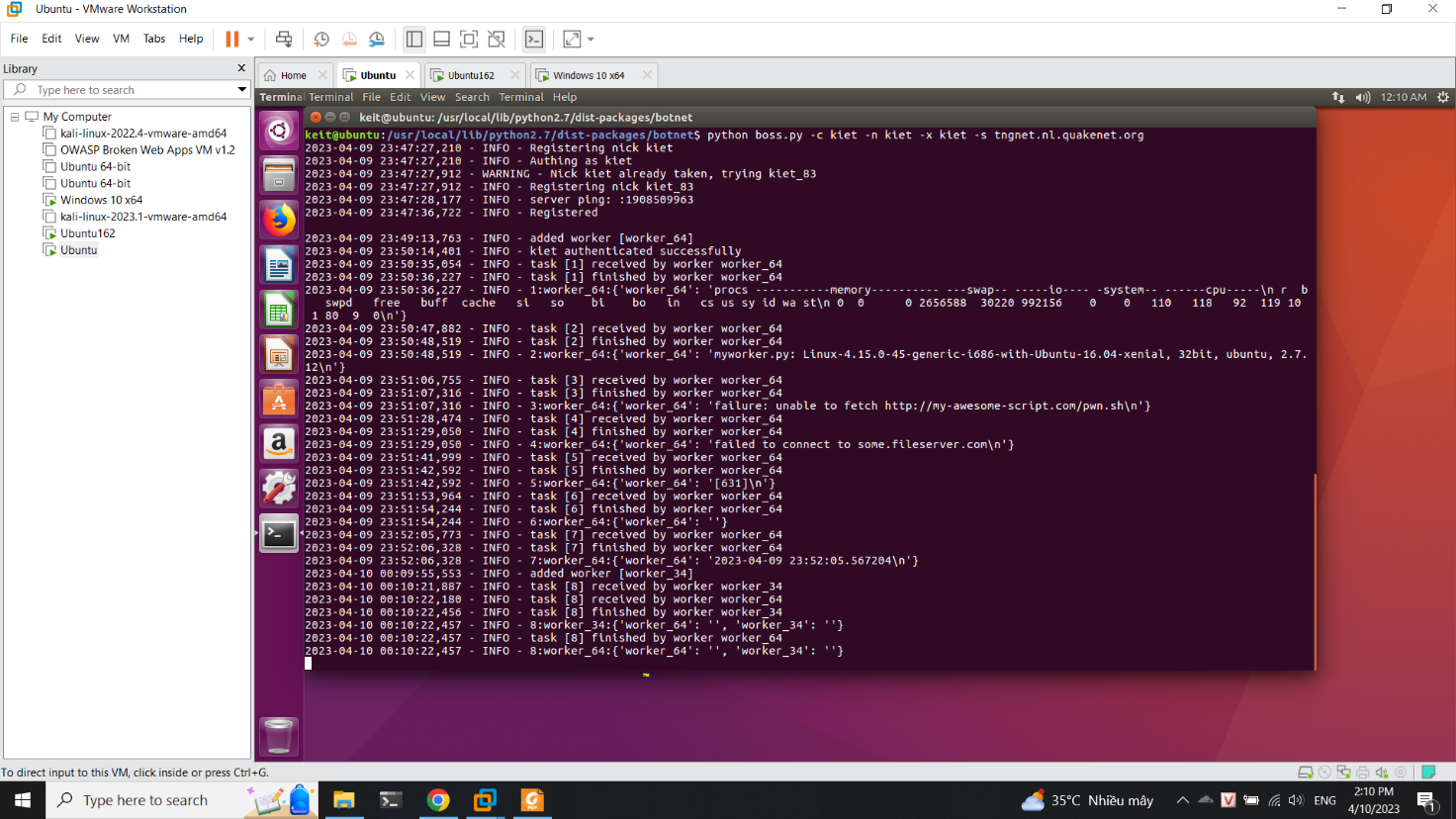
Graphical user interface, text, application, Word

Description automatically generated

## Kịch bản 4

Ở trường hợp khi thực hiện trên lớp do có quá nhiều lượt truy cập gọi đến thì ta sẽ thực hiện việc sử dụng server khác thay vì server mặc định vì do quá nhiều lượt truy cập

Ở máy 1 gọi lệnh python của boss:



Ở máy 2 mở 2 terminal và chạy lệnh python của worker:

A screenshot of a computer

Description automatically generated

Cuối cùng kiểm tra trên máy win thì ta thấy đã kết nối được 2 worker:

Graphical user interface, text, application, Word

Description automatically generated

Full screen:

Graphical user interface, text, application, Word

Description automatically generated

---

***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**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)