BÁO CÁO THỰC HÀNH

**Môn học: Cơ chế hoạt động của mã độc**

**Lab : BOTNET**

*GVHD: Nguyễn Hữu Quyền*

1. **THÔNG TIN CHUNG:**

Lớp: NT230.N21.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hoàng Văn Anh Đức | 20520890 | 20520890@gm.uit.edu.vn |
| 2 | Nguyễn Mạnh Cường | 20520421 | 20520421@gm.uit.edu.vn |
| 3 | Lê Quang Minh | 20520245 | 20520245@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Thành viên thực hiện** |
| 1 | 1-> | Đức + Cường |

**BÁO CÁO CHI TIẾT**

# Giả lập Botnet

## Yêu cầu 1: boss.py: Từ kết quả Wireshark thu thập được, hãy phân tích quá trình gì đang diễn ra.

Set up môi trường để thực hiện bài

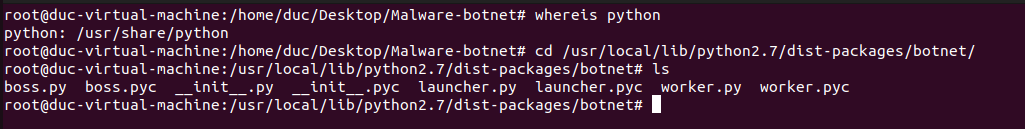
* Chạy file setup.sh và apt.sh

A screenshot of a computer

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated with medium confidence



* "**python2 boss.py -c nt230k15 -n k15master -x qwerty -s irc.axon.pw**"
  + sẽ chạy một chương trình Python có tên là "boss.py" và cung cấp các tham số để thiết lập kết nối đến một server IRC trên địa chỉ "irc.axon.pw" với tên người dùng là "k15master" và mật khẩu là "qwerty" để tham gia vào kênh "nt230k15"

Boss->server : boss assign nick name (“k15master”)

A screenshot of a computer

Description automatically generated

Boss->Server : Boss assign hostname (“**irc.axon.pw**”)

A screenshot of a computer

Description automatically generated

Server không phân giải được hostname của boss , thiết lập connection thông qua IP

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Server->boss : Tạo hostname và channel thành công

A screenshot of a computer

Description automatically generated with medium confidence

Boss join vào channel

A screenshot of a computer

Description automatically generated

## Yêu cầu 2: worker.py: Từ kết quả Wireshark thu thập được hãy phân tích những gì đang diễn ra.

-Chạy 2 file này để setup môi trường

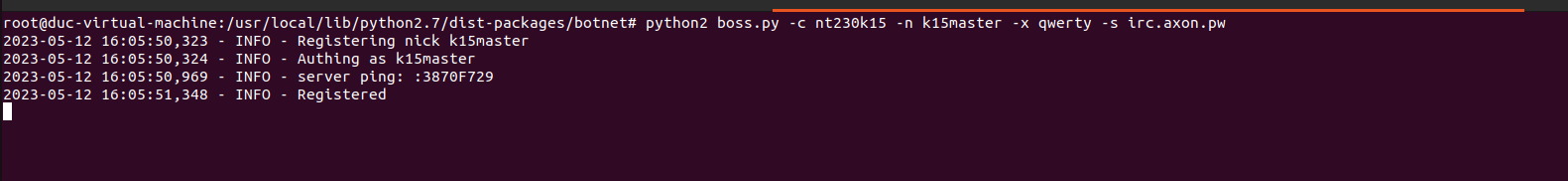
A screenshot of a computer

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated with medium confidence

Tạo channel để worker join vào (botnet)

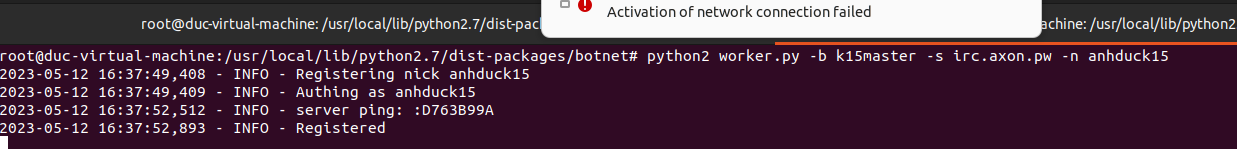


Bật wireshark để bắt các gói tin giao tiếp

A screenshot of a computer

Description automatically generated with low confidence

Ở máy worker join vào channel



Worker->Server : đăng kí nickname

A screenshot of a computer

Description automatically generated

Worker->Server : Hostname

A screenshot of a computer

Description automatically generated

Communicate bằng IP

Server->Worker : Worker host is applied

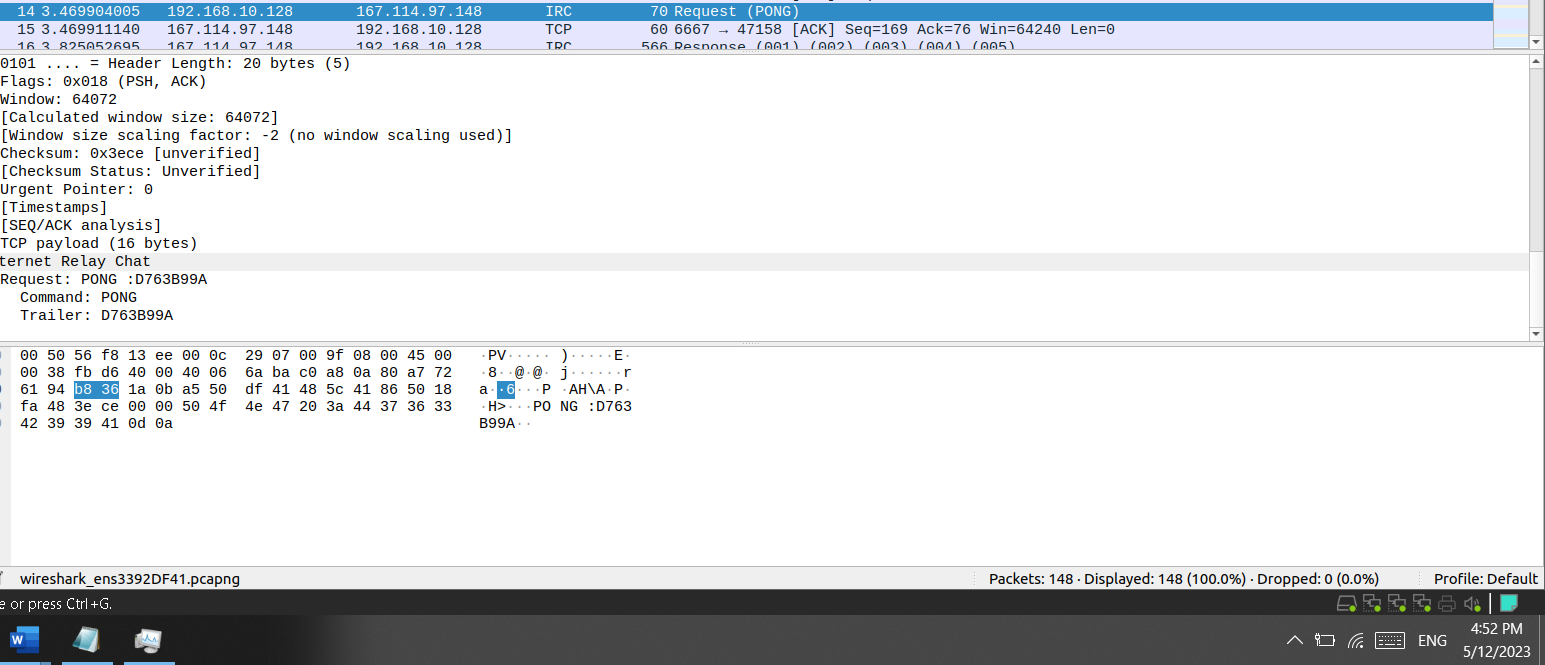
* cấu hình worker host đã được áp dụng thành công. Điều này có nghĩa là worker host đã được đăng ký thành công và sẵn sàng để thực hiện các tác vụ được giao cho nó

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

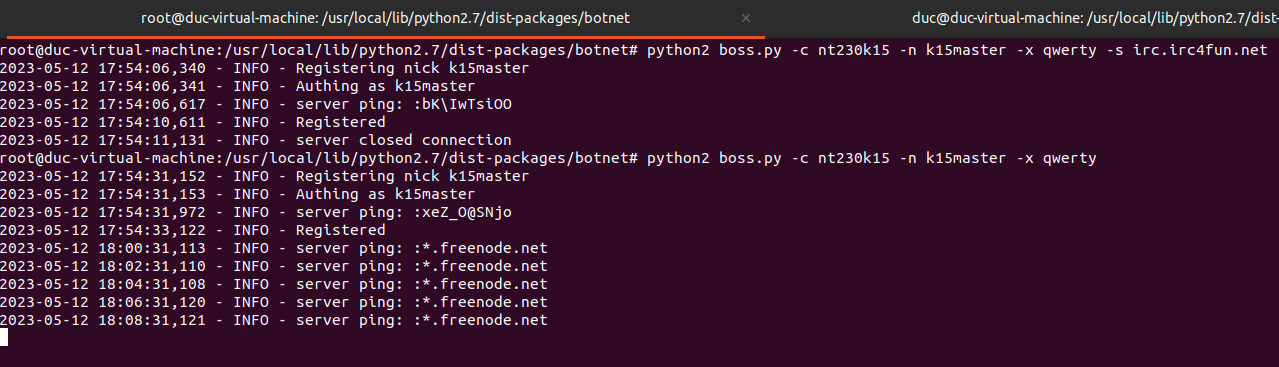


A screenshot of a computer

Description automatically generated

## Yêu cầu 3: Điều khiển worker sử dụng mIRC

Sử dụng command này “**python2 boss.py -c nt230k15 -n k15master -x qwerty**” để tạo channel “**nt230k15**” với tên boss là “**k15master**” , mật khẩu để làm boss là “**qwerty**”



Tải và mở mRIC và điền tên rồi vào channel

(không set -s thì mặc định sẽ là \*.freenode.net)

File -> Select channel

Tại chỗ channel chọn Add

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Ok và nhấn Connect

Tại đây hiện ra cửa sổ mới điền tên của channel -> Join

A screenshot of a computer

Description automatically generated

Chứng thực để thành boss

A screenshot of a computer

Description automatically generated with medium confidence

Ở máy worker sử dụng command bên dưới để join vào channel

A screenshot of a computer program

Description automatically generated with low confidence

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